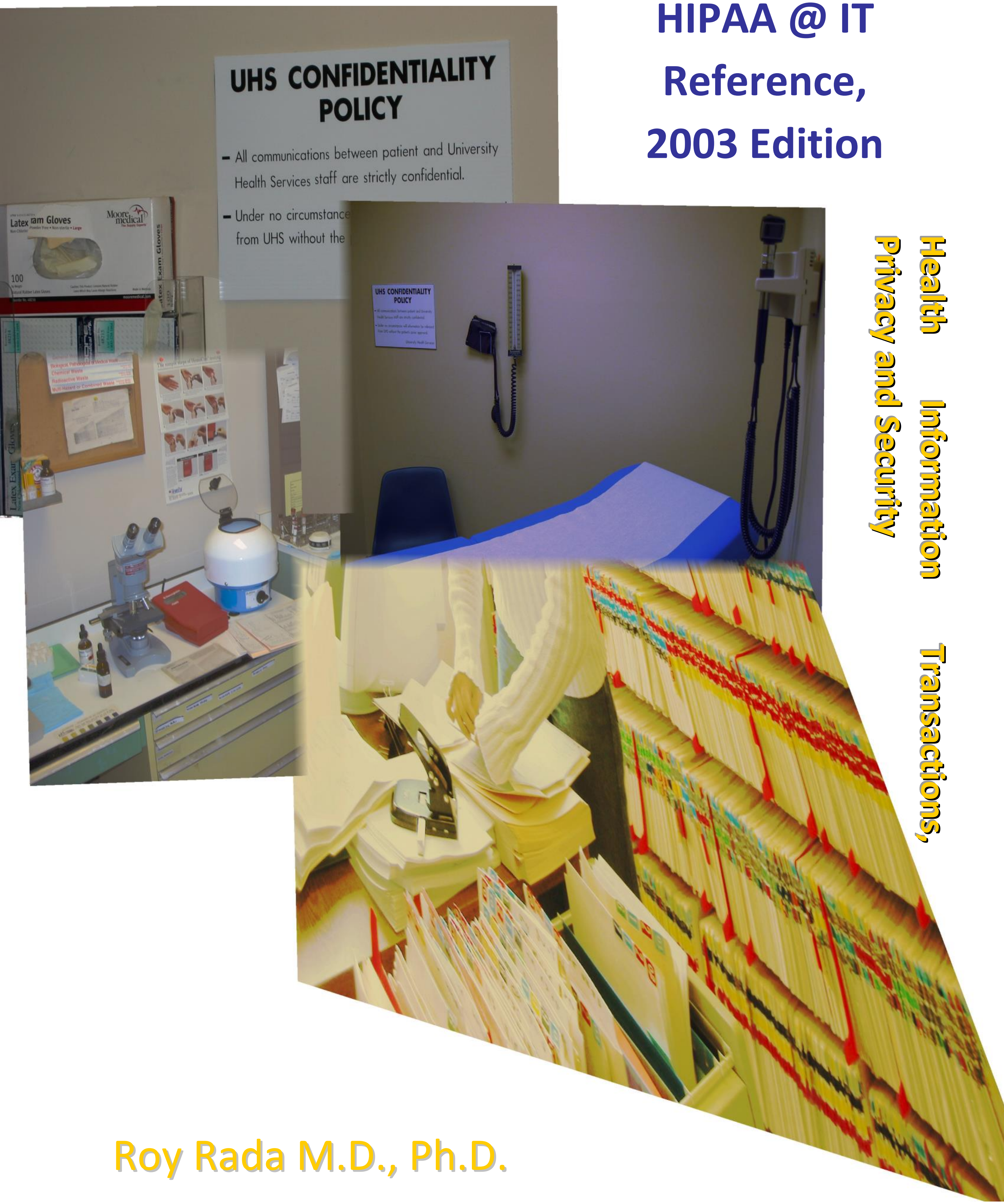
HIPAA @ IT Reference, 2003 Edition

Health Information Transactions, Privacy and Security


UHS CONFIDENTIALITY POLICY
- All communications between patient and University Health Services staff are strictly confidential.
- Under no circumstance
from UHS without the
Latex Exam Gloves
Moore medical
100
UHS CONFIDENTIALITY POLICY

Roy Rada M.D., Ph.D.

HIPAA @ IT Reference, 2003 Edition:

Health Information Transactions, Privacy, and Security

Roy Rada, M.D., Ph.D.

Department of Information Systems
University Maryland, Baltimore County
Baltimore, MD 21250

Hypermedia Solutions Limited

www.hipaa-it.com

Published by: **Hypermedia Solutions Limited**

electronic copies available at **www.hipaa-it.com**

British Library Cataloguing (in process)

Rada, R. (Roy), 1951-

HIPAA@IT Reference, 2003 Edition: Health Information Transactions, Privacy, and Security
ISBN: 1-901857-17-4

Printed October 2002

Preface

People need to understand the information systems ramifications of the Health Insurance Portability and Accountability Act (HIPAA). They are eager to get unbiased and comprehensive information about what HIPAA means for them. This book addresses that need. A two-level outline, a full outline, an executive summary, and then the body of the text follow the preface.

Content

This book is organized into the following three main chapters:

- Transactions and Codes,
- Privacy, and
- Security.

The *Transactions and Codes* Chapter relates to exchanges between healthcare providers and payers. The Chapter covers

- transactions,
- code sets,
- identifiers,
- impact, and
- implementation.

The *Privacy* Chapter focuses on the relationship between patients and the healthcare system, and the chapter addresses

- notice and authorization,
- uses and disclosures
- patient rights,
- administration,
- other regulations, and
- impact.

The *Security* Chapter explains how to keep information safe and covers:

- compliance life cycle,
- real-world security policy;
- computer security models; and
- technical security mechanisms.

The Introduction Chapter gives the history of HIPAA and of compliance more generally. The Conclusion Chapter looks in particular at corporate compliance and at the practices that providers are using to achieve HIPAA compliance.

Healthcare providers and payers have agreed that standardization of the transactions between them would be helpful. Standards for transactions and code sets are vital to efficient and effective communication among healthcare organizations. The impact should be higher quality at less cost.

Privacy relates to power. When one person has another person's private information, that other person loses some control. This power perspective sheds light on the intense conflict that surrounds privacy discussions. The Privacy Rule gives the patient strong rights over his or her information.

The Security Chapter describes how organizations address the proposed Security Rule. Workflow management is vital to healthcare organizations and when done properly gives security as a derivative. Therefore, organizations should see the proposed Security Rule as a challenge to improve their *workflow*.

The book includes several other parts that provide context to the three main chapters. Those *additional parts* include Outlines, Introduction, Conclusion, References, and Appendix, as follows:

- The 'Introduction' explains the background of HIPAA, the history of compliance, and industry trends.
- The 'Conclusion' looks in more detail at the trends.
- The 'References' list approximately 170 sources of further information that are cited in the book.

The Appendix presents the full text of the HIPAA Administrative Simplification provisions, summaries the proposed security rule, and has a 'Competency Test'. If the reader can correctly answer most of the seventeen, multiple-choice questions in the '*Competency Test*', then the reader is probably competent in the subject matter of this book.

Style

The main chapters cover the regulations of administrative simplification with history, background, implications, and examples. The strength of the presentation lies in its comprehensive view of the *conceptual issues*.

The chapter, top-level subsections typically begin with a '*Main Points*' list that mentions each main point of the subsection. These subsections end with a set of '*Review Questions*'. The 'Review Questions' touch on each main point and give the reader a chance to check whether he or she digested the material well enough to answer basic questions. The 'Review Questions' sometimes include 'Project Questions' that take the reader beyond a recounting of what the book presented and ask the reader to explore new content.

The author has marked key terms in the text. These terms have been alphabetically listed in the back of the book with pointers to their occurrence in the body of the text.

Timing

HIPAA calls for the Department of Health and Human Services (DHHS) to develop the rules to standardize transactions, privacy, and security. DHHS went through an extensive information gathering and consensus building process and then published elaborate proposed rules. Each such publication is called a *Notice of Proposed Rule Making (NPRM)*. Then DHHS went through another round of collecting input -- this time specifically as feedback to the NPRMs. The Transactions and the Security NPRMs were published in 1998, and the Privacy NPRM in 1999. Tens of thousands of comments were received. The Transaction Final Rule was published in August 2000 and the Privacy Final Rule in December 2000. However, the Bush Administration took additional comments on the Privacy Rule and delayed official publication till April 2001. The Administrative Simplification Compliance Act of December 2001 allows for a year delay in transactions compliance. Modifications to the Privacy Rule were published in August 2002. The Security NPRM had not been converted into a Final Rule as of September 2002.

The reader is assured that the author will watch for any changes in law or regulation. When a significant change occurs, the author will make available updated information. The publisher also makes available a *Monthly Update* as advertised at the back of the book.

Audience and Related Work

Anyone working in or around healthcare could benefit by reading this book. The targeted audience is people in healthcare organizations that have some information systems responsibility. More particularly, managers in hospitals and information systems consultants have responsibilities that require them to know the content of this book. The book also serves many others, such as nurses or radiologists within the provider community, information systems staff within an insurance company, and salespeople in consulting firms. A company might use the books to help persuade staff about the *relevance of HIPAA* to a company's information policies and tools.

The material assumes no particular background of the audience as regards information systems or healthcare. However, maturity is assumed in terms of understanding both healthcare and information systems.

The author has been unable to find a comparable book on HIPAA plus information systems. Early in the life of HIPAA there were books on the insurance portability issues of HIPAA or the income tax deduction aspects of HIPAA that were written for insurance, law, or accounting professionals. Next came a book for the HIPAA proposed security rule by Tomes (1999). Then two edited books (Britten et al, 2000 and Rada, 2001b) on the proposed security rule appeared. Two books on privacy were recently released (Britten et al, 2001 and Gue and Fox, 2002). Microsoft and Washington Publishing Company have released a book that emphasizes the commercial solution that those companies offer for translating transactions (Bass, et al, 2002). Some books focus on a particular phase in the life cycle of HIPAA compliance (Joseph and Coleman, 2002) and another has appeared on IT (Bogen, 2002). This book *HIPAA@IT Reference* is the most comprehensive on administrative simplification and information systems.

Author and Acknowledgments

The author's educational credentials include:

- Ph.D. from University of Illinois at Urbana in Computer Science, 1981.
- M.D. from Baylor College of Medicine, 1977.
- B.A. from Yale University in Psychology, 1973.

Rada is a Professor of Healthcare Information Systems at the University of Maryland Baltimore County. Previously he was Boeing Distinguished Professor of Software Engineering at Washington State University and Editor of *Index Medicus* at the National Library of Medicine, Bethesda, Maryland. He has authored 200 journal articles and 6 books. The first article appeared in 1979 in *Computers and Biomedical Research* and described his coding system for medical problem statements. He has worked as a consultant on computer-supported diagnosis in pathology and radiology, led a team developing medical informatics standards, and developed online training material for doctors.

The constructive feedback from various readers of the first edition motivated the author to produce the second edition. Rob Fromberg and D'Arcy Gue were particularly helpful in bringing the original book to the attention of others. Students at the university did exercises from an accompanying workbook and provided feedback as to the utility of the book. Any errors in the book are solely the responsibility of the author.

Table of Contents

Executive Summary

Main Points

- The Transaction Rule facilitates information exchange between providers and payers.
- The Privacy Rule gives patients new rights.
- The Proposed Security Rule is for safeguarding information.

HIPAA has become a rallying cry for advocates of information systems improvements in healthcare. Literally, HIPAA means 'Health Insurance Portability and Accountability Act', but the information systems ramifications are mainly in the 'Administrative Simplification' provisions of the Act. Administrative Simplification calls for standardization of transactions between providers and payers. At the same time, it requires that the sharing of electronic information be done securely and privately.

Introduction

Americans originally had a simple economy based on self-employed individuals operating under minimal government intervention. The rise of large industries, however, led the people to seek government constraints on industry.

The rising cost of healthcare stimulated a government effort to reduce administrative overhead by standardizing provider-payer transactions. Concomitant with that standards effort, the government realized that privacy and security of healthcare information deserved further protection. In 1996 legislation to this effect was incorporated into HIPAA. The increasing

- numbers of allied healthcare personnel, now numbering over half of the entire healthcare workforce, and
- use of information systems to semi-automate the healthcare industry

are trends that will keep standards and privacy high on the agenda.

The Department of Health and Human Services (DHHS) publishes a Notice of Proposed Rule Making as it attempts to gain consensus for its approach before publishing a Final Rule. Once a *Final Rule* is published, the industry has approximately two years in which to comply with the rule. Penalties can be severe for failure to comply, but generally speaking, the rules are flexible and call for common-sense behavior.

Transactions

Administrative Simplification means standardization of transactions, security, and privacy. The transactions at issue are largely those between providers and payers. DHHS mandates existing standards wherever practical. The Electronic Data Interchange standards of the standards development organization X12 were chosen for most HIPAA transactions. X12 has developed detailed implementation guides for the representation of healthcare claims, eligibility inquiries, enrollments, and other transactions. Some fields within these transactions must be completed with entries from specified *code sets*. For instance, the code set for diseases is the International Classification of Diseases.

In addition to code sets, the transactions contain *identifiers*. The Employer Identifier is the Employer Identification Number (EIN) assigned by the Internal Revenue Service. The proposed standard for Provider Identifiers is based on an arbitrary string of characters assigned uniquely to a provider but associated with a provider file that contains about one hundred items of information about each provider. The public was so concerned that a patient identifier would be abused that the government has delayed any standardization of a patient identifier.

One challenge in the implementation of the transaction standards is to coordinate different entities to make the same changes at the same time. Third-party certification of compliance also facilitates the implementation phase.

The Administrative Simplification Compliance Act specified an October 2002 deadline for covered entities to submit a plan for achieving compliance with the Transactions Rule and thus earn a 1-year delay in the deadline for compliance with that Rule. The Act also appropriated money to DHHS to provide model compliance plans and threatens to limit Medicare payment to entities that are not compliant.

Each covered entity needs to exhaustively inventory its current information flow and map old data elements to new data elements. Providers and health plans have the option of relying on a clearinghouse to put their transactions into standard format given that they give the clearinghouse the correct data elements. Relying on a clearinghouse is not, however, the best long-term solution for a large entity that could afford to develop its own translators and directly generate transactions in the standard format.

The current standardization of transactions between providers and payers is the beginning. DHHS will coordinate the development of *further transaction standards*, such as standards for claims attachments. Additionally, HIPAA specifically calls for DHHS to study patient medical record information and recommend standardization of that information.

Privacy

The HIPAA Privacy Rule creates a national baseline for the privacy of healthcare information. The Privacy Rule describes how patient information must be handled in the healthcare system. The Rule both

- brings the patient closer to the process and
- requires healthcare organizations to clearly specify what roles are to manipulate what patient information.

Both of these changes could improve the healthcare process.

The Privacy Rule is applicable to all healthcare providers and health plans that engage in electronic transactions. For such covered entities, all *information*, whether paper-based, electronic, or otherwise must be handled in accord with the Privacy Rule.

Entities must post notice about their privacy policies and make clear to patients the strong rights that patients have. These *notices* must be posted or distributed in such a way as to come to the attention of all concerned parties in a timely fashion. Direct treatment providers must make a good faith effort to obtain a patient's written acknowledgment of the notice of privacy rights and practices.

Information is used inside an entity, but disclosed when it leaves an entity. Before *individually identifiable health information* is used or disclosed for other than routine purposes, authorization from the patient is required, except in certain circumstances. An authorization should contain the expiration date of the authorization, the signature of the patient, and certain caveats.

Authorization is not required when:

- about certain patients or
- for certain purposes.

Military patients illustrate the exception for type of patient. *Military patients* lose much of their privacy. The military may want able-bodied people to handle dangerous weapons, and the commanders of troops are expected to have access to medical records of their troops.

The 'exception for purpose' includes infrequent purposes like criminal investigations but also common purposes that go under the heading of *research* or *business associates*:

- Research serves a public good. If researchers needed to get authorization for every patient record that the researcher might see, then research might be slowed. *Researchers* may obtain permission from their institution to see patient records.
- The Rule also permits a covered entity to share information for certain healthcare purposes when a business associate contract has been signed. The business associate contract binds the entity receiving the information to treat the information as confidential.

The Privacy Rule's Minimum Necessary Standard requires policies for what *roles* should manipulate what information. Healthcare professionals must have relatively unencumbered access to the medical record for the purpose of delivering care. Other frequent demands on protected health information must be handled through policies in a systematic way.

The HIPAA Privacy Rule generally treats information about one medical condition the same as information about any other medical condition. Psychotherapy notes are an exception. Psychotherapy notes may not be routinely shared and require patient *authorization* for any disclosure.

The Privacy Rule gives patients basic rights. Three rights are to:

- access the patient record,
- amend the record, and
- see an accounting of what disclosures were made.

If the patient requests a copy of his or her medical record, the healthcare entity can only charge for the cost of reproducing the record and cannot charge for the effort of managing the request or finding the record.

The Privacy Rule has broad administrative requirements. Healthcare organizations must:

- designate a privacy officer,
- document their privacy policies,
- train their staff on privacy,
- safeguard information,
- verify that their business associates treat patient information respectfully,
- be sensitive to complaints from staff and patients about privacy matters, and
- impose sanctions on violators of the privacy policy.

The Rule leaves the specifics to the healthcare organization. For instance, how much training is provided or in what format is to be determined by each organization. The challenge to the healthcare entity is to meet the requirements in a way that integrates smoothly with *current practices* and that improves the quality of the entity's services.

Through HIPAA, Congress defines fines for violators of the Privacy Rule. DHHS enforces the Privacy Rule by both actively reviewing healthcare entity behavior and by openly soliciting any and all complaints from patients or staff.

State health privacy statutes cover a broad range of conditions and, not surprisingly, are weak in some ways and strong in others. In terms of broad consumer protections, one can identify many significant gaps and weaknesses in most state statutes, such as:

- a limited right for a patient to access his or her own medical record;
- little ability for patients to limit disclosure of their medical records; and
- little recourse when the laws are violated.

On the other hand, state laws enacted in response to a particular public concern, or a public health threat are often strong, detailed, and aimed at the states' unique experiences with their citizens. Generally, state laws are narrow and provider-oriented, while HIPAA is broad and patient-oriented.

The Joint Commission on the Accreditation of Healthcare Organizations (JCAHO) helps standardize the behavior of healthcare organizations through its certification criteria. JCAHO is extending its certification criteria to conform to HIPAA's Privacy Rule.

DHHS made an extensive analysis of the cost of implementing the Privacy Rule over a 10-year period. The total cost is estimated to be $18 billion. The two largest items are the employment of a 'Privacy Official' and implementation of 'Minimum Necessary Use', with each costing about $6 billion over the first 10 years. To perform its cost estimates DHHS determined

- the roles that would have to perform the work required by the Privacy Rule,
- how many hours they would take, and
- what the hourly wage was.

The analysis is an excellent starting point for long-term planning of resources and strategies for healthcare entities.

Security

The *Security Notice of Proposed Rule Making* was published in 1998. The Security Rule would apply to each health care entity engaged in electronic maintenance or transmission of health information.

Security begins with real-world policy and proceeds to computer policies and then technical mechanisms. The real-world policy concerns how people work together. Computer policies specify how the machine works with information given it by people. Technical mechanisms are things like passwords.

Each organization must

- become aware of the importance of security,
- assess the gap between its situation and what the community has agreed is a desirable level of security,
- determine what investments would reduce what risks,
- implement security measures, and
- maintain quality control.

All these activities must be documented. Examples of policies from Kaiser Permanente and the Mayo Clinic are available.

Someone in the organization must wear the hat of the *security officer*. In a large organization the security staff may include several specialists. Everyone in the organization needs, at least, basic training about security.

One level beneath the real-world security policy is the computer security policy. Label-based and role-based access controls are popular. In label-based access, top-secret documents can only be read by people with top-secret status. Role-based access control requires an organizational manual that specifies the roles in the organization and what information each role is expected to manipulate. People are assigned dynamically to roles. Role-based access control is part of workflow management.

Computer mechanisms help implement computer policies. Cryptography provides one kind of security by putting information behind an information lock. In the most popular cryptographic technique, each individual has a public and private key. Managing the information keys becomes a challenge. A *public key infrastructure* creates registries for public keys. Healthcare has special needs as regards these registries.

Conclusion

The compliance life cycle is basically one of education, implementation, and audit. This cycle must be repeated over and over again as the objective is not to reach one certain point but rather to operate in a compliant way all the time.

Entities of a certain type should work together to establish policies and procedures that suit their type. In this way, the entities will have saved one another effort and will have been proactive in defining for the government what constitutes best practices. Since HIPAA has to do with how an entity works, each entity within a type might take the policies and procedures agreed among its peers and tailor them to the particular culture of that entity.

HIPAA is an act of Congress. As any act of Congress, it may be modified through time by other acts of Congress. Given the enormous influence of HIPAA on the healthcare industry and patients, much maneuvering continuously occurs to support various amendments to HIPAA. This dynamic is permanent.

Success with HIPAA could be a step towards a more efficient healthcare industry and the electronic medical record. However, the critical issue is not technology but how people work together.

Clinton (Aug. 11, 2000) said: Every day, tens of thousands of health claims are submitted to insurers and other payers by our nation's health care providers. These billing forms are often incomprehensible, inconsistent, and duplicative, frequently serving little useful purpose. ...With today's release of new national standards for electronic claims for health care transactions, we are taking a major step towards eliminating burdensome, time-consuming and wasteful paperwork that costs the nation's health care system billions of dollars each year.

Clinton (Dec. 20, 2000) said: The new rules we release today protect the medical records of virtually every American, they represent the most sweeping privacy protections ever written, ...This action is required by the great tides of technological and economic change that have swept through the medical profession over the last few years. ...So, the rules that we release today have been carefully crafted for this new era, to make medical records easier to see for those who should see them, and much harder to see for those who shouldn't.

William Clinton photo from
www.whitehouse.gov/history

1 Introduction

Targets

Learning Objectives

- Distinguish those aspects of HIPAA germane to administrative simplification from those not.
- Delineate a history of compliance that places HIPAA in context.
- Predict the demand for HIPAA-type reforms based on the trends in the health industry.

Main Points

- The Administrative Simplification Title of HIPAA calls for standard transactions between payers and providers and also for security and privacy of healthcare information.
- The history of compliance shows the importance of cooperation among public, corporate, and government interests.
- This history of 'Administrative Simplification' shows a complex dynamics among healthcare industry components and the government.
- Trends in personnel, administration, and information systems show the increasing role of standardization.
- While corporate compliance has certain broad universal features, the specific compliance program that will work in a particular entity depends on the culture of that entity.

The healthcare enterprise is an information intensive enterprise that in the United States includes healthcare providers, payers, patients, employers, government, and support units in a complex network. Recent legislation, entitled Health Insurance Portability and Accountability Act (HIPAA), has major implications for this healthcare network. Given HIPAA's complexity, many people are confused as to what to do to comply with the legislation. This book analyzes the 'Administrative Simplification' provisions of HIPAA with an emphasis on those aspects of it that have significance for *information systems*.

1.1 HIPAA Overall

Main Points

- HIPAA covers insurance portability, fraud, and administrative simplification.
- The history of insurance portability shows the balancing of state and federal authority.
- Whistleblowers are encouraged to report fraud.
- Administrative Simplification addresses the need to reduce administrative overhead costs in healthcare through standardized transactions.
- Standardized transactions and increased information flow call for heightened privacy and security.

HIPAA was put into law by the American Congress on August 21, 1996 and is heralded as the most significant healthcare legislation in the United States of the past many years. HIPAA covers a wide-range of topics that are not always related to one another. The Act calls for health insurance that is portable and accountable, and the acronym is the 'HIPA Act' or 'HIPAA'. Despite this name based on portable and accountable insurance, the Act is famous for its emphasis on standardized transactions, security, and privacy -- all three of which are placed under the heading of *Administrative Simplification* in HIPAA, although the 'A' in 'Administrative' is not represented in the acronym 'HIPAA.

1.1.1 Overview

HIPAA is also known as Public Law 104–191. The Act's introductory paragraph says:

> … to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and healthcare delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes. Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, … the "Health Insurance Portability and Accountability Act of 1996".

The Act has 5 top-level titles as follows:

- Title I: Healthcare Insurance Access, Portability, and Renewability (eliminates some pre-existing condition exclusions and prohibits discrimination based on health status and guarantees coverage renewal)
- Title II: Preventing Healthcare Fraud and Abuse; *Administrative Simplification*; Medical Liability Reform
- Title III: Tax-Related Health Provisions (medical savings accounts and health insurance tax deductions for self-employed individuals)
- Title IV: Application and Enforcement of Group Health Insurance Requirements
- Title V: Revenue Offsets.

The title of the Act derives from the 'Portability' of insurance in Title I and the 'Accountability' of billing through fraud prevention in Title II.

For the valuable insights that can be had by understanding HIPAA broadly, the next two subsections briefly review the 'Insurance Portability' and 'Accountability' provisions of HIPAA with an emphasis on how those aspects of HIPAA relate to Administrative Simplification. This book explains insurance portability and fraud prevention in detail in the Appendix.

The most direct impact of HIPAA on information systems comes within Title II, Subtitle F 'Administrative Simplification'. 'Administrative Simplification':

- calls for standardization of 'identifiers and code sets' and 'transactions'. In order that a healthcare provider can communicate systematically with multiple payers, standard identifiers for providers, payers, and patients are proposed. The details of the patient condition need to be systematically described, and thus the code sets are standardized. The identifiers and code sets are embedded in a standard transaction.
- is aimed at facilitating electronic communication. The concern naturally arises for the *security* and *privacy* of that information.

This book focuses on privacy and security.

1.1.2 Insurance

The 'IP' in HIPAA is for insurance portability. HIPAA enacts various protections of the insurance options of individuals and small groups. It limits exclusions that insurers can use, provides credit for past insurance that other insurers must honor, and in various other ways tries to assure that insurance can be purchased. This says nothing about the *cost of the insurance*. HIPAA does not make insurance inexpensive but just available to those who can pay for it.

Most interesting about insurance portability to an information systems specialist is its history of state versus federal authority. The administrative simplification provisions require a *balance* between state and federal powers. This balance is evident in the history of insurance. The general principle is that the federal government tries to leave authority to the states unless the federal government believes the states want help in the form of national requirements. Appreciating the history of this balance for insurance portability gives insight as to why the federal and state governments want a balance of authority over information systems provisions too.

Three insurance laws affect state and federal balance:

- The McCarran-Ferguson Act of 1944 exempted insurers from federal antitrust prosecution, so long as state laws were regulating the insurers.
- While some state regulations prevented Health Maintenance Organizations (HMOs) from appearing, the 1973 HMO Act allowed HMOs to exist.
- The Employees Retirement Income Security Act (ERISA) of 1974 allows employers, unions, and certain other groups to be immune from state law.

HIPAA continues the tradition of federal legislation by leaving most insurance regulation to *state law* but by introducing a new floor for certain kinds of insurance provisions. Most states have some legislation regarding individual and small group insurance portability. HIPAA provides that such state laws remain in force so long as they provide at least as much protection as HIPAA's provisions.

As the country has become more familiar with the ins-and-outs of insurance portability, *new legislation* has appeared to give special protections to special groups. Legislated after HIPAA are the:

- 'Women's Health and Cancer Rights Act' for special portability provisions to women and
- 'Mental Health Parity Act' for special portability provisions to mental health patients.

For Administrative Simplification too one might expect to see new legislation that influences the impact of HIPAA.

1.1.3 Fraud

The first 'A' in HIPAA is for '*Accountability*' and means accountability in insurance claims, or, more to the point, accountability means combating fraud. The American people remain concerned about the high rate of fraud committed by healthcare professionals. HIPAA's fraud provisions help government detect and prosecute fraud.

HIPAA builds on the *False Claims Act* that was passed during the American Civil War. Much corruption occurred in federal procurements during the war, and the government was too busy fighting the war to be able to carefully police the procurements that it made. The False Claims Act encourages citizens to 'blow the whistle' on people or entities that defraud the government. Whistleblowers are entitled to a share of the funds that are recovered from those convicted of fraud. HIPAA increases the reward that whistleblowers can earn. HIPAA also loosens the definition of fraud so that more people can be successfully prosecuted for fraudulent behavior.

Historically, insurance companies had little support legally for investigating or prosecuting fraud. Their easier approach was to raise rates, if fraud ate into their profits. However, in the 1980s the *National Healthcare Anti-Fraud Association* began to bring information from various insurers together and to focus on detecting and attacking fraud. HIPAA encourages collaboration between the federal and private sector in fighting fraud.

HIPAA provides funds for fraud investigations and particularly for semi-automated techniques to detect patterns of fraud. With the vast number of claims and with the many rules about how such claims should be made, computers are well suited to detect fraud. Much *software* exists both for generating claims that should avoid fraud and for detecting fraud in submitted claims.

HIPAA's Administrative Simplification provisions may be enforced, in part, by the mechanisms for fraud enforcement:

- whistleblowers and
- software.

Whistleblowers could be employees or patients who detect violations of the Administrative Simplification provisions. Software would monitor the flow of information and detect abnormal patterns.

Fraud legislation and enforcement is a source of controversy, as illustrated by the following:

- On the one hand, the American Medical Association has filed a lawsuit against federal government anti-fraud efforts.
- On the other hand, the American Association of Retired Persons works with the government to help alert seniors to whistleblower opportunities.

All parties want fairly priced healthcare, but the views about how to achieve this vary.

1.1.4 Administrative Simplification

What is administrative simplification? To some administrative simplification means improvement in operation of the information systems infrastructure of healthcare. To others 'administrative simplification' is an oxymoron in which the increased administration entailed by the new legislation necessarily complicates administration.

A considerable portion of every healthcare dollar is spent on provider-payer transactions, including:

- filing a claim for payment from an insurer,
- enrolling an individual in a health plan,
- paying health insurance premiums,
- checking insurance eligibility for a particular treatment,
- requesting authorization to refer a patient to a specialist,
- responding to requests for additional information to support a claim,
- coordinating the processing of a claim across different insurance companies, and
- notifying the provider about the payment of a claim.

Today these processes involve numerous *paper and electronic forms* and many delays in communicating information among different locations.

Because national standards are not in place today,

- the typical health plan continues to process paper forms that differ in content from one plan to another, and
- the typical physician bills multiple health plans with their varying forms and must respond to additional requirements imposed by managed care organizations.

There continues to be a proliferation of proprietary formats in the healthcare industry. Proprietary formats are unique to an individual business. Business partners that wish to exchange information via *Electronic Data Interchange* (EDI) must agree on which formats to use. Since most healthcare providers do business with a number of plans, they have to produce EDI transactions in different formats (NCVHS, 1998).

National standards will reduce costs. They allow for common formats and translations of electronic information that would be understandable to both the sender and receiver. If national standards were in place, there would be no need to determine what format a trading partner was using. Standards also reduce software development and maintenance costs that are required for converting proprietary formats. The basic costs of maintaining unique formats are the human resources spent converting data or in personally contacting entities to gather the data because of incompatible format. These costs are reflected in increased office overhead, and a reliance on paper and third party vendors as well as communication delays.

Having advocated increased flow of standardized, electronic, provider-payer transactions, the Congress was uncomfortable to leave that information to flow without further privacy and security constraints. To that end, Congress required that laws or regulations for privacy and security be promulgated. These privacy and security results have become understandably a hotter topic in the country than the transaction standards.

The Privacy Rule calls for new policies on the flow of information and new rights for patients to see and amend information their record. The proposed Security Rule requires administrative, technical, and physical procedures for all information. The scope of impact on the day-to-day operations of the healthcare industry of the Privacy and Security provisions of HIPAA is vastly greater than the scope of impact of the Transaction Rule.

1.1.5 Covered Entities

HIPAA applies to covered entities, and covered entities are health plans, healthcare clearinghouses, and healthcare providers. The Transaction Rule applies to any covered entity that transmits any health information in electronic form in connection with HIPAA transactions. Given that an entity does any electronic transaction, the Privacy Rule applies to all individually identifiable patient information in whatever form communicated for whatever purpose among any *covered entities*.

Health care providers may be categorized as individuals, organizations, or groups (DHHS, 1998c):

- Individual--A human being who is licensed, certified or otherwise authorized to perform medical services or provide medical care, equipment and/or supplies in the normal course of business. Examples of individuals are physicians, nurses, dentists, pharmacists, and physical therapists.
- Organization--An entity, other than an individual, that is licensed, certified or otherwise authorized to provide medical services, care, equipment or supplies in the normal course of business. The licensure, certification, or other recognition is granted to the organization entity. Examples of organizations are hospitals, laboratories, ambulance companies, health maintenance organizations, and pharmacies.
- Group--An entity composed of one or more individuals, generally created to provide coverage of patients' needs in terms of office hours, professional backup and support, or range of services resulting in specific billing or payment arrangements. Two physicians practice as a group

when they bill and receive payment for their services as a group.

A *health plan* pays the cost of medical care and may also provide care. This definition includes Medicare, Blue Cross, TRICARE, and many others. The statutory definition of a health plan does not include workers' compensation programs, property and casualty programs, or disability insurance programs -- these programs may pay health care costs in the course of administering non-health care benefits but are not considered to be health plans.

A *health care clearinghouse* is a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements. Such an entity is one that currently receives health care transactions from health care providers and other entities, translates the data from a given format into one acceptable to the intended recipient, and forwards the processed transaction to appropriate health plans and other health care clearinghouses, as necessary, for further action. A number of private clearinghouses perform these functions for health care providers. Billing services, re-pricing companies, community health management information systems or community health information systems, value-added networks, and switches performing these functions are also health care clearinghouses.

While HIPAA applies to 'covered entities', senior individuals within those entities may be punished for non-compliance. A senior manager who is aware of a violation cannot avoid responsibility merely by avoiding active participation.

1.2 Compliance History

Main Points

- Colonial America was relatively free of government regulation, but the advent of big corporations prompted citizens and government to want and get constraints on corporations.
- The modern regulatory apparatus is extremely large, involves a complex participation of both public concern and business lobbying, and has moved from an emphasis on the product to an emphasis on how a corporation works internally.
- The ebb and flow of regulatory enthusiasm leads to changes as markedly reflected in the shifts from Carter to Reagan and then again from Clinton to Bush.

HIPAA is a federal law that calls for federal regulation of aspects of the healthcare enterprise. *Government regulation* of industry is not new to this country. Valuable lessons for HIPAA compliance can be gleaned from the history of compliance in America. Ultimately, what would be best for the country is a cooperative effort between government and industry rather than an adversarial one (Sigler and Murphy, 1988).

1.2.1 The Beginning

Beginning in *1764* the English government deliberately abandoned its policy of benign neglect towards the American colonists and imposed regulations. For instance, Americans needed to pay a stamp duty. The American Revolution led to a Constitution that encouraged free enterprise with minimal government intervention.

The *Industrial Revolution* shook the foundations of American society. In 1865 the typical American business concern was owned by an individual entrepreneur, a family, or a partnership. By 1900, giant corporations employed about 90% of all non-agricultural workers.

Most Americans were bewildered by the giant corporation. The *Grange*, a collection of farmers, pressed for state regulation of railroads and warehouses, hoping to improve their lot by controlling these economic forces. Purposive control of business in the name of the public good slowly became the American response to big business. In 1887 Congress created the Interstate Commerce Commission (ICC) to investigate railroad operations. At first, the ICC's powers were vague and compliance was left to the federal courts.

The *Sherman Anti-trust Act* of 1890 made illegal every contract that restrained free trade. The Act symbolizes (Cotter, 1960)

> the transition from a society in which government is regarded as the chief source of threats to individual freedom to one in which private economic power is recognized as an equal source of danger.

The balances among government, corporation, and individual are complex.

1.2.2 The Modern Regulatory System

In 1800, only *300 civil officials* were employed in the nation's capital. The State Department consisted of the Secretary of State, a chief clerk, seven lesser clerks, and a message boy. By the early 20th century, the federal government included numerous, massive administrative agencies.

Government regulation of business is partly a response to public opinion. However, government regulations typically require significant support of some businesses. The development of the *Pure Food and Drug Act* of 1906 illustrates this point. In 1883 Dr. Harvey Wiley, chief chemist of the U.S. Department of Agriculture, started a campaign against adulterated food. At the time, many basic foods were routinely mixed with additives and preservatives:

- Formaldehyde was used for preserving milk.
- Hydrochloric acid was added to apple jelly.
- Pork fat was mixed with butter.

Wiley attempted to persuade Congress to take action, but Congress would not listen. Wiley enlisted the support of the

- American Medical Association and
- Pharmaceutical Manufacturers Association.

How did Wiley manage to get these representatives of businesses to join his anti-business cause? They had *self-serving interests*:

- The Pharmaceutical Manufacturer Association provided crucial support because it would help eliminate competitors in the patent medicine business who were not members of the Association.
- The American Medical Association supported the measure to increase its monopoly on the treatment of disease.

While protection of the public is one result of the Food and Drug Act of 1906, the bill also disadvantaged certain businesses while helping others. (In addition to the general public, lawyers and information systems consultants stand to gain from HIPAA).

Concern for health and safety prompted much of the regulatory activity of the early twentieth century. However, the larger issue was how to constrain the growth of enormous corporations. President Theodore Roosevelt wanted the ICC to have greater power to constrain enormous corporations. Roosevelt expected the ICC to exercise quasi-legislative powers to determine rates and quasi-executive powers of investigation and enforcement. This 'extended ICC' was strange in 1905 but has become a model for the *administrative state*.

In 1913, Congress passed the *Federal Trade Commission* (FTC) Act. The FTC was given the power to issue restraining orders against 'unfair methods of competition'. The FTC Act stated a general ethical and economic principle and relied upon the course of administrative and judicial decisions to give it content. Since no one knew for sure what an 'unfair method of competition' was, only adversarial probing, investigation, and litigation could provide the meaning.

Since the late 1960's, new regulations have appeared that affect corporate *internal operations*. The Occupational Safety and Health Administration, for example, may specify precise engineering controls that must be adopted by all industries. These regulations reach inside the production process. Management decisions are even more affected by applying the standards for equal employment opportunity in hiring, firing, advancement, and discipline of employees.

The new social regulations have added costs and burdens to business without adding to their ability to pay for these costs. While the public enjoys a safer environment and fairer working conditions, the *costs* for these gains has been high. The consumer ultimately bears the price.

1.2.3 Ebb and Flow

The 1980 election brought *Ronald Reagan* to the White House and a different approach to regulation. Under the banner of deregulation, regulatory relief, or privatization, the regulatory agencies were reduced in their influence. In his first presidential news conference, Reagan declared a crusade against 'runaway government'. He froze 172 pending regulations that had been left him by outgoing President Jimmy Carter.

Reagan gave the *Office of Management and Budget* (OMB) primary supervisory responsibility over new regulations. OMB became an active agent for the reduction in number of proposed regulations, and a critic of customary approaches of regulatory agencies. For instance, OMB put pressure on the Environmental Protection Agency to make less stringent regulations to safeguard the environment. OMB questioned the scientific accuracy of EPA's reasoning and even the truthfulness of some of the EPA staff. OMB intervention, frequently in the name of cost-benefit analysis, blocked or altered many proposed regulations in a direction deemed acceptable to some major industrialists.

George Bush had served as Vice-President under Reagan, and when he became President, he continued the policies of Reagan. *Bill Clinton* was President from 1993-2001 and favored various forms of government regulation of business. In January 2001, George W. Bush became President and immediately froze Clinton recommendations, not unlike Reagan froze Carter's recommendations.

American politics swings between friendship and hostility towards business. Sometimes regulatory policy is too rigid and excessively costly. Sometimes it is too lax. A *balance* is needed that allows business to prosper and the public to be protected against business excess. Ideally, government promotes cooperation between government and business.

1.3 HIPAA History

Main Points

- The insurance industry agreed with President George Herbert Bush in 1991 that it could mend its own house and reduce overheads by standardizing transactions.
- The insurance industry failed to standardize, and government introduced standards for transactions and privacy.

1.3.1 Overhead Costs

In the 19th century, doctors took care of patients who paid for their services directly. Later insurance became the dominant mode by which doctors were paid. Different forms led to high administrative overheads. A medical assistant textbook written in 1980 said (Lindsey, 1980):

> Since the advent of medical and hospitalization insurance, the medical assistant has found a great deal of his or her time now spent billing various insurance companies so that the doctor's fees can be collected. .... While each company seems to have its own special form that will need to be completed in order to secure payment for services rendered, the basic information required on each is the same.

The American Medical Association approved a *universal claim form* in April of 1975. However, many insurance service organizations and government fiscal intermediaries did not adopt this AMA form.

The healthcare transaction standards were stimulated by the anxiety about rising healthcare costs in the 1980s. Political debates at that time said that the nation's multiplicity of private insurers contributed to high costs and uninsured poor people. One movement called for universal health coverage funded by industry, and another movement called for elimination of the insurance industry to be replaced with a government-based healthcare system. Those in favor of the government-based system noted the *administrative waste* in the insurance industry and provided the following data (Morrissey, 2000):

- Twelve cents of every premium dollar goes into overhead and profits for insurance companies.
- In the government-based healthcare system in Canada the insurance aspect of the operation only takes 1 cent on the dollar.

- The healthcare providers in the U.S. spend about 20% of total revenues for billing and administrative costs because of the complexity of dealing with hundreds of insurers.

In another estimate, administrative costs comprise 17 percent of total health expenditures (Dobson and Bergheiser, 1993). Whether 12, 17, or 20 per cent, such data highlighted healthcare's *paper-based*, arcane methods of handling insurance claims and led to efforts to examine the obstacles to automating the process.

1.3.2 Bush '89-'93

The 1991 Bush Administration called a group of healthcare industry leaders together to discuss how healthcare administrative costs could be reduced. The group was called the *Workgroup for Electronic Data Interchange (WEDI)*. WEDI was co-chaired by the President of Travelers Insurance Company and the President of the Blue Cross and Blue Shield Association and its membership was similarly a star-studded array of people largely from the American health insurance industry (Owens, 2000). The government asked WEDI to increase the number of claims moved electronically by at least 10% each year and to evaluate electronic claims standardized billing issues for the purpose of advancing electronic data interchange. WEDI was to solve the paper problem.

Also in 1991 the American National Standards Institute (ANSI) established a health insurance subcommittee to arrive at an industry consensus on billing standards. One goal of WEDI's charter was to encourage implementation of the to-be-developed ANSI *standards*.

WEDI was also asked to identify what role the federal government could play. In 1992 the position of WEDI was that the business reasons for moving to a paperless system were so compelling that legislation would not be necessary. The Chairman of the House Ways and Means Committee said that legislation was needed because he was skeptical that such a network could be developed voluntarily and because skyrocketing healthcare costs demanded quick action. WEDI said legislation would derail a promising opportunity for public-private partnership.

The federal government announced in 1992 that it would wait until 1994 for ANSI (a private sector operation) to produce usable standards. If no standards were developed by 1994, then the government would develop the standards. By 1993 ANSI had enough of the transaction standards in place that it discouraged any movement to have government take on the development.

Meanwhile, WEDI's reports on the issues of electronic health information became the foundation for many of the administrative simplification precepts that started making the rounds in Congress. The WEDI precepts became part of the reformation battle that followed President Clinton into office.

The private-public partnership that WEDI had promised was not materializing. The implementation of the standards was *sporadic* at best. Even leaders of the insurance standardization movement could not break from the vested interests and capital tied into the proprietary ways their organizations were exchanging information. No private insurer wanted to go first, but each said, "We'll follow." Case studies of individual successes in reducing costs by standardizing were not enough to convince others to be early adopters of the standards.

The reluctance to standardize held for the *healthcare providers*. Despite arguments that standards could help trim days in accounts receivable and ease the financial pinch, providers saw the project not as a potential benefit but as another burden they could not afford. Providers did not want to be early adopters of a new and capital-intensive effort.

Contrary to other players in the healthcare field, DHHS moved eagerly towards standardization of its operation. DHHS conversion to a standard remittance-advice transaction whetted its appetite for additional transactions.

1.3.3 Clinton '93-'01

In 1993 the Clinton administration included standardized transactions in its blueprint for healthcare reform. Three attempts to pass such legislation in 1993 failed. By 1994 Congress had grown so tired of healthcare reform that proposals about standardizing transactions were unacceptable.

Table “NPRM Dates”

Standard	**NPRM Published**
Transactions	5/07/1998
National Provider Identifier	5/07/1998
National Employer Identifier	6/16/1998
Security	8/12/1998
Privacy	11/3/1999
Privacy (again)	3/27/2002
Transactions (again)	5/31/2002

The new Congress in 1995 was receptive to standardizing electronic transactions in healthcare. The challenge now became to find a practical way to introduce the proposal into a specific piece of legislation. Political momentum was developing on the issue of portability of insurance. Bi-partisan legislation to make insurance more portable was given good odds of passage in *1996*.

The heightened prospects of passage of the electronic standards provisions brought sobering political observations about the risks of endorsing easier transmission of patient-identifiable medical details. Magazine articles and news items about breaches in confidentiality of medical records raised consciousness about who was looking at people’s data. Concerns from the Congress led to the inclusion of *security* and *privacy* provisions into the legislation. With extensive support from the insurance industry, the legislation known as HIPAA was finally passed.

The implementation schedule for administrative simplification was delayed. The portability regulations of HIPAA were politically important to have as a top priority. Thus DHHS focused first on portability. Instead of HIPAA providing an immediate jump-start to standardization, the HIPAA regulations on standardization became secondary to other issues of the time. DHHS had also to comply with the Balanced Budget Act of 1997, outpatient prospective payment systems, and the Y2K threat.

George W. Bush assumed the Presidency in January 2001 after a hotly contested election. His victory coincided with a many Republicans holding other elected offices. This administration favors minimizing government regulation of business.

1.3.4 Schedule

HIPAA requires extensive consultation with industry groups regarding what standards should be used. The government has made an impressive effort to comply with both the letter and spirit of those requirements. There have been numerous public hearings and briefings.

Finalized rules were to have been announced by February 1998, with compliance required by February 2000. The draft rules are first published as Notices of Proposed Rulemaking (NPRMs). The first four NPRMs were published in 1998 – a full *two years late* (see Table “NPRM Dates”). They were:

- Transactions and Code Sets,
- National Provider Identifier,
- National Employer Identifier, and
- Security.

The Privacy NPRM was published in 1999. Three further NPRMs are under development but have not yet been published for comment; they are:

- National Health Plan Identifier,
- Claims Attachments, and
- Enforcement.

Work on the National Individual Identifier has been indefinitely postponed.

The government was deluged with comments on the published NPRMs. Over 17,000 comments were received on the Transactions and Code Sets NPRM and over 50,000 on the Privacy NPRM prior to December 2000. DHHS evaluates those comments before producing final rules.

The Transaction and Code Sets Final Rule was published in the Federal Register on August 17, 2000. The Rule becomes effective 60 days after its appearance in the Federal Register. Compliance is required within 24 months of the effective date. However, small health plans are given an extra year to comply. To quote from the government web site (DHHS, 2000c):

> All health plans, all health care clearinghouses, and any health care provider that chooses to transmit any of the transactions in electronic form must comply within 24 months after the effective date of the final rule (small health plans have 36 months). ... Therefore, compliance with the final rule is required by October 2002 (October 2003 for small health plans).

However, Congress passed and the President signed the Administrative Simplification Compliance Act in December 2001 that allows covered entities to submit a plan for compliance by the original compliance deadline and thus earn an extension of 1-year till compliance with the transactions rule is required. In March 2002 a simple 2-page form was released by DHHS which was easy to complete and could be submitted either at the DHHS web site or via paper mail. Submission of the form automatically assured the entity of an extension.

Proposed modifications to the Transactions Rule were published in May 2002. The Final Employer Identifier Rule was also published in May 2002.

The Privacy Final Rule was released in December 2000. However, the Bush administration found a loophole in the rules that allowed it to delay the Rule (DHHS, 2001):

> We have determined that the report to the Congress required by 5 U.S.C. 801(a)(1) was not received, as previously thought, concurrent with the transmission of the Rule to the Federal Register. The required report was received by the Congress on February 13, 2001. Under 5 U.S.C. 801(a)(3)(A), the effective date of a major rule is, as pertinent here, ``the later of the date occurring 60 days after the date on which * * * the Congress receives the [required] report * * *, or * * * the rule is published in the Federal Register * * *". Thus, the published effective date, which was 60 days following the date of publication of the Rule in the Federal Register, is erroneous; rather, under 5 U.S.C. 801(a)(3)(A), the actual effective date of the Privacy Rule is 60 days after the receipt by the Congress of the final rule, or April 14. This final rule corrects the previously published effective date of the Privacy Rule accordingly.

Then the Secretary of DHHS announced a new comment period for March 2001. Many anticipated that the Administration would announce a delay in the effective date of the regulation. However, on April 12, 2001, President Bush said (Bush, 2001):

> Today, I directed [DHHS] Secretary Thompson to allow a federal rule that will protect the privacy of medical information for millions of Americans to become effective. …. I recognize that legitimate concerns have been raised about the current rule, which I share, such as parents' concern that the rule limits their right to have access to their children's medical records. I have asked Secretary Thompson to recommend appropriate modifications to the rule to address these concerns.

The effective date of the final Privacy Rule is 60 days after Congress was officially notified, which happened on Feb. 13, 2001. All healthcare entities other than small health plans have two years from April 14th, 2001 to be compliant with the Privacy Rule. Small health plans are granted an additional year to comply.

On August 14, 2002 modifications to the Privacy Rule were published in the Federal Register. These modifications consistently make compliance easier for covered entities and represent the efforts of the Bush administration to be sensitive to the needs of the health care industry. The compliance deadline was not modified.

HIPAA asks providers to implement new business and information system policies and procedures. The size and scope of the rules related to HIPAA could redefine how providers access, transmit, and disclose health data (Moynihan and McLure, 2000).

1.4 Health Industry Trends

Main Points

- Increasingly, the healthcare workforce is composed of aides who work in standardized, factory models more than in individualized cottages.
- The shrinking profit margins of providers lead them to resist HIPAA.
- Information systems are bringing the patient closer to the resources of the industry and suggesting standard ways of dealing with patient concerns.

The best way to predict the future is to know the past. The *trends* in personnel, administration, and information systems are next reviewed. These trends call for increased support of the healthcare enterprise by information systems that will require enlightened participation of an increasingly large portion of those people who participate in the healthcare process. Furthermore, these trends suggest the importance of processes such as those advocated by HIPAA.

This book repeatedly argues that the essence of HIPAA is not transactions or privacy per se but standardization, workflow management, and patient power. To improve communication, a common language needs to be agreed. Standards provide a common language. The concerns about privacy and security reflect a concern for how information is shared. For the *human organization* to deal with this concern, privacy and security are but a part of the broader concern for information and workflow.

1.4.1 Personnel

The 20th century has witnessed a dramatic growth in the number and types of *personnel* employed in the health care sector. The numbers have risen from about 0.5 million in 1910 to about 7.5 million in 1990. This growth has shown an increasing ratio of health personnel to the general population (see Table “Health Personnel over Time”).

	1910	1990
Employed in health sector	500,000	7,500,000
Total US population	93,000,000	250,000,000
1 health person covers how many people	1 health person per 186 people	1 health person per 33 people

Table “Health Personnel over Time”

More extraordinary than the increased supply of health personnel has been the variety of categories of personnel. The U.S. Department of Labor recognizes 400 different job titles in the health sector. Physicians constituted 30 percent of all health personnel in 1910 but 10 percent in 1990. Dentists and pharmacists have also fallen in numbers from about 10 percent of the health care workforce in 1910 to about 2 percent of the health care workforce in 1990. Registered nurses have risen in number from about 17 percent of the workforce in 1910 to 25 percent in 1990. What has been remarkable has been the growth in the categories of *allied health technicians*, technologists, aides, and assistants. They constituted 1 percent of the health workforce in 1910 and over half the health workforce in 1990 (Mick and Moscovice, 1993).

The concerns of physicians have played a role in the relatively slow diffusion of computerized patient records. While many observers have enumerated the failings of paper records, such records may have a number of positive features from the perspective of clinicians, including familiarity, portability, and considerable flexibility in recording data (Institute, 1997). Only recently has the computer interface approached the ease of using pencil and paper. Where supporters of automation see great potential in using computer-generated ‘reminders’ to prompt clinicians to ask patients certain questions or run particular tests, some clinicians may see this as ‘cookbook medicine’ that limits their *professional autonomy* (Dowling, 1987).

The healthcare industry is moving from a cottage industry in which the physician treats the patient in a solo-practice office towards integrated delivery networks. In these networks most roles are performed by non-physicians, and the coordination of this vast, specialized work force requires new ways of working that do not mesh well with the cottage industry ways. In particular, the needs are for

- standardization of information so that communication can be smooth from person to person and
- information and work flow that assure the patient that quality care is being delivered and that the patient information is private to the patient.

The trend is towards increasing numbers of allied health professionals dominating the work force, and this trend will support further the need for *standardized workflow*.

1.4.2 Administration

The healthcare delivery industry in the United States is highly fragmented and very complex. While science and medical technology continue to make significant breakthrough progress in dealing with human disease and injury, the management and clinical processes of these complex delivery organizations have made little progress in the past twenty years. Even today, the major clinical workflow depends on manual, paper-based medical record systems augmented by *spotty automation*. This has resulted in an industry that is economically inefficient and produces significant variances in medical outcomes. Medical error is one of the top ten causes of death in the United States (Kohn, et al, 2000). The industry must address these issues by identifying ways to enhance efficiencies and improve the quality of care.

Significant external forces have buffeted the healthcare industry. Managed care organizations have defined themselves as an intermediary in the flow of funds and exerted pressures on healthcare spending. These pressures resulted in lowering total spending on healthcare but did not necessarily address any of the larger, systemic issues in the industry. As a result of the pressures created by managed care, healthcare providers consolidated both horizontally and vertically into newly defined *delivery systems*. Many of these delivery systems were created to form entities to negotiate with managed care but many organizations also expected new economies of scale. For the most part these economies never materialized.

Federal *government policy* in the United States has also been an active force shaping the health care environment. The Balanced Budget Act reduced payments to healthcare providers by over $250 billion dollars over a five-year period. This legislation took its full grip on providers in the United States during 1999, significantly reducing the operating margins of hospitals and physician groups while raising their cost of capital.

Healthcare providers are feeling besieged. Government regulations without money to pay for the compliance with the regulations are resisted by the industry. However, neither the providers or the insurance companies are paying for healthcare; the patient or the government is ultimately paying the bill. The administration of healthcare tends not to face a concerted, financial view of the patient because of the complex process by which money goes from patients, employers, government, and insurance companies to the healthcare providers. The government regulations for 'Administrative Simplification' do not make clear to providers how the *cost* will be covered by the benefit.

1.4.3 Information Systems

Healthcare information systems are evolving to meet the needs of a changing marketplace. Beginning in the 1960's, computer systems developed for use in healthcare were financially oriented, with a focus on the ability to capture charges and generate patient bills and update the general ledger. Later, hospital and commercial organizations began to use clinical information systems, which automate the activities within clinical departments, such as laboratory, pharmacy, radiology and surgery departments, to improve the productivity of resources and automate the production and use of significant amounts of clinical information. During the late eighties and early nineties, individual clinical departments selected systems based upon specific features on a 'best of breed' basis resulting in disparate and disconnected information systems within the institution. There has been a shift from the purchase of disparate clinical systems selected on a 'best of breed' basis to systems that are able to *integrate* communication effectively throughout the healthcare enterprise. This approach requires a common model with standardized message formats.

In order to be competitive in the dynamic healthcare marketplace, healthcare enterprises should deploy information systems solutions that internally automate the paper-based medical record systems and externally create smart connections between the major participants in health care: the consumer, the physician, the hospital and the managed care organization. The Internet's role in the transformation of healthcare is not well defined at present, but indications are that it will be an enabler of a shift to a consumer-centric industry. As more households have Internet access, consumers have access to an increasing amount of health information, resulting in an informed and empowered healthcare *consumer*.

Consumers may have the option of working closely with their healthcare provider to organize and manage their care. Some software and services now support a patient record online that is largely maintained by the patient but also used by the physician and other health care professionals for entering certain information, like drug prescriptions. Since the patient has some *control* over and responsibility for the record, one might expect the record to be generally more complete and to contain fewer errors. The patient should also be able to retrieve information tailored to the patient's situation that the patient can browse and read in more leisurely fashion than when in the doctor's office. The patient would also have access to care guidelines and could actively participate in the management of treatments.

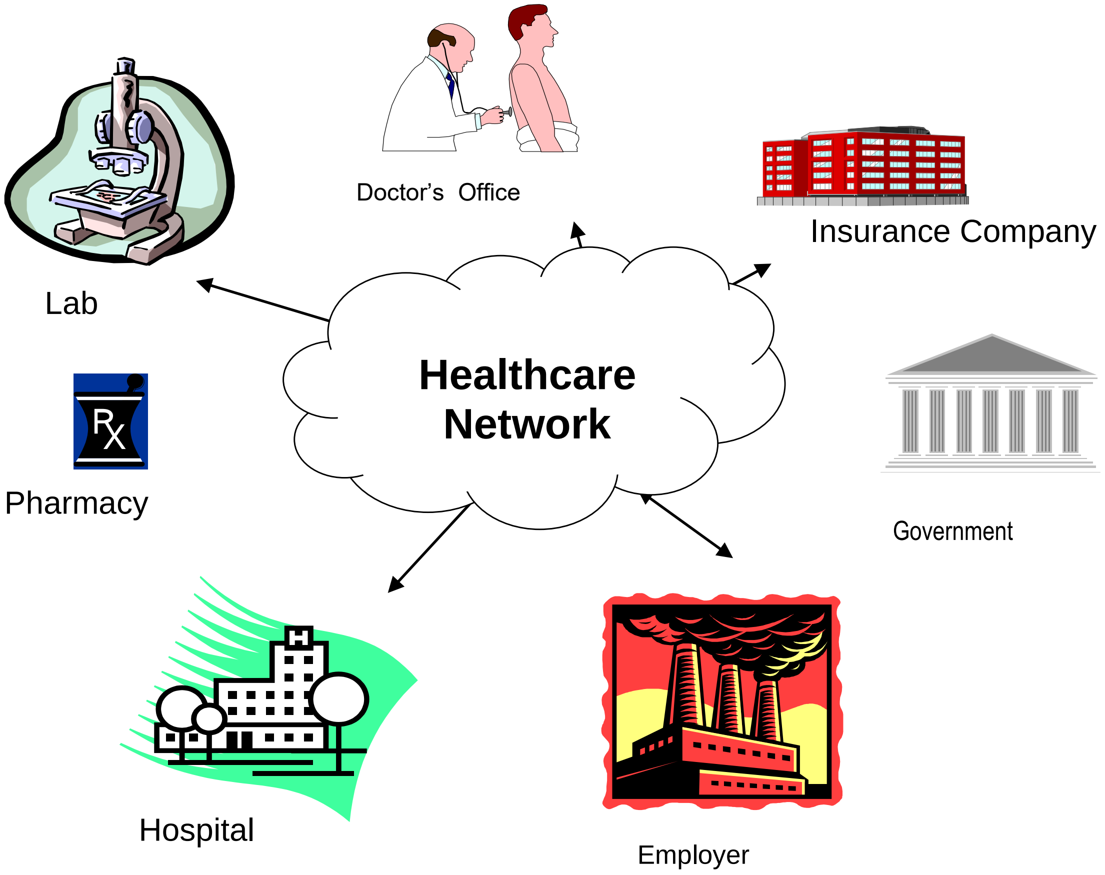
The *information systems trends* fit neatly into the reasons to have HIPAA's Administrative Simplification. These reasons, again, include:

- With increased connectivity across information system components, standardization of the transactions and codes contributes to efficiency and effectiveness.
- With increasing information flow and connectivity of patients, the value of ensuring patient privacy and access grows.

These trends are in support of 'Administrative Simplification'.

1.5 Review Questions

1. What are the 5 Titles within HIPAA and how do they relate to the acronym HIPAA?
2. Summarize the history of insurance legislation in the United States in terms of state versus federal involvement.
3. What is the relationship between fraud and the first 'A' in HIPAA?
4. How did the rise of the big corporation correspond to the rise of government regulation of business?
5. Describe the AMA role in the Pure Food and Drug Act of 1906?
6. How does the transition from Presidents Carter to Reagan demonstrate how government regulation changes?
7. What was WEDI's role in HIPAA?
8. Why did 'Administrative Simplification' get placed in HIPAA?
9. When is the Federal Register important in the distribution of regulations? What 'administrative simplification' announcements have already appeared in the Federal Register?
10. What does the history of the legislation and regulation suggest about future legislation and regulation?
11. How does the financial situation of providers relate to the resistance to the new regulations?



2 Transactions and Codes

Target

Learning Objectives

- Construct a sketch of an X12 message based on Implementation Guide details and certain data content.
- Describe different code sets and issues relevant to mapping terms from one code set to terms in another code set.
- Distinguish 'identifiers' from 'code sets' and illustrate the complexities of creating a neutral identifier but a rich associated file.
- Estimate the cost-to-benefit relationships for different entity types over time as a result of complying with the transactions regulation.
- Design an implementation plan for an entity to achieve compliance.

Main Points

- Numerous 'standards' exist in healthcare information systems, and DHHS has systematically chosen a few to make mandatory.
- Transaction standards specify the format.
- Code sets and identifiers specify the content.
- The impact of this standardization should be a reduction in the administrative overhead of healthcare.
- Implementation specifics reveal the complexity of a national switch to a standard language for provider-payer transactions.

The first HIPAA Administrative Simplification rule finalized was the 'Transactions Rule'. Transactions go between provider and payer. The Rule specifies the format of transactions and the codes that will fill the fields in the forms.

2.1 Legislation

Main Points

- The legislation requires transaction standards for the most important provider-payer transactions.
- The legislation applies to providers, clearinghouses, and health plans.

The government rules about which standards to use in transactions were developed in response to legislative mandate.

2.1.1 Standards Required

HIPAA requires DHHS to adopt standards to facilitate Electronic Data Interchange (EDI). HIPAA requires that DHHS (DHHS, 1998) adopt standards for financial and administrative transactions, and data elements for those transactions. Standards are required for the following transactions:

- health claims,
- health encounter information,
- health claims attachments,
- health plan enrollments and dis-enrollments,
- health plan eligibility,
- healthcare payment and remittance advice,
- health plan premium payments,
- first report of injury,
- health claim status, and
- referral certification and authorization.

In addition, DHHS is required to adopt standards for any other financial and administrative transactions that DHHS deems appropriate.

Standards must be adopted for

- unique health identifiers for all individuals, employers, health plans, and healthcare providers,
- code sets for each data element for each healthcare transaction, and
- transmission of data elements needed for the coordination of benefits and sequential processing of claims.

If an entity desires to conduct a transaction with a health plan as a standard transaction, the following apply:

- The health plan may not refuse to conduct the transaction as a standard transaction.
- The health plan may not delay the transaction or otherwise adversely affect the entity or the transaction on the ground that the transaction is a standard transaction.
- The information transmitted and received in connection with the transaction must be in the form of standard data elements of health information.

In other words, the health plan must fully comply.

Entities must comply with the standard within 24 months (or 36 months for small health plans) of its adoption. An entity may comply by using a healthcare clearinghouse to transmit or receive the standard transactions. Compliance with modifications to standards must be accomplished by a date designated by DHHS.

Modifications to any of these standards may be made after the first year, but not more frequently than once every 12 months. DHHS must also ensure that procedures exist for the routine maintenance, testing, enhancement, and expansion of code sets and that there are crosswalks from prior versions.

HIPAA establishes a civil monetary penalty for violation of the administrative simplification provisions. Penalties may not be more than $100 per person per violation and not more than $25,000 per person per violation of a single standard for a calendar year.

2.1.2 Applicability

HIPAA’s transaction standards apply broadly. They apply to all health plans, all healthcare clearinghouses, and any healthcare providers that transmit any health information in electronic form in connection with HIPAA transactions. Electronic transmissions would include transmissions using all media, even when the transmission is physically moved from one location to another using magnetic tape, disk, or CD media. Transmissions over the Internet (wide-open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, and private networks are all included.

Interactions between server and browser, direct data entry, and fax back transmissions must comply with the data content, but not with the data format. For example, with ‘dumb’ terminals, where the provider directly keys data into a health plan's computer, the format need not comply with the standard, but the data elements or content must comply. A health plan may not offer an incentive for a healthcare provider to conduct a transaction under the *direct data entry exception*.

Healthcare clearinghouses are an exception. A clearinghouse would be able to accept *nonstandard transactions* for the sole purpose of translating them into standard transactions and would be able to accept standard transactions and translate them into nonstandard formats for receiving customers. The transmission of nonstandard transactions, under contract, between a health plan or a healthcare provider and a healthcare clearinghouse would not violate the law.

The fundamental policy is that covered entities must use a standard transaction inside or outside the entity when transmitting a transaction electronically. For example, a hospital that is wholly owned by a managed care company has to use the standards to pass encounter information back to the home office. DHHS decided not to create an exception for standard transactions within a *corporate entity* (DHHS, 2000b). DHHS was not able to define 'corporate entity' so that the exception would not defeat the rule. The rapid pace of mergers, acquisitions, and dissolutions in the corporate healthcare world would make such an exception extremely difficult to implement.

2.2 Standards

Main Points

- Standards may de jure or de facto but are important to the extent that they are used.
- Numerous organizations develop standards for healthcare information, and some receive special endorsement for their open process.
- The Department of Health and Human Services has defined criteria for a good standard and measured candidate standards against these criteria.
- The transaction standards apply to entities engaged in electronic exchange of provider-payer information.

The provisions of HIPAA have come to dominate the healthcare data standards development process. The Transactions Rule is intimately related to a large body of standards activity in the technical realm for information exchange in healthcare. What organizations have been active in such standardization and what are the characteristics of good, technical standards?

2.2.1 Definition

A standard is defined as

> something established by authority, custom, or general consent as a model or example.

When used as an adjective, the definition of 'standard' includes (Amatayakul, 2000)

> conforming to a standard as established by law or custom [which is] sound and usable.

Standards arise either from official standards activity or arise by the force of practice. An official standard is a de jure standard, while those which arise by practice are de facto standards. For instance, the Open Systems Interconnection (OSI) standards of the International Organization of Standards are de jure standards, while Microsoft Office is a de facto standard (Rada et al, 1994).

Practically speaking a standard is simply what people use. Microsoft Office is a standard because many people use it and not because it was created by a formal standards development organization.

The most important aim of standardization is to produce standards which are wanted and used. Additionally, a de jure standard should be impartial in the sense that it should not give exclusive advantage to the product or service of any individual supplier. A standard is cost-effective when the effort to make and gain compliance with the standard costs less than the benefit. In areas of rapid development, the balance must be struck between inhibiting innovation by standardizing too soon and proliferating wasteful or mutually incompatible solutions by leaving standardization until too late.

Progress has been made in the development of messaging or data exchange standards (see Figure "Messages"). Standards exist for exchanging clinical data (Health Level Seven), images (DICOM), clinical observations (ASTM), bedside instrument data (IEEE), prescription data, and administrative data associated with claims (X12).

Interoperability refers to the ability of one computer system to exchange data with another computer system. Three levels of interoperability are (NCVHS, 2000):

- *Basic interoperability* allows a message from one computer to be received by another but does not expect the information to be interpreted.
- *Functional interoperability* is an intermediate level that defines the syntax of messages. This ensures that messages can be interpreted at the level of data fields. For example, when one computer has a field for 'Ear Exam', that computer should be able to pass data to another computer and have it appropriately stored in a comparable field for 'Ear Exam'. Neither system, however, understands the meaning of the 'Ear Exam'.
- *Semantic interoperability* requires that the information can be used in an intelligent manner and takes advantage of both the structuring of the message and the codification of the data within the fields. Thus the 'Ear Exam' may have an attribute of 'Inflammation' with a value of 'positive' and this could trigger reactions in the receiving computer.

For optimal value, standards for semantic interoperability are needed.

Typically, standards are produced in large numbers, and entities pick or choose which ones to follow. Standards are only important when organizations adhere to them. A standard becomes binding when compliance is *mandatory* by legislation or when a party is contracted to work to it (Rada, 1993). Governments currently make some standards important by insisting on purchasing only products or services consistent with a certain standard. A yet more absolute way to make a standard important is for the government to mandate that organizations comply with the standard. The Transaction Rule is powerful because the government has mandated that healthcare organizations comply with the standards indicated in the Rule.

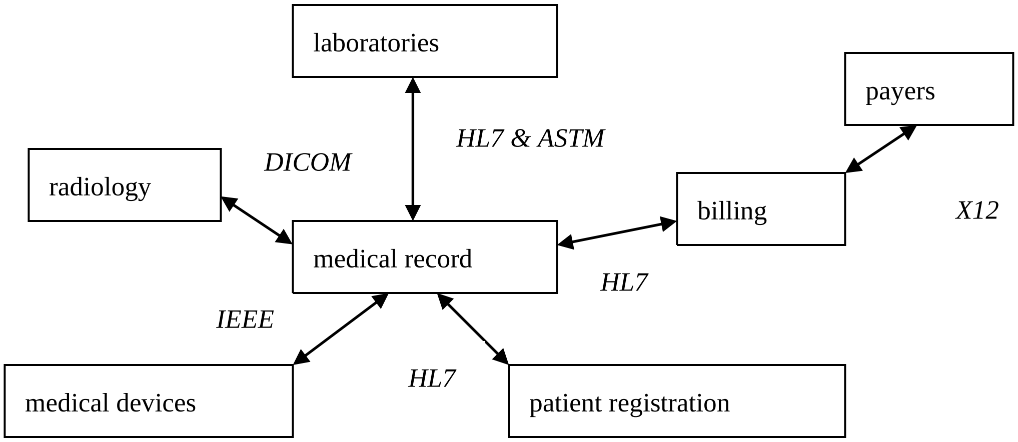


Figure "Messages": Medical record in center connected to other activities via messaging. The square boxes are the activities. The arrows indicate the flow of messages. The italicized term refers to the standard organization that has a standard relevant to that message or transaction.

2.2.2 Standards Organizations

A standards development organization is any organization that develops standards. However, the term 'standards development organization' is typically used to refer to an organization that has been recognized by some authority for its process. The process should be open to the public and should not only develop the standard but also maintain it over time.

The American National Standards Institute (ANSI) is a private, non-profit standards organization. ANSI coordinates formal voluntary consensus standards activities in the United States and approves American National Standards. Members of ANSI include over 1,000 companies, 30 government agencies, and over 250 professional, trade, and consumer organizations. The organization ensures that a single set of non-conflicting American National Standards are developed by ANSI-accredited standards development organizations and that all interests concerned have the opportunity to participate in the development process. All ANSI approved standards also must undergo regular review and revision. The ANSI *Healthcare Informatics Standards Board (HISB)* was created within ANSI to help coordinate and promote adoption of standards relating to healthcare information system applications. HISB focuses on encouraging communication among existing standards development organizations in the healthcare domain. HIPAA requires DHHS to adopt standards that have been developed by an ANSI-accredited standards development organization wherever possible.

The *American Society for Testing and Materials (ASTM)* is an ANSI-accredited standards development organization and has been developing standards since 1898. ASTM began doing healthcare informatics standards in the 1960s. ASTM's first healthcare standards addressed laboratory message exchange, properties for electronic health record systems, and health information security. *Health Level Seven (HL7)* is an ANSI-accredited standards development organization and in 1987 developed its first in a wide range of message format standards for patient registration, orders, and observations reporting.

Some healthcare standards organizations are not ANSI-accredited. The development of standards in the healthcare arena has not typically relied as extensively on formal standards development organizations as have some other industries. Initially, a clinical specialty group or professional association would identify a need for a standard in a specific area. The *College of American Pathologists* started developing a nomenclature of pathology in 1965. The College of American Pathologists first became an ANSI-accredited standards development organization in February 2000. In 1974, DHHS (which is not an ANSI-accredited standards development organization) promulgated the first Uniform Hospital Discharge Data Set. The American Medical Association's 'Current Procedures and Terminology' is a standard code set of medical procedures and is an example of a standard developed by a professional society that is not ANSI-accredited.

In an unusual approach to developing a medical standard that had both strong practitioner input and was associated with an ANSI-accredited standards development organization, the American College of Radiology (ACR) and the National Electrical Manufacturers Association (NEMA) collaborate. ACR is not ANSI-accredited but NEMA is. ACR-NEMA identified a need in 1985 for standards for communicating biomedical images and created what is now called the 'Digital Imaging and Communications in Medicine' (better known as DICOM) standard.

The *National Council for Prescription Drug Programs (NCPDP)* first started developing standards in 1977 with the development of the Universal Claim Form (www.ncpdp.org). NCPDP's Telecommunication Standard is used to process over 1 billion claims per year. NCPDP achieved ANSI accreditation status in 1996.

Other standards development organizations are active in the healthcare arena of which the most prominent one to be discussed in detail elsewhere is X12. HIPAA contains requirements concerning standard setting, as follows:

- DHHS may adopt an existing standard from a standard setting organization that has consulted with the National Uniform Billing Committee, the National Uniform Claim Committee, WEDI, and the American Dental Association.
- DHHS may also adopt a standard other than one established by a standard setting organization, if the different standard will reduce costs for healthcare providers and health plans, the different standard is promulgated through negotiated rulemaking procedures, and DHHS consults with each of the above-named groups.
- If no standard has been adopted by any standard setting organization, DHHS is to rely on the recommendations of the National Committee on Vital and Health Statistics (NCVHS) and consult with the above-named groups.

DHHS must rely on the recommendations of the NCVHS, consult with appropriate State, Federal, and private agencies or organizations, and publish the recommendations in the Federal Register.

2.2.3 Standards Development

The HIPAA implementation strategy assures coordination among DHHS agencies. Particular responsibilities within DHHS fall to the DHHS Data Council and Implementation Teams. The *DHHS Data Council* is the Department's senior internal data policy body and oversees implementation of Administrative Simplification. The Council consists of representatives from each major operating and staff division within DHHS. The Implementation Teams focus on the detail work and are composed of various DHSS staff.

Principles guide choices for the standards. These principles are based on direct specifications in HIPAA and principles that are consistent with the regulatory philosophy. To be designated as a HIPAA standard, each standard should (DHHS, 1998b):

1. Improve the efficiency and effectiveness of the healthcare system.
2. Meet the needs of healthcare providers, health plans, and healthcare clearinghouses.
3. Be consistent and uniform with the other HIPAA standards -- their data element definitions and codes and their privacy and security requirements -- and, secondarily, with other private and public sector health data standards.
4. Have low additional development and implementation costs relative to the benefits of using the standard.
5. Be supported by ANSI-accredited standards developing organization or other private or public organization that will ensure continuity and efficient updating of the standard over time.
6. Have timely development, testing, implementation, and updating procedures.
7. Be technologically independent of the computer platforms and transmission protocols used in electronic transactions, except when they are explicitly part of the standard.
8. Be precise and unambiguous, but as simple as possible.
9. Keep data collection and paperwork burdens on users as low as is feasible.
10. Incorporate flexibility to adapt to changes in the healthcare infrastructure and information technology.
11. Support patient privacy and information quality (NCVHS, 2000).

To encourage innovation and promote development, DHHS allows an organization to request a revision or replacement to any adopted standard. An organization could request a revision or replacement to an adopted standard by requesting a *waiver* from DHHS to test a revised or new standard. The organization would be required, at a minimum, to demonstrate that the revised or new standard offers a clear improvement over the adopted standard.

2.2.4 Review Questions

1. What does HIPAA specify be developed as regards transaction standards?
2. What is the difference between a de jure and a de facto standard?
3. What organizations have contributed most to the development of healthcare information standards?
4. What are the DHHS criteria for a good standard?
5. Under what circumstances do the transaction standards apply to an organization?
6. In the typical information systems activity, the American government emphasizes standards produced by ANSI-accredited standards development organizations. CPT is not such a case. Most scholarly works on standards would accept as axiomatic that a good standard development process was one that was open in the sense that any interested party had an opportunity to contribute to the development of the standard. Why is this criterion not mentioned in the DHHS list of criteria for a good standards development process? (Project Question)

2.3 Transactions

Main Points

- Claims and EDI histories show the move to standardization.
- The government has chosen the standards organization X12 and NCPDP to develop and maintain the transaction formats.
- X12 has already electronic data interchange standards that specify how an envelope should be put around a message and how the content should be structured in the message. Implementation guides have been prepared that say how these standards should be used for healthcare transactions between providers and payers.
- The technical details of the implementation guides occupy thousands of pages of details about records, fields, and values for fields.
- The handful of transactions now standardized includes eligibility and claims transactions.
- Software exists to help providers generate claims.
- The experiences of the major vendors point to the challenges of converting from the existing way of working to a new (albeit standardized) way.

In his book *Business @ the Speed of Thought*, Bill Gates (1999) says,

> The successful companies of the next decade will be the ones that use digital tools to reinvent the way they work. These companies will make decisions quickly, act efficiently, and directly touch their customers in positive ways.

Patient financial services leaders can help their organizations achieve these performance levels by spearheading the redesign of their organizations' revenue-cycle-processing, organizational, and customer-service models to conform to the HIPAA-mandated *transaction standards*.

2.3.1 Background

The history of insurance claims and of Electronic Date Interchange lead to transaction standards.

2.3.1.1 Claims History

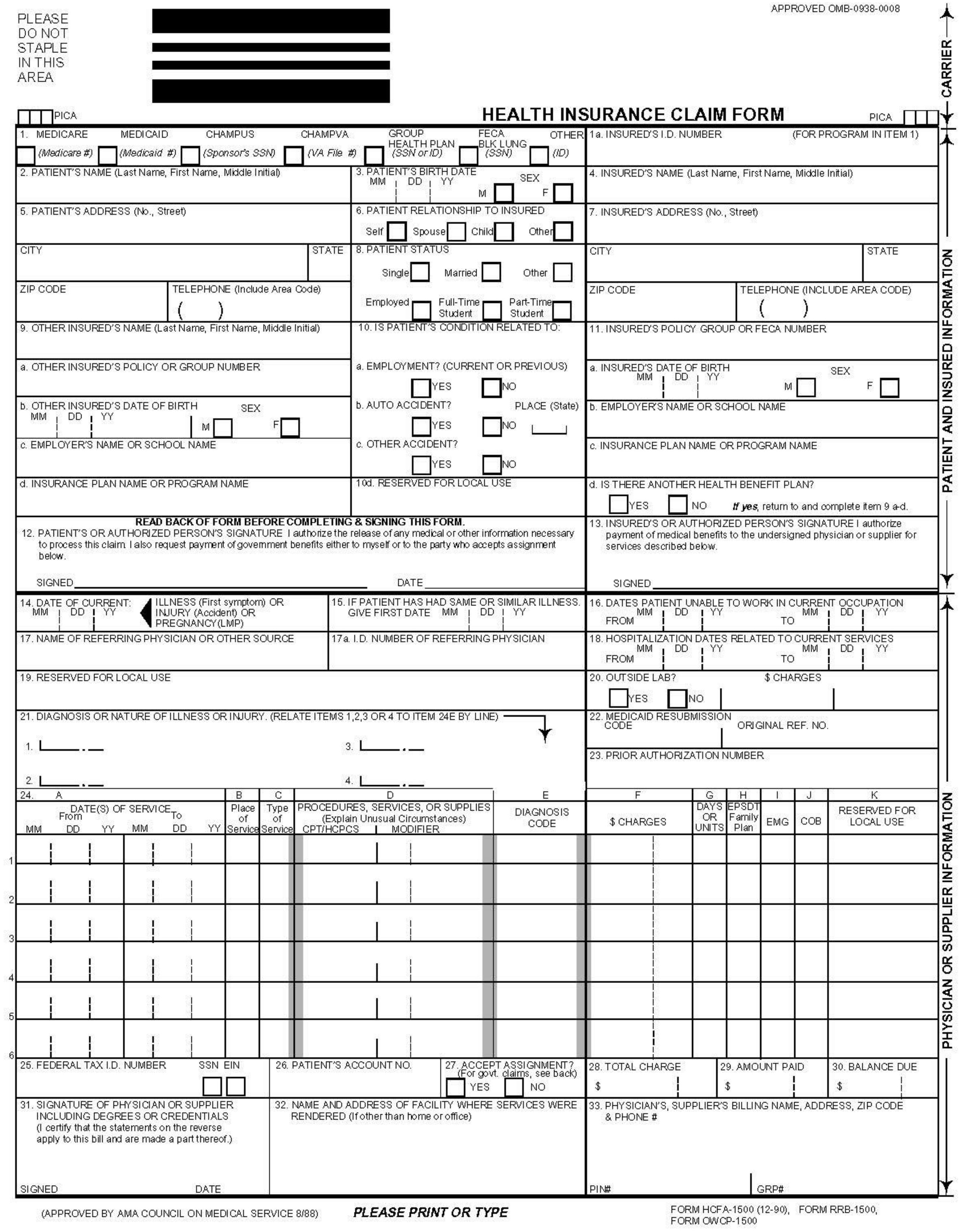
In 1958, the Health Insurance Association of America (HIAA) and the American Medical Association (AMA) attempted to standardize the insurance claim form. However, third-party payers did not universally accept this form, and as the types of coverage become more variable, new claims forms, requiring more information, were developed. In April,1975, the AMA approved a "Universal Claim Form" called Health Insurance Claim Form or HCFA-1500. It could be used for both group and individual claims. HCFA-1500 answered the needs of many health insurers who were processing claims manually.

In 1990, the HCFA-1500 was revised and printed in red ink to support optical scanning of claims by insurance carriers. Beginning in May 1992, all services for Medicare patients from physicians had to be billed on the scanable HCFA-1500 form. The revised form was adopted by the Office of Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) and received approval from the AMA Council on Medical Services. HIAA endorses and recommends that their members, private insurance companies, accept the form. In some states, it is even used to process claims for Medicaid and workers' compensation. The Medicare hospital claim form (called the UB-92) is used by most hospitals and nursing facilities for inpatient and outpatient claims but is customized so extensively by many plans and healthcare providers that it does not function as an EDI standard.

The HCFA-1500 form is divided into two sections (see Figure “HCFA-1500”):

- Patient and Insured Information and
- Physician or Supplier Information.

The ‘Patient and Insured Section’ contains eleven fields for information and two fields for signatures. The ‘Physician or Supplier Section’ consists of nineteen spaces for information, and one space for the physician’s signature.



PLEASE
DO NOT
STAPLE
IN THIS
AREA

APPROVED OMB-0938-0008

CARRIER

□□□ PICA

HEALTH INSURANCE CLAIM FORM

PICA □□□

1. MEDICARE □ *(Medicare #)* MEDICAID □ *(Medicaid #)* CHAMPUS □ *(Sponsor's SSN)* CHAMPVA □ *(VA File #)* GROUP HEALTH PLAN □ *(SSN or ID)* FECA BLK LUNG □ *(SSN)* OTHER □ *(ID)*

1a. INSURED'S I.D. NUMBER (FOR PROGRAM IN ITEM 1)

2. PATIENT'S NAME (Last Name, First Name, Middle Initial)

3. PATIENT'S BIRTH DATE MM | DD | YY SEX M □ F □

4. INSURED'S NAME (Last Name, First Name, Middle Initial)

5. PATIENT'S ADDRESS (No., Street)

6. PATIENT RELATIONSHIP TO INSURED Self □ Spouse □ Child □ Other □

7. INSURED'S ADDRESS (No., Street)

CITY STATE

8. PATIENT STATUS Single □ Married □ Other □
Employed □ Full-Time Student □ Part-Time Student □

CITY STATE

ZIP CODE TELEPHONE (Include Area Code) (   )

ZIP CODE TELEPHONE (INCLUDE AREA CODE) (   )

9. OTHER INSURED'S NAME (Last Name, First Name, Middle Initial)

10. IS PATIENT'S CONDITION RELATED TO:

11. INSURED'S POLICY GROUP OR FECA NUMBER

a. OTHER INSURED'S POLICY OR GROUP NUMBER

a. EMPLOYMENT? (CURRENT OR PREVIOUS) □ YES □ NO

a. INSURED'S DATE OF BIRTH MM | DD | YY SEX M □ F □

b. OTHER INSURED'S DATE OF BIRTH MM | DD | YY SEX M □ F □

b. AUTO ACCIDENT? □ YES □ NO PLACE (State)

b. EMPLOYER'S NAME OR SCHOOL NAME

c. EMPLOYER'S NAME OR SCHOOL NAME

c. OTHER ACCIDENT? □ YES □ NO

c. INSURANCE PLAN NAME OR PROGRAM NAME

d. INSURANCE PLAN NAME OR PROGRAM NAME

10d. RESERVED FOR LOCAL USE

d. IS THERE ANOTHER HEALTH BENEFIT PLAN? □ YES □ NO ***If yes***, return to and complete item 9 a-d.

READ BACK OF FORM BEFORE COMPLETING & SIGNING THIS FORM.

12. PATIENT'S OR AUTHORIZED PERSON'S SIGNATURE I authorize the release of any medical or other information necessary to process this claim. I also request payment of government benefits either to myself or to the party who accepts assignment below.

SIGNED ______________________ DATE ____________

13. INSURED'S OR AUTHORIZED PERSON'S SIGNATURE I authorize payment of medical benefits to the undersigned physician or supplier for services described below.

SIGNED ______________________

PATIENT AND INSURED INFORMATION

14. DATE OF CURRENT: MM | DD | YY ◀ ILLNESS (First symptom) OR INJURY (Accident) OR PREGNANCY(LMP)

15. IF PATIENT HAS HAD SAME OR SIMILAR ILLNESS. GIVE FIRST DATE MM | DD | YY

16. DATES PATIENT UNABLE TO WORK IN CURRENT OCCUPATION FROM MM | DD | YY TO MM | DD | YY

17. NAME OF REFERRING PHYSICIAN OR OTHER SOURCE

17a. I.D. NUMBER OF REFERRING PHYSICIAN

18. HOSPITALIZATION DATES RELATED TO CURRENT SERVICES FROM MM | DD | YY TO MM | DD | YY

19. RESERVED FOR LOCAL USE

20. OUTSIDE LAB? □ YES □ NO $ CHARGES

21. DIAGNOSIS OR NATURE OF ILLNESS OR INJURY. (RELATE ITEMS 1,2,3 OR 4 TO ITEM 24E BY LINE)

1. ___ . __
2. ___ . __
3. ___ . __
4. ___ . __

22. MEDICAID RESUBMISSION CODE ORIGINAL REF. NO.

23. PRIOR AUTHORIZATION NUMBER

24. A						B	C	D		E	F	G	H	I	J	K
DATE(S) OF SERVICE From			To			Place of Service	Type of Service	PROCEDURES, SERVICES, OR SUPPLIES (Explain Unusual Circumstances)		DIAGNOSIS CODE	$ CHARGES	DAYS OR UNITS	EPSDT Family Plan	EMG	COB	RESERVED FOR LOCAL USE
MM	DD	YY	MM	DD	YY			CPT/HCPCS	MODIFIER							
1																
2																
3																
4																
5																
6																

25. FEDERAL TAX I.D. NUMBER SSN EIN □□

26. PATIENT'S ACCOUNT NO.

27. ACCEPT ASSIGNMENT? (For govt. claims, see back) □ YES □ NO

28. TOTAL CHARGE $

29. AMOUNT PAID $

30. BALANCE DUE $

31. SIGNATURE OF PHYSICIAN OR SUPPLIER INCLUDING DEGREES OR CREDENTIALS (I certify that the statements on the reverse apply to this bill and are made a part thereof.)

SIGNED DATE

32. NAME AND ADDRESS OF FACILITY WHERE SERVICES WERE RENDERED (If other than home or office)

33. PHYSICIAN'S, SUPPLIER'S BILLING NAME, ADDRESS, ZIP CODE & PHONE #

PIN# GRP#

PHYSICIAN OR SUPPLIER INFORMATION

(APPROVED BY AMA COUNCIL ON MEDICAL SERVICE 8/88) ***PLEASE PRINT OR TYPE***

FORM HCFA-1500 (12-90), FORM RRB-1500,
FORM OWCP-1500

Figure "HCFA 1500”: This is the claims form widely used in healthcare as of 2001.

2.3.1.2 EDI History

Early electronic interchanges were based on *proprietary formats* agreed between two trading partners. In the 1960's a cooperative effort between industry groups produced a first attempt at common, electronic, data formats. The formats, however, were only for purchasing, transportation, and finance data, and were used primarily for intra-industry transactions. Not until the late 1970's did work begin for national Electronic Data Interchange (EDI) standards. Both users and vendors input their requirements to create a set of standard data formats that:

- were hardware independent;
- were unambiguous and could be used by all trading partners;
- reduced the labor-intensive tasks of exchanging data, such as data re-entry; and
- allowed the sender of the data to control the exchange, including knowing if and when the recipient received the transaction.

In 1979, the American National Standards Institute chartered the Accredited Standards Committee X12 to develop uniform standards for inter-industry electronic interchange of business transactions. *Accredited Standards Committee X12* (or simply X12) develops, maintains, interprets, publishes and promotes the proper use of American National and EDIFACT (EDI For Administration Commerce and Trade) Standards. *EDIFACT* is the international standard for electronic interchange formats sponsored by the United Nations. X12 originally had its own formats that differed from the formats of EDIFACT, but since the early 1990s X12 has agreed to align its work with that of EDIFACT. The X12 and EDIFACT standards are mandated for use within the Federal Government (Garguilo and Markovitz, 1996).

HIPAA also specifically mentions the *National Council for Prescription Drug Programs (NCPDP)* as a developer of standards for information transactions. Transactions between pharmacies and health plans are typically done in a NCPDP standard, while transactions between all other providers and plans are done with X12 standards.

The DHHS transaction final rules say:

- For ‘Healthcare Eligibility Benefit Inquiry and Response’ and for ‘Healthcare Payment and Remittance Advice’ the standard transaction for retail pharmacy drugs is the NCPDP Telecommunications Standard for ‘Eligibility Verification and Response, and Enrollment’.
- For ‘Healthcare Claims or Equivalent Encounter Information’ and for ‘Healthcare Claims for Coordination of Benefits’ the standard transaction for retail pharmacy drugs is the NCPDP Telecommunications Standard Format for Retail Pharmacy Drug Claims.

For other transactions with plans, pharmacies might use X12 formats.

2.3.1.3 Software

Software can help providers generate claims. In fact, billing has been the first item to be computerized in American healthcare (Lindberg, 1979). Several efforts to provide such support are described next. First is the case of financial management system, then a traditional, mid-sized third-party claims processor, and finally a regional EDI network.

The product Business1 (Per-Se, 2001) supports providers in creating bills. Business1 is a patient financial management system that supports traditional patient accounting, contract management, and professional billing. Business1

- gives users access to various aspects of the patient demographic, insurance and other information.
- uses a rules engine to help ensure that all required information is collected for efficient closure of the revenue cycle.

Each provider can mark certain fields as "required fields" to comply with provider admission policies and payer requirements. With color-coded alerts, users can identify and locate pages that are incomplete. These up-front edits ensure that the payer's billing requirements are met.

The Accounting Viewer provides a summary of receivables for the patient and guarantor across the entire Integrated Delivery Network. The viewer contains information about both the receivables and the episode from which the receivables were generated (see Figure “Accounting Viewer”). As payer contract provisions become increasingly more complex, the billing clerk must have an understanding of how provider cases are consolidated or split into the products from which invoices are generated. Business1 also creates a single patient statement describing all the services rendered across the provider network.

National Claims Administrator Services (NCAS) provides claims processing and administrative services for about 80 self-funded employers headquartered in Mid-Atlantic states, covering about 50,000 lives. Like many third-party administrators, NCAS scans in paper claims. NCAS uses scanning products from Insurdata, a Texas software development company that also offers third party services, to convert the paper forms to electronic

Guarantors	Invoice ID	Provider	Payer Name	Total Charges	Amount Received
John Smith	HH0089	SEMB	Mut. Ohio	14,823.00	7,588.13
	Line Items				
	Item	Rev. Code	Description	Units	Charge
	1	128	Room-Board	5	2,138.80
	2	210	Coronary Care	5	4,170.00

Figure "Accounting Viewer": This schematic of a screen from the Per-Se Business1 software shows the 'accounting viewer'. In this screen a number of products have been identified and billed.

data, saving time and reducing keystroke errors (Cupito, 1998). However some forms have information that computers cannot properly interpret due to poor handwriting or crowded forms, and then data entry clerks must key in the data. For those manual data entry purposes, the clerk views the scanned form on one side of a split screen and types into the system on the other side of the screen.

In addition to its paper scanning operations, NCAS participates in fully online processing. NCAS is working with Insurdata for fully automatic data processing for one of the major Preferred Provider Organizations that NCAS services. Claims are submitted by providers to the Preferred Provider Organization, which determines its allowances, and sends them electronically to Envoy Corporation, a claims clearinghouse. Envoy sends the claims electronically to Insurdata's bulletin board. NCAS has an online connection to Insurdata's bulletin board and reviews the claims online at Insurdata. After NCAS's review, Insurdata issues paper checks and mails them. Interestingly these three companies, NCAS, Insurdata, and Envoy are geographically remote from one another with NCAS being in Virginia, Insurdata in Texas, and Envoy in Tennessee. However, online they work as though shoulder-to-shoulder. Being able to process claims electronically is a competitive advantage that a company the size of NCAS typically would not have otherwise. Insurdata allows payment on a per-transaction basis, avoiding large, up-front expenditures that NCAS would have to make in order to perform such electronic work on its own.

A group of providers and payers in New England has started its own network using standard electronic formats for sharing information. The *New England Healthcare EDI Network* includes three hospital systems, Partners HealthCare System and CareGroup Healthcare System, Boston; Lifespan, Providence, R.I.; and two insurers, Harvard Pilgrim Healthcare, Quincy, Mass.; and Tufts Health Plan, Waltham, Mass. The systems have most of their hospitals and affiliated doctors' offices connected to the network as well. The participants use *EDI standards* that all accept. So far the network is being used primarily for insurance eligibility transactions, which are settled in seconds. The system has been successful because the three competing care providers have agreed that such standardization of payer information is mutually beneficial (HHN, 2000).

2.3.2 X12

The X12 provider-payer transactions are described next from three views:

- the administration of X12,
- the technical details of how the X12 implementation guides direct a healthcare entity to create a transaction, and
- software systems to support X12 transactions.

2.3.2.1 X12 Administration

Subcommittees in X12 perform technical work. The largest subcommittee in X12 is the Insurance Subcommittee, also called X12N. The principle responsibilities of the X12N Insurance Subcommittee are development and maintenance of standards and implementation guidelines for insurance (Duke, 1996).

The *Healthcare Task Group* is a standing Task Group of the X12N Insurance Subcommittee. This Task Group oversees multiple Work Groups that develop standards and industry implementation guides in the area of healthcare and health insurance administration. The purpose of the Healthcare Task Group is the development and maintenance of data standards that support the exchange of business information for *healthcare administration*. The

Healthcare Task Group is developing exactly those standards that HIPAA requires. As required by HIPAA, the Healthcare Task Group sends liaisons to represent X12 at the National Uniform Claim Committee, the National Uniform Billing Committee, the ANSI Health Informatics Standards Board, and Health Level 7.

The X12 standards provide flexibility regarding how application data is represented. Application data can be mapped to one of several different EDI structures. For example, within the X12 843 (Response to Request for Quotation) a supplier can provide pricing information in the header of the document or as individual line item entries. To remove some of the ambiguities of the standards and to ensure the successful exchange of information, trading partners adhere to *Implementation Guides*.

An important point to understand about the X12 transaction standards is the meaning of 'standard'. The X12 standard is a *framework* for structuring and defining various types of information (WPC, 1998). Typically transaction sets have some required segments or elements and may specify certain code values. Yet segments and elements often allow a range of variability with regard to both inclusion type and content. X12N Implementation Guides stipulate specific usage of the transaction set segments and data elements. Implementation guides specify how to use X12 standards. They are developed and published by specific industries to facilitate the implementation of selected standards within that industry. The implementation conventions are typically updated as the standards are updated.

2.3.2.2 X12 Technical Details

Every X12 transaction occurs within an *envelope*. The envelope structure has four levels:

- The Communications Transport Protocol is determined by the communications network transporting the transactions. This has no affect on the transactions themselves, and this information is never used by any application other than the network software.
- The Interchange Control Header is used to determine how the translators will operate on the transactions when arriving, what X12 version to use, what characters are used for terminators, and so on.
- The Functional Group Header is the first level of information that is application oriented. It is basically used to indicate what type of transactions are in the transaction sets that follow. The primary use of this information is for routing data to the correct processing queues or systems for processing.
- The Transaction Set Header is where actual application data begins.

Within a Transaction Set Header are various Data Segments. A *Data Segment* is an intermediate unit of information in a transaction set. It appears as:

- segment identifier,
- one or more data elements, and
- a segment terminator.

A segment can be repeated in a transaction set. A specified maximum number of occurrences must be defined at each specified position.

Data Segments may also indicate *hierarchical relations*. For instance, a certain information source may have a subscriber who has a dependent who is covered. The three levels of source, subscriber, and dependent could be indicated with hierarchical pointers from dependent to subscriber to information source.

Data Elements are the smallest unit of information within a Transaction. A Data Element may be mandatory to appear, may be optional, or may be conditional. A conditional element will appear only if some specified preceding data element is present.

The value that can go in a Data Element may be constrained by a *code set*. These codes may be internal to X12 or may be defined and maintained external to X12. For the internally developed codes, X12 maintains a data dictionary. For instance, the Data Dictionary includes a 'Provider Code'. The Provider Code can occur at most three times in a given segment to describe one provider. The codes and their meaning include:

H	Hospital
R	Rural Health Clinic
AD	Admitting
AS	Assistant Surgeon
AT	Attending
BI	Billing
BS	Billing Service
CO	Consulting
CV	Covering
HH	Home Healthcare
LA	Laboratory
ON	On Staff
OP	Operating
OR	Ordering
OT	Other Physician

When a Transaction is actually prepared for transmission, it is placed into a *stream of characters*. Each data element is separated from the data elements before or after it with a special character, such as '*'. For instance the transmission might include:

PROVIDERS	routing	PAYERS	routing	SPONSORS
Eligibility Verification	270 eligibility inquiry →→ ←←271eligibility information	Enrollment	←← 834 enroll	Enrollment
Claim	837 claim submission →→	Claims Processing		
Accounts Receivable	←← 835 payment advice	Accounts	←← 820 premium	Premium Payment

Figure "Transactions among Provider, Payer, Sponsor": Adapted from WPC, 1998.

ITA * 1 * 1 * CA * 1.08 * CT * CB * 141151 ;

where ITA is the data segment initiator. The subsequent two 1's are data elements separated by '*'. The segment is terminated with a ';'. Again, the symbols that will be used in a given message as separators of data fields and of segments are defined in the Interchange Control Header.

The following sections first overview the transactions and then summarize the '270/271 Eligibility Request and Response Transaction' Implementation Guides.

2.3.2.3 Transaction Overview

The following transactions are mandated by HIPAA:

- Health claims and equivalent encounter information.
- Enrollment and disenrollment in a health plan.
- Eligibility for a health plan.
- Health care payment and remittance advice.
- Health plan premium payments.
- Health claim status.
- Referral certification and authorization.
- Coordination of benefits.
- Claims attachment.

These transaction standards are related to one another (see Figure "Transactions among Provider, Payer, Sponsor"); for instance:

- The *834 Enrollment Transaction* contains demographic, eligibility, and plan information pertinent to the covered lives within an insurance plan (Root, 2000). The health plan member completes an enrollment form and the information is entered into a member database or a payroll system. This information is forwarded to the health plan in an '834 Enrollment Transaction'.
- The healthcare provider may request eligibility information from the health plan by using the *270 Eligibility Request Transaction*. The health plan returns the requested eligibility information to the provider using the '271 Eligibility Response Transaction'.
- The *837 Healthcare Claim Transaction* contains the information required to submit a claim for payment or reporting purposes.
- The health plan returns an *835 Remittance Advice Transaction* to notify the provider of the benefit determination. The actual payment may be done using Electronic Fund Transfer or by generating and mailing a check.

The Rule permits the government to develop additional standards and to build on the relationships among the transactions.

2.3.2.4 Eligibility Technical Details

The 'eligibility' implementation guide applies to transaction sets 270 and 271. The '270 Healthcare Eligibility Benefit Inquiry' and '271 Healthcare Eligibility Benefit Response' work in concert to provide access to accurate plan eligibility and benefit information. The '270' is used to request information, and the '271' is used to respond with coverage, eligibility, and benefit information. The basic *flow* is for a requester (usually a provider) to ask a responder (usually a payer) about healthcare coverage eligibility and associated benefits:

PROVIDER	ROUTING	PAYER
Step 1 INITIATION prepare inquiry	→ Step 2 270 Transaction	Step 3 ACCEPT accept inquiry
Step 6 USE RESPONSE accept information	← Step 5 271 Transaction	Step 4 PREPARE RESPONSE

Figure “Eligibility Transaction Workflow”

1. A provider initiates a 270 transaction and routes it to a payer (see Figure “Eligibility Transaction Workflow”).

2. The payer accepts the inquiry and prepares a response.

3. The response is formatted into the 271 transaction that is sent to the provider.

The requester is normally asking about one individual. Sometimes the responder is a third party administrator, or a Utilization Review Organization, or a self-paying employer. However, in all cases the basic flow is the same — a request sent and a response received.

The ‘270/271 Implementation Guide’ *Table of Contents* includes:

Purpose

Document Use

Business Use

Information Flows

Data Overview

Transaction Sets

270 Inquiry

Header

Detail Information Source

Detail Information Receiver

Detail Subscriber

Detail Dependent

271 Information

Under ‘271 Information’ is the same outline as under ‘270 Inquiry’. The ‘Implementation Guide’ is about 400 pages long.

The ‘270/271 Transaction’ has a *loop* inside a Header and Trailer which loop gives details of first information source, then information receiver, then subscriber, and finally dependent as follows:

Transaction Set Header
  Loop
    Information Source
    Information Receiver
    Subscriber
    Dependent (if needed)
Transaction Set Trailer

The details of a particular data segment become rather mundane but seeing the completion of the fields for some specific examples gives an understanding of what exactly is entailed. The structure of the data segment for the *Information Source Name* follows with the field name on the left and its value in this particular example on the right:

Entity Identifier Code: PR
Entity Type Qualifier: 2
Name, Last or Organization: Blue Cross Blue Shield Illinois
Name, First:
Name, Middle:
Name, Suffix:
Identification Code Qualifier: PI
Identification Code: 12345

The results are transmitted as *alphanumeric strings* without any further structure. Thus the ‘Information Source Name’ is transmitted as:

PR*2*Blue Cross Blue Shield Illinois*****PI*12345~

Blank fields are indicated by *field separators* without any characters between them, as in ‘**’. To continue the example and more fully indicate the way the data segments are completed, the ‘Information Receiver Name’ loop is completed as:

Entity Identifier Code: 1P

Entity Type Qualifier: 1
Name, Last or Organization: Welby
Name, First: Marcus
Name, Middle
Name, Suffix: MD
Identification Code Qualifier: XX
Identification Code: 123456789

The resultant data stream is:

1P*1*Welby*Marcus***MD*XX*1234567
890~

The two loops have the same structure but different values. Given that both the sender and the receiver of the transaction are expecting the X12 messages, the computer can correctly parse these messages.

2.3.2.5 Sybase's HIPAA Toolkit

Sybase Corporation has a product called 'HIPAA Toolkit' for healthcare transactions. This toolkit is a product enhancement to the map development tool, ECMap (Sybase, 2001).

ECMap is a packaged solution enabling transformation of large volumes of data among customers, suppliers and partners. ECMap translates industry-standard and proprietary formats to or from the database. ECMap's business rule and flow logic design is driven by the fact that data messages, while based on standards, are context sensitive. For example, an incoming purchase order may require cross-reference checking for valid part numbers, verification of credit, arithmetic to validate totals or other necessary steps to complete the integration into business applications. These rules and the associated flow logic are created within ECMap's graphical user interface and shared between maps.

The EC Gateway Server is an enterprise message management server to support inter- and intra-company EDI messages. It provides facilities for job-control production scripting and event-driven scheduling, permitting lights-out operations. Additional services include mailbox management, trading partner administration, logging, archiving, data communications and reporting.

The HIPAA Toolkit provides template transactions for the implementation guides as defined by HIPAA. It can be electronically imported to ECMap, so users need only map the required fields of the implementation guide to their application system. In addition, compliance checking maps can be generated to verify compliance to the implementation guide. The HIPAA Toolkit incorporates template transactions for the HIPAA-defined implementation guides. These include Eligibility (270/271), Claim Status (276/277), Service Review (278), Premium Payment (820), Enrollment (834), Claim Payment (835) and Claim Submission (837).

Compliance checking maps can be generated from within the toolkit to verify conformity to the implementation guides. These are baseline compliance maps to which specific rules can be added. The rules further narrow down the implementation guides to allow for business logic and flow. Rules may be created, for example, to validate information such as member numbers.

2.3.2.6 Envoy

Envoy is the largest clearinghouse and processes over 1.4 million claims per day. Envoy implemented the X12 transactions for some of its customers before the government required compliance with X12 transaction formats (Meisner, 2000). Envoy's experience anticipates some of the difficulties that others might also have.

Envoy is experiencing three major problems in moving to X12 formats:

- Many payers seem to be under the mistaken assumption that they need only use the general X12 format and do not need to follow the specific implementation guides from X12. This is an education problem that Envoy has addressed.
- In the new standards, providers may be required to provide some data that was previously not required. Alternatively, the provider may be familiar with providing some data that the new standard does not accept. The result is that the information provided by the payer does not meet the requirements of the X12 implementation guide.
- The order in which the HIPAA mandates are appearing is another cause for difficulty. For instance, if the transaction formats are official but the unique identifiers are not official, the transactions must carry secondary identifiers and demographic information to account for the absence of the national identifier. This adds to the overhead of processing.

Print images are responsible for a large percentage of EDI claim volume. Many EDI products work with Practice Management Systems to take in the print image and convert to data formats for transmission. Until the forms have been upgraded with the data content of the HIPAA Implementation Guides, these submitters will not become HIPAA compliant, and the claims will revert to *paper*.

2.3.3 Review Questions

1. What are the desirable characteristics of data formats for EDI?
2. What are the structures and processes of X12 and where do healthcare EDI standards fit in X12?
3. What are the four levels of an X12 transaction and how do they relate to one another?
4. Describe the flow of the 270, 271, 834, 835, and 835 Transactions in the healthcare setting.
5. Take an example statement such as "PR*2*Blue Cross Blue Shield Illinois*****PI*12345~". Put your own values in the statement and explain what the statement would mean based on the 'Information Source Name' of the 270 transaction.
6. Describe how one piece of commercial software supports claims transactions from the healthcare provider.
7. What problems has Envoy experienced during migration to the HIPAA X12 specifications?

2.4 Code Sets

Main Points

- Code sets are mandated by HIPAA to be standardized and certain fields in transactions must be completed only with values from those code sets.
- For diseases the prime code set is ICD and for procedures is CPT.
- Mapping among code sets is required during the conversion time.
- Ambiguity remains a problem with code sets.

The administrative simplification provisions of HIPAA require DHHS to adopt standards for code sets for administrative and financial transactions (DHHS, 1998). Two types of code sets are required for data elements in the transaction standards:

- large code sets for medical data, including coding systems for diseases, causes of disease, actions taken to prevent, diagnose, treat, or manage diseases, and any supplies used to perform these actions; and
- smaller sets of codes for other data elements such as race, type of facility, and type of unit.

The HIPAA Implementation Team recommends the *code sets* that become HIPAA standards for medical data. The smaller sets of codes for other data elements in transactions standards are part of the transaction standards themselves and are specified in the ASC X12 Implementation Guides.

2.4.1 Conceptual Models

Usability and expressiveness may conflict. The biggest challenge to using a medical vocabulary is to balance usability with the necessity to capture adequately rich information. For example, a physician may order vital signs to be taken at specific intervals, but different physicians may have different concepts of what *vital signs* means. The physician might say vital signs are temperature, pulse, respiration, and blood pressure. However, a sign like 'blood pressure' might be different if the patient is standing, sitting, or supine. The physician is unlikely to be comfortable to have to specify the full details each time of what 'vital signs' means to that physician. The various users of the concept must agree in advance as to exactly what is intended by the use of any potentially ambiguous concept, such as 'vital signs'.

A code is a representation assigned to a term so that it may more readily be processed. A simple listing of codes and the terms with which they are associated is a *code set*. For example, in the state postal code set, the code for Maryland is MD and for Virginia is VA.

Coding systems include code sets but have additional structure. The ASTM gives these criteria for good coding systems:

- Concepts are clearly defined and the concepts do not overlap with one another. Plus the set of concepts covers all the necessary concepts of the intended scope of the vocabulary.
- Structured relationships among the concepts facilitate the use of the concepts in indexing and retrieval.
- The coding system is designed so as to readily support refinement across time.

Librarians, biologists, philosophers, and others have studied the nature of coding systems for centuries. A coding system may be used to index documents, classify animals, or represent human knowledge.

One type of coding system is a *classification language*. The classic way to develop a classification language is to study members of the population (be they medical journal articles, organisms, or something else) to be represented by the language and to first determine the key concepts needed to describe the members of the population. Each key concept is associated with a key term. Given that several alternate key terms exist, they are represented as synonyms of one another and a definition for the concept is provided. To better understand the classification language, the key concepts are organized in a hierarchy. Each time a member of the population appears that raises questions about the ability of the language to adequately represent that member, then those developing the language need to consider whether the concepts appropriate to the new member map to existing concepts or require the generation of a more specific (narrower) concept than any already in the language or a more general (broader) concept than any already in use.

Another type of coding system is a thesaurus. In a *thesaurus* concepts are defined, synonyms to a concept are indicated, and hierarchically related concepts are identified. An example of a good thesaurus is the Medical Subject Headings of the National Library of Medicine. It has about 100,000 concepts in a 10-level hierarchy and is used to index over seven million biomedical documents.

For the standardization of transactions and the information within them, code systems are vitally important. The concepts in the code system are the eligible entries into the fields of a transaction. Given that agreement exists about what codes are used, the meaningfulness of the transactions is increased. Furthermore, these codes are often used to identify the diagnosis and treatment of a patient and to, in turn, determine the financial reimbursement to the healthcare provider from the payer.

2.4.2 Diseases, Drugs, and Procedures

The code for diseases is the *International Classification of Diseases, 9th edition, Clinical Modification (ICD-9-CM)*. The specific data elements for which ICD-9-CM is the required code are enumerated in the Implementation Guides for the transactions (DHHS, 1998d). The complete ICD-9-CM is available for free from DHHS (National, 1998). ICD-9-CM includes one volume as an alphabetical index and another volume as a tree-structure in which concepts are located hierarchically by their associated code numbers. For example, in the alphabetical index one finds at 'nasopharyngitis' the following information:

- Nasopharyngitis (acute) (infective) 460
- Natal tooth 520.6
- Nausea 787.02

In the hierarchical index at the code 460 for nasopharyngitis, one finds:

- 460-519 RESPIRATORY SYSTEM DISEASES
- 460-466 Acute Respiratory Infections
- 460 Acute nasopharyngitis [common cold]
- 461 Acute sinusitis

ICD-9-CM is utilized to facilitate payment of health services, to evaluate utilization patterns, and to study the appropriateness of healthcare costs. ICD-9-CM also provides access to medical records for medical research and public health purposes.

ICD-9-CM is not always precise or unambiguous. However, there are no viable alternatives immediately. Many problems cannot be resolved within the current structure, but are being addressed in the development of *ICD-10-CM*.

Different coding systems are used for physician procedures, dental procedures, and other health-related services:

- For dental procedures the *Code on Dental Procedures and Nomenclature* is available from the American Dental Association for a charge.
- For inpatient hospital services 'ICD-9-CM, Volume 3 Procedures' is appropriate.

- For physician services a combination of the *Current Procedural Terminology-4* (available from the American Medical Association for a charge) and the *HCFA Procedural Coding System* (available for free from DHHS) is appropriate.

The Healthcare Financing Administration Procedural Coding System (HCPCS) contains three levels:

- Level I (CPT-4) is developed and maintained by the AMA and captures physician services.
- Level II of HCPCS contains codes for products, supplies, and services not included in CPT-4.
- Level III is local codes and includes codes established by insurers and agencies to fulfill local claim processing needs.

The local codes have been a source of *confusion*. Covered entities may not use local codes in standard transactions after compliance with the final rule is required. All local codes must be eliminated. Users that need codes must apply to the appropriate organizations (e.g. HCFA for HCPCS codes, the AMA for CPT-4 codes) for national codes.

The standard code set for drugs is the National Drug Code Directory from the Food and Drug Administration. The full Directory is available for free (FDA, 2000). The drug codes are also published in the *Physicians' Desk Reference* under the individual drug product listings. While the "Transactions and Code Sets" Final Rule required NDC for drugs and biologics, a guideline for change includes (NCVHS, 2001):

> The NCVHS recommends that HHS work with ANSI X12N to ensure that HCPCS codes, as well as NDC codes, can continue to be used in the standard institutional and professional claims transactions.

NDC is very useful in retail pharmacy systems where bottles of pills are tracked. NDC identifies the manufacturer, the size of the bottle, and so on. However, when a physician wants to inject 2 grams of gamma globulin, NDC does not support the specification of the quantity of injection. Yet, such information may be entered in a hospital claim form. HCPCS partially supports such quantity of injection information and thus meets a need that NDC does not. A better drug and biologics code set is needed. In May 2002 the government published a Proposed Rule for Transactions and Code Sets that allows transactions other than retail pharmacy ones to contain drug codes other than NDC.

The standard use of codes harmonizes the sharing of information among providers and payers. However, all the codes have the problem of being imprecise and ambiguous. No better alternatives are currently available for codes, although the currently used codes should improve in future versions.

2.4.3 Mapping and Metadata

The ASC X12 transaction standards limit which of the codes on the various X12 code lists can be used for a particular transaction. However, some of these codes are currently not used by either providers or payers. Enabling these codes will require either a *mapping* of the current list being used by the provider or payer to the X12 code list or a modification of their current system to utilize the X12 code list. Of greater impact is the adoption of the standard code lists such as CPT and ICD-9-CM. For those who currently use 'in-house' codes mapping to other codes might be difficult (IBM, 2000).

Code length may be a problem. The length of some of the HIPAA codes might be greater than what a payer's or provider's system can currently accommodate. An example is the use of the National Drug Code Directory in place of the Procedure Coding System for billing of drug therapy given in a provider's office. The current length of a code in the Procedure Coding System is 5 bytes while a code in the National Drug Code Directory code may be 11 bytes. Modifications will be required to accommodate the new coding regulations.

To deal with the mapping problem, a master data dictionary will be created. This master data dictionary is also called metadata. This will provide for common data definitions across the standards selected for implementation and support semi-automated mapping. At a minimum, the dictionary will include data element names, definitions, and appropriate references to the transactions where they are used.

The work on this master data dictionary will benefit from the experience of the Australian government. The Australian government has said (Australian, 2000):

> In Australia it is crucial that data collected by the different health jurisdictions be consistent with uniform definitions, and follow guidelines and standards. This is necessary to allow comparison between these jurisdictions and with other countries, and to enable aggregation of data at the national level. In May 1993 the Commonwealth …. signed an agreement to improve the quality of and cooperation in the development of national health information.

The *Australian National Health Information Knowledge Base* is an electronic repository and query tool for health metadata. The Knowledge Base includes a number of different but inter-related areas of health information, namely:

- information models, including the National Health Information Model;
- data element definitions, including the National Health Data Dictionary and the National Community Services Data Dictionary;
- data agreements, including for instance the specification of a minimal data set required in certain circumstances; and
- a keyword system to access subject-related data elements.

The knowledge base incorporates an electronic version of the National Health Information Model. Users of this model can 'drill down' from high-level entities, through entity sub-types to reach data element definitions

The Australian metadata standards are based on *ISO/IEC 11179* 'Specification and Standardization of Data Elements' (ISO, 1999). ISO/IEC 11179 describes standardizing and registering data for the purpose of making it shareable. ISO/IEC 11179 has six-parts as follows:

- Framework for the specification and standardization of data elements,
- Classification of concepts for the identification of domains,
- Basic attributes of data elements,
- Rules and guidelines for the formulation of data definitions,
- Naming and identification principles for data elements, and
- Registration of data elements.

The need for such a standard has become evident with the increasing emphasis being placed on electronic dissemination of and access to data. The standard seeks to ensure that the exact meaning of the data is clearly communicated.

Australia has created a metadata directory for health information, and comparable efforts are underway in the United States. The *United States Health Information Knowledgebase (USHIK)* project is to:

- build, populate, demonstrate, and make available for general use a data registry to assist in cataloging and harmonizing data elements across organizations and
- utilize selected HIPAA elements for demonstration of its capability (USHIK, 2000).

As in the Australian case, USHIK relies heavily on ISO 11179 for a conceptual model of metadata. The data element descriptions from selected health industry standards organizations have been loaded into appropriate fields in the USHIK with as little modification as possible. For the purpose of demonstrating the capabilities of a metadata registry, the linking of elements to a model has been focused on the data elements in the X12 834 Benefit Enrollment and Maintenance transaction and implementation guide. These data elements have also been linked to the Australian model.

2.4.4 Ambiguity and post-2000

The recommended code sets meet some of the needs of the community. However, many practical problems exist, such as overlaps among different procedure codes and inadequate coverage of allied health services. To meet all of the community's needs will require changes to the code sets recommended or their replacement by newer systems, once these have been fully tested and revised. Essentially all segments of the healthcare community testified that there was *no practical alternative* to the recommended code sets for the immediate future (DHHS, 1998d).

All of the recommended code sets are supported by U.S. government agencies or private sector organizations that have demonstrated a commitment to *maintaining* them over time. The owners of the code sets have existing procedures for updating the code sets at least annually. The organizations are, however, not necessarily ANSI-accredited Standards Development Organizations.

Although the exact timing and precise nature of changes in the code sets designated as standards for medical data are not yet known, it is inevitable that there will be changes to coding and classification standards over time. Changes will be required to address current coding system deficiencies that adversely affect the efficiency and quality of administrative data creation and to meet international treaty obligations. For example, ICD-10-CM is likely to replace ICD- 9-CM as the standard for diagnosis data. When any of the standard code sets are replaced by wholly new or substantially revised systems, the information systems that support those codes may need to be changed. For instance, the current draft of ICD-10-CM for diagnoses contains 6 digit codes; while the longest ICD-9- CM codes have 5 digits. In addition to accommodating the initial code set standards, those that produce and process electronic administrative health transactions should build the system flexibility that will allow them to implement different code formats in the future.

Any major change in coding systems involves significant *initial costs* and dislocations, as well as some level of discontinuity in data collected before and after the change. These factors must be weighed against expected improvements in the efficiency of data creation and in the accuracy and utility of the data collected. In the future, more *flexible health data systems* may assist in reducing the costs of implementing changes in administrative coding and classification standards, especially if administrative codes can be generated automatically from more granular clinical data.

2.4.5 Review Questions

1. What is a ‘coding system’ and how are coding systems important in standardizing transactions?
2. What are some features of the Medical Subject Headings? What are some features of ICD-9-CM?
3. What are the Australians producing in the way of a metadata dictionary?
4. What is the difference between a classification language, a thesaurus, and a knowledge base? (Project Question)

2.5 Identifiers

Main Points

- HIPAA mandates national identifiers be developed for providers and DHHS has developed a simple, numeric Provider Identifier but also requires a National Provider File that gives substantial identifying information about a provider.
- An Employer Identifier has also been mandated and is the Internal Revenue Service’s existing Employee Identifier Number.
- The public has opposed the development of a Personal Identifier and the government has stopped progress on that.

What follows is based on the ‘National Provider Identifier’ NPRM, the ‘National Employer Identifier’ Final Rule, and the aborted effort to produce a Personal Identifier.

2.5.1 Provider Identifiers

A provider identifier is needed. Currently, there is no universally accepted national identification and enumeration system for healthcare providers. Providers must use multiple identifiers for programs and organizations with which they do business. Data are not readily transportable among systems and, thus, must be collected redundantly. The problems and costs of exchanging *provider data* are great, hampering coordination of benefits and fraud and abuse detection efforts.

2.5.1.1 Selection criteria

What makes a good provider identifier? Of the *ten criteria* for selecting good standards that DHHS enumerated, four are particularly important in selecting a provider identifier and are described here in the specific context of the provider identifier:

#1. Improve the *efficiency and effectiveness* of the healthcare system.

In order to be integrated into electronic transactions efficiently, standard provider identifiers must be easily accessible. Health plans must be able to obtain identifiers and other key data easily in order to use the identifier in electronic transactions. Existing healthcare provider files have to be converted to the new standard. In addition, healthcare providers will need to know other healthcare providers’ identifiers (for example, a hospital needs the identifiers of all physicians who perform services in the facility). To meet this criterion, the identifier should not be proprietary; that is, it should be possible to communicate identifiers freely as needed. Moreover, the issuer must be able to reliably issue each healthcare provider only one identifier and to issue each identifier only once.

#2. Meet the needs of the health data standards user community.

The identifier must be comprehensive. It must accommodate all healthcare provider types or must be capable of being expanded to do so. Based on the definition of "healthcare provider", this includes individual healthcare providers who are employed by other healthcare providers and alternative practitioners who may not be currently recognized by health plans. The identifier must have the capacity to enumerate healthcare providers for many years without reuse of previously assigned identifiers. To meet this criterion, over time, the identifier must be capable of uniquely identifying at least 100 million entities.

#3. Be consistent and uniform with other HIPAA and other private and public sector health data standards in providing for privacy and confidentiality.

Confidentiality of certain healthcare provider data must be maintained. Certain data elements (for example, social security number and date of birth) needed to enumerate an individual healthcare provider reliably should not be made available to the public.

#10. Incorporate flexibility to adapt more easily to changes.

To meet this criterion, the identifier must be *intelligence-free* (the identifier itself should not contain any information about the healthcare provider). Intelligence in the identifier would require issuing a new identifier, if there is a change in that information. For example, an identifier containing a State code would no longer be accurate if the healthcare provider moves to another State.

2.5.1.2 Candidate identifiers

A number of *candidate identifiers* were assessed to see whether they met the four specific criteria highlighted in the preceding discussion. Several alternatives have been critiqued, including:

- the unique physician identification number, which is issued by DHHS;
- the health industry number, which is issued by the Health Industry Business Communications Council; and
- the National Association of Boards of Pharmacy number, which is issued by the National Council for Prescription Drug Programs in cooperation with the NABP.

Details of these alternatives are presented next.

Unique Physician Identification Numbers are currently issued to physicians, limited license practitioners, group practices, and certain non-institutional providers (for example, ambulance companies). These numbers do contain intelligence (the first position designates a provider type, e.g., physician) and are only six positions long, which would not be able to accommodate a sufficient number of future healthcare providers. The Unique Physician Identification Number does not meet criteria 2 or 10.

The *Health Industry Number* is used for contract administration in the health industry supply chain, as a prescriber identifier for claims processing, and for market analysis. It consists of a 7-position alphanumeric identifier and a 2-position alphanumeric suffix identifying the location of the prescriber. The suffix contains intelligence. Health industry numbers can enumerate individual prescribers as well as institutional providers. They are issued via a proprietary system maintained by the Health Industry Business Communications Council, which permits subscriptions to the database by data re-sellers and others. The health industry number does not meet criteria 1, 3, or 10.

The *National Association of Boards of Pharmacy number* is a 7-digit numeric identifier assigned to licensed pharmacies. It is used to identify pharmacies to various payers. Its first two digits denote the State, the next four positions are assigned sequentially, and the last position is a check digit. A 7-digit numeric identifier would not yield a sufficient quantity of identifiers, and there is intelligence in the number. This number does not meet criteria 2 or 10.

The Social Security Number issued by the Social Security Administration, the Drug Enforcement Administration Number issued by the Drug Enforcement Administration, and the Employer Identification Number issued by the Internal Revenue Service were considered. Neither the Social Security Number nor the Drug Enforcement Administration Number meets the accessibility test. The Privacy Act protects the use of the *Social Security Number* by Federal agencies, and the *Drug Enforcement Administration Number* must remain confidential in order to fulfill its intended function of monitoring controlled substances. The *Employer Identification Number* does not meet the comprehensiveness test, because some individual healthcare providers do not qualify for one. Given the various problems with any existing alternatives, DHHS has proposed a new system for identifying providers and called it the National Provider System.

Organizations with a need to enumerate providers had joined in an effort, begun by the Healthcare Financing Administration in 1993, to establish a national system for identifying and uniquely enumerating healthcare providers. This *National Provider System (NPS)* enumerates healthcare providers by

- assigning the National Provider Identifier to each individual, organization, and group provider and
- associating a file with the Identifier to give details about the provider.

The design of NPS proves superior to any existing alternatives for the needs of HIPAA.

2.5.1.3 National Provider Identifier

The proposed National Provider Identifier (NPI) is an 8-position alphanumeric identifier (DHHS, 1998c). It includes as the 8th position a numeric check digit to assist in identifying erroneous or invalid NPIs. The NPI format would allow for the creation of approximately *20 billion unique identifiers*.

The *8-position alphanumeric format* was chosen over a longer numeric-only format in order to keep the identifier as short as possible while providing for an identifier pool that would serve the industry's needs for a long time. Some healthcare providers and health plans might have difficulty in the short term in accommodating alphabetic characters. Therefore, DHHS would issue numeric-only identifiers first and introduce alphabetic characters starting with the first position of the NPI. This would afford additional time for healthcare providers and health plans to accommodate the alphabetic characters.

2.5.1.4 National Provider File

The proposed National Provider System (NPS) collects and stores in the National Provider File (NPF) information about a healthcare provider. The majority of this information is used to uniquely identify a healthcare provider, such as name and Social Security Number. Some information is used for administrative purposes, such as the provider's address. A discussion of some of the attributes of the File follows.

The data elements that may be expensive to either validate or maintain (or both) are the license information, provider practice location addresses, and membership in groups:

- *Licenses* may be critical in determining uniqueness of a healthcare provider (particularly in resolving identities involving compound surnames) and are, therefore, considered to be essential by some. License information is *expensive to validate* initially, but not expensive to maintain because it does not change frequently.
- The *provider practice location address* can be used to aid in investigating possible provider matches, in converting existing provider numbers to National Provider Identifiers, and in research involving fraud or epidemiology. Some potential users felt that practice addresses changed too frequently to be maintained efficiently at the national level. The average Medicare physician has two to three addresses at which he practices. Group providers may have many more practice locations. About 5 percent of healthcare providers require updates annually, and addresses are one of the most frequently changing attributes. As a result, maintaining more than one practice address for an individual provider on a national scale could be burdensome and time consuming. Many potential users believe that practice addresses could more adequately be maintained at local levels.
- Some potential users felt that *membership in groups* was useful in identifying healthcare providers. Many others, however, felt that these data are highly volatile and costly to maintain. These users felt that membership in groups could not be satisfactorily maintained at the national level.

A few of the data elements are collected at the request of potential users that have been working with DHHS in designing the database. For example, *Race* is important to some, and since it is not maintained, only stored, the cost of this data element is low. Other data elements (Resident/Intern Code, Provider Certification Code and Number, and Organization Type Control Code), while not used for enumeration of a healthcare provider, have been requested by some. These data elements are optional and do not require validation.

2.5.1.5 Data Dissemination

In addition to the healthcare provider's name and National Provider Identifier (NPI), it is important to make available other information about the healthcare provider so that people with existing healthcare provider files can associate their healthcare providers with the appropriate NPIs. DHHS would establish *two levels of users* of the data in the NPS for purposes of disseminating information:

- Enumerators would have access to all data elements for all healthcare providers in order to accurately resolve potential duplicate situations (that is, the healthcare provider may already have been enumerated). Enumerators would be required to protect the privacy of the data in accordance with the Privacy Act.

- The public (which includes individuals, healthcare providers, software vendors, health plans that are not enumerators, and healthcare clearinghouses) would have access to selected data elements.

The access to the public data would be electronic in order to support frequent users. The public data would be widely available. The Unique Physician Identification Number Directory (currently available to the public) would be discontinued and replaced with a similar document or electronic file once the NPS is in place.

2.5.1.6 Converting Cost

Healthcare providers would have to obtain an NPI and report changes in pertinent data. Current Medicare providers might receive their NPIs automatically, and other healthcare providers may be enumerated in this manner to the extent that appropriate valid data files are available. New healthcare providers would have to apply for an NPI. This does not impose a new burden on healthcare providers. The vast majority of health plans issue identifiers to the healthcare providers with whom they transact business in order to facilitate the electronic processing of claims and other transactions. The information that healthcare providers must supply in order to receive an *NPI* is significantly less than the information most health plans require to enroll a healthcare provider.

Some existing provider identifier systems assign multiple identifiers to a single healthcare provider in order to distinguish the multiple identities the healthcare provider has in the system. In these systems, the healthcare provider may have a different identifier to represent each contract or provider agreement, practice location, and specialty or provider type. Since the NPI is a unique identifier for each healthcare provider, the NPI does not distinguish these multiple identities. Systems that need to distinguish these identities would need to use data other than the NPI to do so. The change to use other data would add complexity to the conversion to the NPI or to any other standard provider identifier, but it is necessary in order to achieve the goal of *unique identification* of the healthcare provider.

Conversion costs depend on identifier intelligence. The complexity of the conversion would be significantly affected by the degree to which health plans' processing systems currently rely on intelligent identifiers. For example, a health plan may route claims to different processing routines based on the type of healthcare provider by keying on a provider type code included in the identifier. Converting from one unintelligent identifier to another is less complex than modifying software logic to obtain needed information from *other data elements*. However, the use of an unintelligent identifier is required in order to meet the guiding principle of assuring flexibility.

What is the cost to the NPS host? The NPS would be used to generate NPIs and serve as the central enumeration system and database. DHHS began to develop the NPS for Medicare use. As the NPS becomes national in scope, the cost of maintaining the NPS software, hardware, and telecommunications, and operating a Help Desk to deal with user questions, would cost approximately $10.4 million over the first three years of operation and approximately $2.9 million per year thereafter. Roughly half of these costs are attributable to telecommunications expenses.

The NPS database is loaded using health plans' existing, prevalidated files to the extent possible. This would reduce costs by not repeating the process of soliciting, receiving, controlling, validating and keying applications from healthcare providers that have already been enumerated by a trusted source. For example, DHHS would use existing Medicare provider files to initially load the NPS database. The majority of work to reformat and edit these files has already been completed.

NPIs are needed for

- 1.2 million current healthcare providers and
- 30,000 new healthcare providers annually

because they conduct HIPAA transactions. An additional 3 million healthcare providers (120,000 new healthcare providers annually) do not conduct HIPAA transactions, but may choose to be enumerated at some future time. These healthcare providers would be primarily individual practitioners, such as registered nurses and pharmacists, who perform services in institutions and whose services are not billed by the institution.

Based on Medicare carriers' costs, the average cost to enumerate a healthcare provider should not exceed $50. *Enumeration activities* would include:

- assisting healthcare providers and answering questions,
- accepting the application for an NPI,
- validating as many of the data elements as possible at the point of application to assure the

submitted data are accurate and the application is authentic,
- entering the data into the NPS to obtain an NPI for the healthcare provider,
- researching cases where there is a possible match to a healthcare provider already enumerated,
- notifying the healthcare provider of the assigned NPI, and
- entering updated data into the NPS when notified by the healthcare provider.

The $50 estimated average cost to enumerate a healthcare provider is an upper limit.

The cost would decrease significantly, if the NPS would capture only one practice address for an individual or organization provider and would not assign location codes. Costs would decrease because DHHS would collect significantly less data at the time of enumeration, and the data that would be collected would not need to be updated very frequently. Consultations with the industry reveal a growing consensus for this alternative.

One option calls for enumeration of healthcare providers by a *consortium* of private health plans and government agencies. Medicare, Medicaid, CHAMPUS, and the Department of Veterans Affairs already assign identifiers to healthcare providers with whom they conduct business. They would simply begin to use the NPS to issue NPIs instead of using their own systems to assign the identifiers they now use.

2.5.2 Employer Identifier

HIPAA directed DHHS to develop an Employer Identifier. Employers, as sponsors of health insurance for their employees, often need to be identified in healthcare transactions, and a standard identifier for employers would be beneficial for transactions exchanged electronically. Healthcare providers may need to identify the employer of the participant on claims submitted to health plans electronically. Employers need to identify themselves in electronic transactions when they enroll or disenroll employees in a health plan or make premium payments to health plans on behalf of their employees. Employers and healthcare providers may need to identify an employer as the source or receiver of information about a participant's eligibility.

The Employer Identifier Final Rule specifies that the 'Employer Identifier' is the Employer Identification Number (EIN) assigned by the Internal Revenue Service. The EIN is the *taxpayer identifying number* and has nine digits separated by a hyphen, as follows: 00-0000000.

2.5.2.1 Selection Criteria

The EIN as the employer identifier standard can be evaluated according to the ten criteria explained earlier. EIN meets:

- Criteria #1, #2, #4, and #6 in that it is a nationally defined and assigned employer identifier and is the most widely used employer identifier in the United States.
- Criteria #3 and #5 in that it is already in use in the Accredited Standards Committee X12 electronic transactions that require an employer identifier, including the transactions used for the Health Claim, Enrollment and Disenrollment in a Health Plan, Eligibility for a Health Plan, and Health Plan Premium Payment.
- Criterion #7 in that it is technologically independent of computer platforms and transmission protocols.
- Criterion #8 in that it is a relatively short identifier that would fit into many existing formats.
- Criterion #9 in that it is an identifier already assigned to each employer for tax identification purposes. Its adoption as a standard would not result in additional data collection or paperwork burdens on users.
- Criterion #10 in that it is flexible enough to identify any employer, regardless of services, organization, or provider type.

Since the IRS is responsible for issuing the EIN, DHHS consulted with the IRS on the legality and feasibility of using the EIN as the standard employer identifier for electronic health transactions, and the IRS concurred.

What alternatives existed to the EIN? Could the *PAYERID*, the 9 position numeric identifier developed by DHHS as the unique identifier for health plans, have been used as the employer identifier? Since all employers are already enumerated by EIN, an entirely new employer identifier would require everyone to convert to a new identifier in addition to the EIN, which would still be used. Another key drawback to the use of the PAYERID as the employer identifier is that the PAYERID numbering scheme does not have sufficient numbers available to enumerate all health plans and all employers. In addition, PAYERID's data capabilities were developed based on the data requirements for health plans, which are not the same as those for employers. Based on these limitations, the PAYERID would not meet criteria #1, #2, #4, #9, and #10 and would not be acceptable as a candidate for the employer identifier.

The *D-U-N-S number* and the D-U-N-S+4 number, maintained by Dun & Bradstreet, are sometimes used to identify business entities including employers (primarily in premium payment transactions). Since the D-U-N-S and D-U-N-S+4 numbers were not widely used in the claim, the enrollment and disenrollment in a health plan, and the eligibility for a health plan transactions, these numbers did not meet criteria #1, #2, #4, and #9 and were less appropriate than the EIN as candidates for the employer identifier.

2.5.2.2 Affected entities

The Employer Identifier Final Rule was published on May 31, 2002 (DHHS, 2002a). It took effect 60 days later, namely, July 30, 2002. Covered entities (other than small health plans) have 2 years in which to achieve compliance – i.e., until July 30, 2004.

Healthcare providers that conduct electronic transactions with health plans will have to obtain and use the EIN to identify the employer in those electronic transactions that require an employer identifier. In most cases healthcare providers currently use the EIN of the employer in those transactions that require an employer identifier. Any negative impact on healthcare providers generally would be related to the initial *implementation period* for providers that currently use an identifier other than the EIN to identify the employer in electronic transactions. They will incur implementation costs for converting systems from other employer identifiers to the EIN. Some healthcare providers would incur those costs directly and others would incur them in the form of fee increases from billing agents and healthcare clearinghouses.

Healthcare plans and healthcare clearinghouses that engage in electronic commerce will have to modify their systems to use the EIN, if they do not currently use the EIN to identify the employer in electronic transactions that require an employer identifier. In most cases healthcare plans and clearinghouses currently use the EIN of the employer in those transactions that require an employer identifier. The conversion for those currently using an employer identifier other than the EIN will be a *one-time cost*.

Each employer will have to disclose its EIN, when requested, to any entity that conducts standard electronic transactions that require the employer's identifier. Entities that conduct electronic transactions that require an employer identifier commonly obtain that identifier from the employer as a normal business practice. This practice would not change. Any impact on employers would be the *one-time impact* to disclose the EIN to entities that have previously used a different identifier for that individual.

2.5.3 Personal Identifier

The Personal Identifier is the most important identifier for administrative simplification but has met stiff resistance from privacy advocates. At the moment different systems use different methods of trying to uniquely identify individuals. Mistakes in this identification process lead to various adverse consequences. For instance, if a person is uniquely identified by his or her name, then what happens when different hospital staff enter the name in different ways? When Robert Smith goes to the emergency room and identifies himself as Robert Smith, a search for any previous record in the hospital for that individual is made. If, however, Robert had been previously uniquely identified as Bob, then no match may be found. A new record is created for Robert Smith, although records for this individual already existed as Bob Smith. The possible adverse medical consequences of not being able to see the record of previous diagnoses and treatments for the patient could be severe. Hospitals frequently experience such problems. A reliable unique personal identifier would alleviate this problem.

When the public learned that the government was proposing personal health identifiers, various protests ensued that were magnified by the media. The concerns were that government would connect personal health information to financial information and use this connection to the detriment of individuals. Protestors raised the specter of a police state in which no freedom exists for any citizens. These protests led the government to *withdraw* its plans to create personal identifiers until such time as privacy and security regulations were adequately agreed.

Robert Gellman, as a member of the National Committee on Vital and Health Statistics, said:

> The Committee characterizes the public response to its July 1988 hearings by stating that 'there was great concern expressed that privacy protections were essential before any universal health identifier is put in place'. In my opinion, that is a distortion of the objections. The public appeared to be dead set against an identifier without qualification. …. The Committee expressed no reservation about the costs of an identifier, about any possible negative consequences for the availability of healthcare, or about the nature of privacy

> controls that might be needed. In my opinion, none of the health privacy proposals offered to date would prevent a health identifier from becoming a universal national identifier for all governmental and private purposes.

The negative public response to the personal identifier led to reactions by the executive and legislative branches of the government. Congress enacted a moratorium on the administrative adoption of a patient identifier.

For those who want their personal records as secret as possible, having such records temporarily in the hands of a physician could be a threat to *secrecy*. Yet, without such sharing of information the person cannot get the best care from the healthcare system. The debate over the personal identifier continues.

2.5.4 Review Questions

1. Describe the National Provider System. What is the role of the National Provider Identifier and of the National Provider File?
2. What are the costs of maintaining the National Provider System and what collaborations are anticipated to reduce that cost?
3. Why would HIPAA call for an Employer Identifier and what are the reasons for the preferred choice of an Employer Identifier?
4. Why is a Personal Identifier important and why has progress on a Personal Identifier stalled?
5. The costs of maintaining the National Provider System or any such identifier system could be enormous. However, the opportunity might exist to have a system in which people would go to a web site and enter or update their attributes as appropriate. What are the pros and cons of this ‘self-organizing’ approach? (Project Question)
6. What countries have national personal identifiers already? What lessons can be learned by Americans about how to deal with the issue of personal identifiers from the experiences of other countries? (Project Question)

2.6 Impact Analysis

Main Points

- The general principle behind the cost saving is the reduction in the number of conversions that have to occur from one format to another.
- DHHS has made extensive cost/benefit tables and shown how savings increase over time and how the relative financial benefits initially favor payers.
- The ultimate criterion of cost/benefit should be the quality of healthcare and for that standardization of transactions should clearly bring greater benefit than cost.

Administrative costs comprise 17 percent of total health expenditures (Dobson and Bergheiser, 1993). Paperwork inefficiencies are a component of those costs, as are the inefficiencies caused by the more than 400 different data transmission formats currently in use. However, migration to these recognized standards has been hampered by the inability to develop a concerted approach.

2.6.1 One versus Many

DHHS chose to designate a single standard for each identifier and transaction. On the surface, allowing alternate standards would seem to be a more flexible approach, permitting healthcare providers and health plans to choose which standard best fits their business needs. In reality, health plans and healthcare providers generally conduct EDI with multiple partners. Since the choice of a standard transaction format is a bilateral decision between the sender and receiver, most health plans and healthcare providers would need to support all of the designated standards for the transaction in order to meet the needs of all of their trading partners. Single standards will maximize net benefits and minimize ongoing confusion.

To understand the costs of multiple standards, an analysis of the number of converters or translators will be presented. Assume there are standards A and B and messages have to be shared that might be in either format. A *converter* is needed from format A to format B and conversely (see Figure "Two Standards"). If there are 4 standards A, B, C, and D, then 12 converters are needed: A to B, A to C, A to D, B to A, B to C, B to D,…., D to A, D to B, D to C (see Figure "Four Standards"). The 12 can be computed from 4 times (4-1). In general, for n formats, n times (n-1) converters are needed. Thus for 400 standards there would be needed 400 times 399 or approximately 160,000 converters.

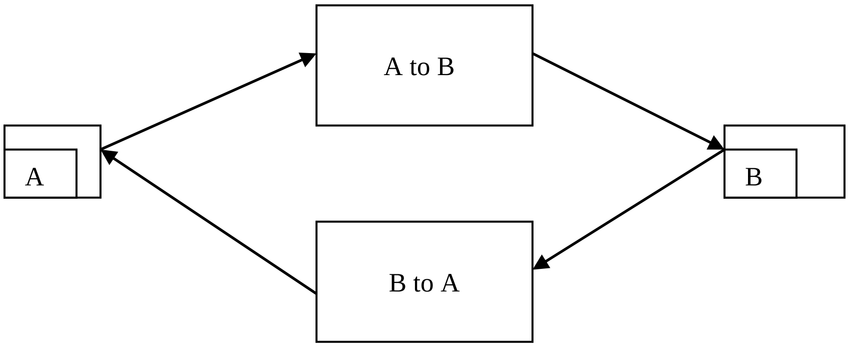


Figure "Two Standards": A to B and B to A

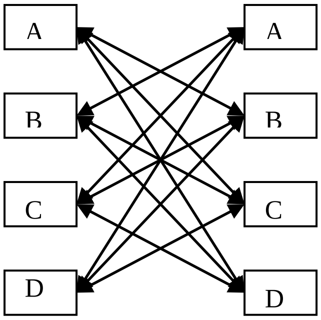


Figure "Four Standards": The formats A, B, C, and D are connected by converters. A has to be converted to B when sent to B, and B has to be converted to A when sent to A and so on. Each bi-directional arrow between x and y represents two converters – one from x to y and the other from y to x.

To tailor the conversion efforts to the healthcare case, consider first a provider that has a medical record with a certain format and local codes. When the provider sends a claim to health plan$_1$, the provider needs to translate the relevant parts of its internal record into the format of plan$_1$ and the local codes of plan$_1$. Likewise, when the provider wants to send a claim to health plan$_2$, the provider needs to translate its information into the format and local codes of plan$_2$ (see Figure "Provider to Plans"). For each different format and local code of a plan, the provider needs a different translation effort. The translation effort is actually double, as translating would be required for the formats and for the codes.

Continuing in this way but considering only formats and not also codes, one can see that if

- for 100 providers each has a distinct internal medical record format and
- for 200 health plans each has a unique claims formats, then
- 100 times 200 or 20,000 translators would be needed.

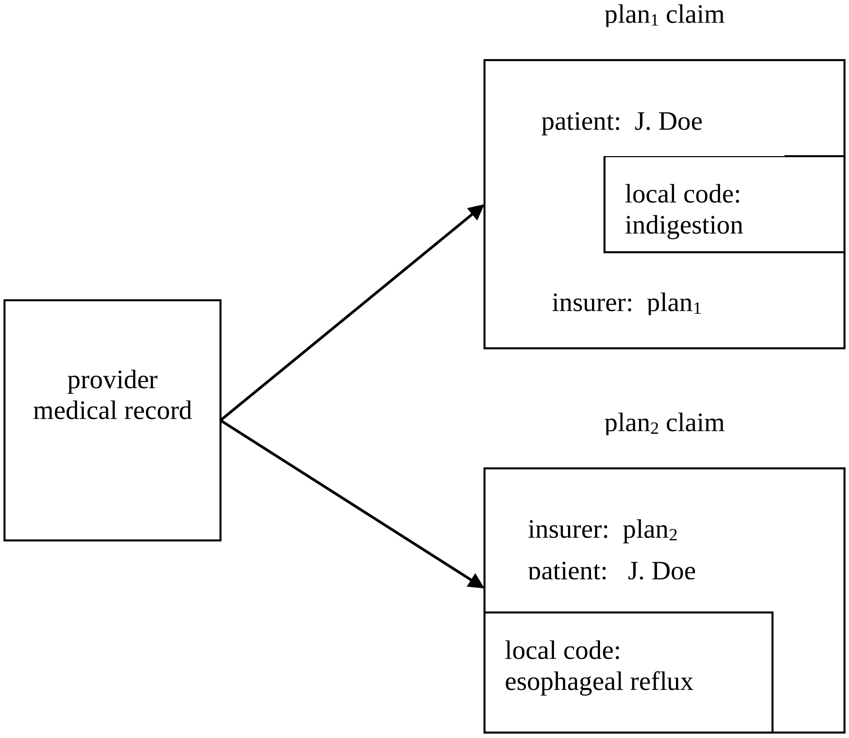


Figure "Provider to Plans": The provider has a medical record structure and coding scheme. Different health plans require the provider to translate information into formats and codes accepted by the different plans, illustrated here by plan$_1$ and plan$_2$. In the claims forms, fictitious local codes have been created for illustrative purposes only -- the intention is to show that two different codes might be required for the same diagnosis. The patient name is the same in both cases, but the plans require that information in different locations on their forms.

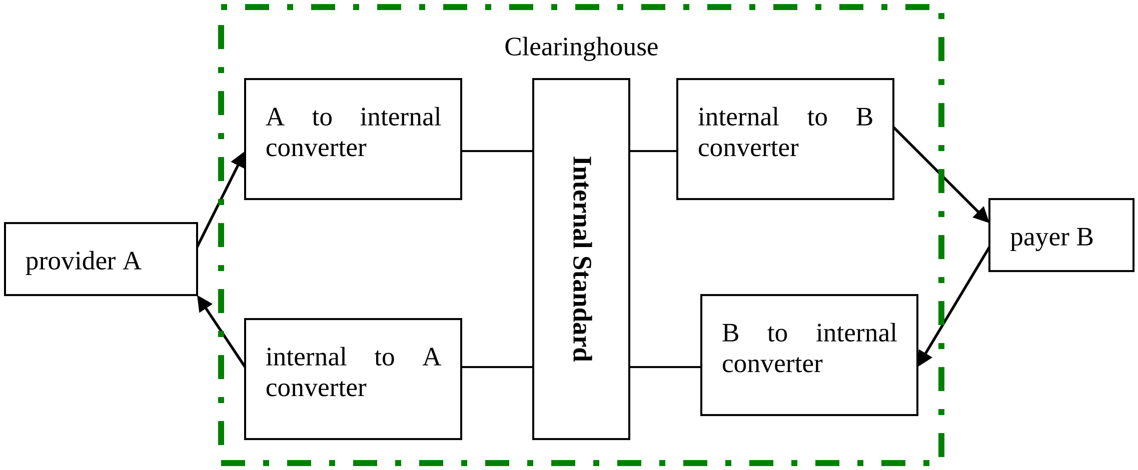


Figure "Internal Standard": Messages received in language A are translated into the internal standard and when sent to someone in language B have to be translated from the internal standard to B.

Furthermore, if one considers communication among plans or among providers, then the efforts required increase as follows:

- if the plans needed to communicate with one another when multiple plans were insuring the same patient, then 200 times (200-1) = 39,800 translators might be required among plans, and
- if providers need to share records, then 100 times (100-1) = 9,900 translators might be required among providers.

The total number of translators that might be needed is thus 20,000 + 39,800 + 9,900 = 69,700.

Providers often send claims to clearinghouses and let the clearinghouses deal with the translator challenges. A clearinghouse might develop its own, internal standard and translate every message into its internal standard. Then to send a message to another organization in a certain format, the clearinghouse needs to translate from its internal standard to that target format (see Figure "Internal Standard"). In this way the clearinghouse only needs *2 times n translators* instead of n times (n-1) translators. It needs a translator to take each format into its standard and another translator to translate its standard to each format.

An example from natural languages may help convey the impact of using an *internal standard*. If in a set of 4 people, the first only knows Russian, the second only knows English, the third only knows French, and the fourth only knows German, then the translation problem could be solved as follows:

- One translator hears Russian from the Russian speaker and translates into English for the English person, another translator hears Russian and translates into French for the French person, and a third translator hears Russian and translates into German for the German person. Continuing in this way, one gets 4 * 3 translators to go from each speaker to the target hearers,
- If, however, the translators agree a common intermediate language, then 4 translators are needed to get from each language into the common language and 4 translators to take from the common language into each target language for a total of 4 * 2 translators.

For the case of 4 languages, the common intermediate language allows a reduction from 12 to 8 translators. If, however, 400 languages exist, then this is a reduction from 400*399 to 400*2, which is substantial. On the other hand, for only 2 languages or standards, the intermediate language is a disadvantage because then one goes from 2*1 to 2*2 or from 2 converters to 4 converters. However, as soon as more than 3 languages or standards exist, then the advantage goes to the internal standard.

The experience with an internal standard is one step in the direction of reducing the costs of conversion. The ultimate reduction comes when everyone uses the same standard. When everyone communicates in a common language, then no translators are needed.

Agreeing to a single standard is not easy. In the case of natural language, people having been struggling for many, many years to agree to a standard. In Europe, such efforts as *Esperanto* were intended to standardize language across all European countries but the efforts have failed. For another example from natural language, the native language of Eskimos illustrates the importance of differences. The Eskimos have dozens of words for snow, whereas many languages have simply the single word snow. For Eskimos subtle variations in snow are so vital to their way of life that distinguishing each kind of snow is important. For the same reasons, providers and payers often argue for local codes that are unique to some geographical region. In healthcare situations, different organizations may have reasons to want different standards.

In 1993 the *Workgroup for Electronic Data Interchange* (WEDI) analyzed the financial impact of EDI standards in healthcare. WEDI used an extensive amount of information to develop its estimates, including data from a number of EDI pilot projects. The report included a number of electronic transactions that are not covered by HIPAA, such as materials management. The report projected implementation costs ranging between $5.3 billion and $17.3 billion and annual savings for the transactions covered by HIPAA ranging from $8.9 billion to $20.5 billion. In other words, WEDI projected decided financial benefits from transactions standardization. A 1995 study commissioned by the New Jersey Legislature estimated yearly savings of $760 million in New Jersey alone, related to EDI claims processing, reducing claims rejection, performing eligibility checks, decreasing accounts receivable, and other potential EDI applications.

The WEDI report assesses the savings from a totally EDI environment, which HIPAA does not mandate. Healthcare providers may still choose to conduct HIPAA transactions on paper. In addition, a significant amount of movement toward EDI has been made (especially in the claims area) in the last few years, and it is reasonable to assume that EDI would have continued to grow at some rate even

Figure “Practice Spreadsheet”: One enters whatever one wants into the ‘General Practice Information’ and ‘Amount of Time Spent to’ fields, then selects any ‘Yearly Cost Estimates’ to get an updated computation. To determine the savings from a reduction in bad debt, one enters the values for the current bad debt and the expected bad debt after automation in the next to last row, and then selects the last cell.

1. **General Practice Information (column a)**	**Your Data (column b)**	**Electronic (column c)**
2. Number of Visits Per Week	260	x
3. Average Claim Value ($)	191	x
4. Number of Visits with Insurance per week	215	x
5. Staff Cost per hour ($/hr)	14	x
6. Average number of eligibility checks in a week	33	x
7. Average number of claim follow-ups in a week	44	x
8. Average number of referrals in a week	25	x
9. **Amount of time spent to (minutes)**		
10. Obtain eligibility on a patient	11	0.5
11. Prepare a claim	6	0.5
12. Post a Payment	11	0.5
13. Obtain status of a claim	18	0.5
14. Referral check	13	2
15. **Yearly Cost Estimates**		
16. Eligibility Verification	$4,404.40	$ 200.20
17.Claims Preparation	$15,652.00	$1,304.33
18. Account Posting	$28,695.33	$1,304.33
19. Claim Status Follow-up	$9,609.60	$ 266.93
20. Referral Prepared	$3,943.33	$ 606.67
21. **Total Estimated Yearly Costs**	**$62,304.66**	**$3,682.46**
22. **POTENTIAL YEARLY SAVINGS**	**$58,622.20**	
23. To look at the impact of reducing bad debt on your practice, enter your overall level of bad debt into the cell below in the first column. Then, enter a guess as to your bad debt after you were to do more eligibility inquiries, claim status inquiries, and referral checks. Enter that figure in the white cell below in the second column. Bad debt expense 5%=0.05.		
0.10	0.05	
25. Increase in Potential Profits –Yearly ($)	$106,769.00	

without HIPAA. Thus, the influence of HIPAA is difficult to disentangle from the influence of other factors.

2.6.2 Ecommerce for Small Provider

This section looks at the small group physician practice as an illustration of the two basic advantages of ecommerce, reduction in labor costs and increased cash flow:

- Ten minutes on the phone to check eligibility compared to six seconds electronically adds up.
- Electronic submission offers the potential for automatic error checking, so that clean claims can be sent out the first time. Payment will be delayed until the clean claims are submitted and processed.

With faster, more accurate eligibility inquiries and claims, the number of denied claims could be reduced significantly and impact the gross proceeds of the practice on an annual basis to the tune of hundreds of thousands of dollars.

The calculation basics are illustrated in a few lines of data:

1. Number of claims per week: 215
2. Average claim value: $191
3. Time to prepare a manual claim: 6 minutes
4. Time to prepare an electronic claim: 0.5 minutes
5. Staff cost per hour: $14
6. Manual cost per year: #1 * #3 * #5 * (1 hr/60 min) * (52 wks/yr) = $15,652.
7. Electronic cost per year: #1 * #4 * #5 * (1 hr/60 min) * (52 wks/yr) = $1,304.
8. Labor saving is #6 - #7 = $14,348.
9. Bad debt now: 10 %
10. Bad debt after automation: 5%
11. Annual savings from debt change: #1 * #2 * (#9 - #10) * (52 wks/yr) = $106,769.

This labor savings from automation is about $14,000. The savings from bad debt reduction is about $105,000 (see Figure "Practice Spreadsheet" for details).

2.6.3 350-Bed Hospitals

The impact of standardization on the operation of a hospital (a typical 350-bed hospital) is viewed for the eligibility and the claims inquiry and then summarized (Brutscher, 2001).

2.6.3.1 Eligibility (270/271)

The *270/271* for verifying patient coverage tends to require more data, such as more detailed benefit information than what providers had been using. These new data requirements necessitate changes in the information collection process with physicians and clinical departments. Forms and screens used by schedulers, pre-registration personnel, and physicians who refer patients must be modified.

A typical 350-bed hospital has 5 financial eligibility employees involved in the verification process. This staff normally verifies coverage for 250 visits or admissions daily. Approximately 100 per day require telephone calls for *payer verification*. The average electronic verification takes 90 seconds, while the average verification by telephone call takes 600 seconds. Based on these statistics, the facility will save approximately one-and-a-quarter FTEs by fully implementing this transaction standard with all payers. This FTE could be used to expand the pre-registration function to help a provider verify coverage on more services and address coverage issues or deductibles with the patient before the visit or admission. Expanding pre-registration contributes to reductions in claim denials and bad debts.

2.6.3.2 Claims Inquiry (276/277)

The 276 Transaction is a claims inquiry from a provider, and the 277 Transaction is the response by the payer. Some of this claims status inquiry is done through clearinghouses and some on the telephone. The *276/277 Transactions* will help providers develop systems that can automate significant portions of the follow-up process and dramatically affect patient accounting.

Rules tables should be set up to submit the 276 transactions to the payers at certain intervals. The 276 inquiries will result in receipt of a 277 from the payer. The response contains coding that identifies the status of the claim:

- Some responses will indicate that payment has been made on the account.
- Others indicate the claim is pending receipt of additional information.
- While others will indicate a denial.

Providers will be able to automate resubmission of some claims based on the nature of the response from the payer.

- Some responses will require no additional follow-up from the provider.
- Other claims will need to be loaded into a work queue for review by a staff member. For example, 277 responses that indicate there is no claim on file can be automated in the system to transmit a new claim to that payer.
- Responses that show the claim has been paid will create a note in the system indicating the account needs no follow-up.

Patient accounts management will need to establish rules for each inquiry response. Effectively structuring these rules will determine how much

Type of Plan	**Number of Plans**	**% EDI**	**Cost in millions $**	**Savings in millions $**
Large commercials	250	.90	350	620
Smaller commercials	400	.50	200	354
Blue Cross/ Blue Shield	75	.90	106	188
Third-party administered	750	.50	375	665
HMO/PPO	1,500	.50	375	665
Self- administered	16,000	.25	600	1,063
Other employer plans	3,900,000	.00	195	345
TOTAL			2,201	3,900

Table "Health Plan Impact": Cost in millions and savings in millions but 'number of plans' is direct number. % EDI indicates the percent of activity at that kind of entity that is done electronically now.

facilities will benefit from this particular transaction. The Information Systems Department will need to work with the Patient Accounting Department to input the rules. They will also help test these rules and provide ongoing updates to the structure.

A typical 350-bed hospital has eleven personnel doing follow-up on outstanding accounts. Experience suggests that approximately 25 percent of the *follow-up activity* could be automated by rules on a computer accessing the claim and other information. This could reduce the FTE needs of the accounting department by 25 percent – namely, a saving of 3 FTEs.

2.6.3.3 Financial Impact

The overall staff reductions could be about 8 FTE (see Table "Review of FTE Reductions"). If 2 of these 8 staff savings are allocated to further collection of payments, 6 FTE reductions result.

Table "Review of FTE Reductions": Data based on hypothetical 350-bed hospital.

Area	Current FTE	Future FTE
Authorization (278)	5	3
Eligibility (270/271)	5	4
Billing (837)	5	4
Claim Inquiry (276/277)	11	8
Cash Posting (835)	3	2
Total	29	21

The savings that might accrue to the hospital then could be summarized as follows:

- Personnel: If 6 FTEs are eliminated and the average salary plus benefits is $40,000 per FTE, this would mean a saving of $240,000.

Table "Savings": Savings at 350-bed Hospital after standardization and automation.

Personnel	$240,000
Bad debt reduction	$2,500,000
Authorization Write-off	$500,000
Total	$3,240,000

- Bad Debt Reductions: If 20% of bad debt results from poor registration data, then shifting personnel to doing more pre-registration should reduce this number. If the current bad debt percentage is 5 percent, after better pre-registration this could become 4%. If the annual revenue of the hospital were $250 million, then this bad debt reduction would save the hospital $2.5 million per year.
- Authorization and other write-offs: The average hospital of this size writes off $1 million of its revenue due to authorization and timely filing issues. This could be reduced by 50 percent upon implementing the standards and thus save the hospital $500,000 per year.

This sums to over $3.2 million (see Table "Savings") without considering other benefits, such as reduced costs for paper bills and mailing of statements to patients.

2.6.4 Provider/Payer Cost/Benefit

The costs to providers and payers include the cost of upgrading software. The benefits include the decrease in per transaction overheads.

2.6.4.1 Software Costs

Healthcare providers and plans incur costs to convert existing software to utilize the standards. Health plans and large healthcare providers generally have

Type of Provider	**Number of Providers**	**Average Cost**	**% EDI**	**Total Cost (in Millions)**	**Savings (in Millions)**
Hospitals <100 beds	2,850	$100,000	.86	$ 388	$ 369
Hospitals 100+ beds	3,150	250,000	.86	1,071	1,019
Nursing facility <100 beds	27,351	10,000	.50	274	260
Nursing facility 100+ beds	8,369	20,000	.50	167	159
Home health agency	10,608	10,000	.75	133	126
Hospice	1,191	10,000	.10	7	7
Dialysis facility	1,211	10,000	.75	15	14
Specialty outpatient	7,175	10,000	.75	90	85
Pharmacy	70,100	4,000	.85	379	360
Medical labs	9,000	4,000	.85	49	46
Dental labs	8,000	1,500	.50	12	11
Durable Medical Equipment	116,800	1,500	.50	175	167
Physicians solo and groups <3	337,000	1,500	.20	354	337
Physicians groups 3+ with mainframe	17,000	8,000	.75	170	162
Physicians groups 3+ with PCs	15,000	4,000	.40	54	51
Physicians groups 3+ no automation	2,000	0	.00	0	0
Osteopaths	35,600	1,500	.10	32	30
Dentists	147,000	1,500	.14	141	134
Podiatrists	8,400	1,500	.05	7	6
Chiropractors	29,000	1,500	.05	24	23
Optometrists	18,200	1,500	.05	14	14
Other professionals	23,600	1,500	.05	20	19
TOTAL				$3,574	$3,400

Table “Provider Impact”: Healthcare Provider Implementation Costs and Savings (in Millions) over 5 years.

their own information systems, which they maintain with in-house or contract support. Small healthcare providers are more likely to use off-the-shelf software developed and maintained by a vendor. Examples of *software changes* include the ability to generate and accept transactions using the standard and converting or cross-walking current provider files and medical code sets to chosen standards. However, healthcare providers have considerable flexibility in determining how and when to accomplish these changes. One alternative to a complete system redesign would be to purchase a translator that reformats existing system outputs into standard transaction formats. A health plan or healthcare provider could also decide to implement two or more related standards at once or to implement one or more standards during a software upgrade. Adopting the approach to suit the situation will reduce cost.

The Tables “Health Plan Impact” and “Provider Impact” illustrate the costs for health plans and healthcare providers to implement the standards and the savings that will occur over time as a result of the HIPAA administrative simplification provisions. All estimates are stated in 1998 dollars. The costs are based on estimates for the cost of a moderately complex set of software upgrades. The *range of costs* that health plans and healthcare providers will incur is quite large and is based on such factors as the size and complexity of the existing systems, ability to implement using existing low-cost translator software, and reliance on healthcare clearinghouses to create standard transactions. The cost of a moderately complex upgrade represents a reasonable midpoint in this range. In addition, health plans and healthcare providers with existing EDI systems will incur implementation costs related to *manual operations* to make those processes compatible with the EDI systems. For example, manual processes may be converted to recognize standard identifiers or to produce paper remittance advices that contain the same data elements as the EDI standard transaction. Those costs are estimated to be equal to 50 percent of the upgrade cost.

2.6.4.2 Savings

The savings per claim processed electronically instead of manually is

- *$1 per claim* for health plans and physicians, and
- $.75 per claim for hospitals and other healthcare providers.

Savings are expected from simplifications in manual claims and are *ten percent* (per transaction) of those that are projected for conversion to electronic billing.

Table “Provider Impact” illustrates the costs and savings attributable to various types of healthcare providers. Estimated percentages of EDI billing are based on the 1997 edition of Faulkner & Gray’s Health Data Directory or are actuarial estimates. The $3.4 billion in savings represents savings to healthcare providers for the first five years of implementation. This provides a sense of how the HIPAA administrative simplification provisions would affect various entities. As in Table “Health Plan Impact”, the savings have been apportioned to each type of healthcare provider based on the ratio of the cost for that entity type to the cost of all healthcare providers.

Savings are almost twice cost for payers, but costs exceed savings for providers. This discrepancy in the costs versus the savings may account in part for the strong support for the HIPAA Transaction Rule from payers and the relative resistance from providers.

The proportion of claims that would be processed electronically without HIPAA is assumed to grow at a similar rate from 1998 through 2002 as it did from 1992 to 1996. The increase in EDI transactions from providers attributable to HIPAA is highly uncertain but is critical to the *savings estimate*. Because the rate of growth in electronic billing is already high, there is not much room for added growth (see Table “Growth in EDI Claims”).

Table “Five-Year Net Savings” shows the annual costs, savings, and net savings over a five-year implementation period. Much of the cost will be incurred within the first three years, since the statute requires health plans other than small health plans to implement within 24 months. As each health plan implements a standard, healthcare providers that conduct electronic transactions with that health plan would also implement the standard. No savings accrue in the first year, because not enough health plans and healthcare providers would have implemented the standards. Savings would increase as more health plans and healthcare providers implement. By the fourth year, the majority of health plans and healthcare providers should have implemented the standards, and costs should decrease and benefits increase as a result.

2.6.5 Third-Party Vendors

Many healthcare providers use billing agents or claims clearinghouses to facilitate EDI. Those entities would also have to reprogram to accommodate standards. Clearinghouses could initially most benefit from standardization, but in the long run clearinghouses need to diversify their business models because standardization should facilitate providers and payers directly communicating.

The Health Data Dictionary (Peters, 1997) lists 100 third-party claims processors. Third-party claims processors are:

- clearinghouses that take electronic and paper healthcare claims data from healthcare providers and
- billing companies that prepare bills on a healthcare provider’s behalf.

The third party claims processor acts as a conduit to

% Growth in EDI Claims Attributable to HIPAA

Type of Provider	Yr 1	Yr 2	Yr 3	Yr 4	Yr 5
Physician:					
% before HIPAA % after HIPAA Difference	45% 45 --	50% 52 2	55% 59 4	60% 66 6	65% 73 8
Hospital:					
% before HIPAA % after HIPAA Difference	86% 86 --	87% 88 1	88% 89 1	89% 91 2	90% 92 2
Other:					
% before HIPAA % after HIPAA Difference	75% 75 --	76% 78 2	77% 81 4	78% 84 6	79% 87 8

Table “Growth in EDI Claims”: This table was originally done with year 1 being 1998.

health plans; it batches claims and routes transactions to the appropriate health plan in a form that expedites payment. Seven third-party processors handled more than 20 million electronic transactions per month.

A *billing company* works primarily with physicians either in office or hospital-based settings. Billing companies, in effect, take over the office administrative functions for a physician; they take information such as copies of medical notes and records and prepare claim forms that are then forwarded to an insurer for payment. Billing companies may also handle the receipt of payments, including posting payment to the patient's record on behalf of the healthcare provider. They can be located within or outside of the physician's practice setting. The International Billing Association is a trade association representing billing companies. The International Billing Association estimated that there are approximately *4500 billing companies* currently in business in the United States.

Software system vendors provide computer software applications support to healthcare clearinghouses, billing companies, and healthcare providers. They particularly work with healthcare providers' practice management and health information systems. These businesses provide integrated software applications for such services as accounts receivable management, electronic claims submission (patient billing), record keeping, patient charting, practice analysis and patient scheduling. Some *software vendors* are also involved in providing applications for translating paper and nonstandard computer documents into standardized formats that are acceptable to health plans. The Health Data Dictionary (Peters, 1997) lists

- 104 physician practice management vendors and suppliers,
- 105 hospital information systems vendors and suppliers,
- 134 software vendors and suppliers for claims-related transactions, and
- 28 translation vendors.

Software vendors would be affected positively in the short term. The implementation of administrative simplification would enhance their business opportunities as they would be involved in developing computerized software solutions that would allow for healthcare providers and other entities that exchange healthcare data to integrate the new transaction set into their existing systems. They may also be involved in developing software solutions to manage the crosswalk of existing healthcare provider and health plan identifiers to the national provider identifier and health plan identifier until such time as all entities have implemented the identifiers.

Competition among healthcare clearinghouses and billing companies will increase over time. Threats and opportunities include:

- Standards will reduce some of the technical limitations that currently inhibit healthcare providers from conducting their own EDI. For example, by eliminating the requirement to maintain several different claims standards for different trading partners, healthcare providers will be able to more easily link themselves directly to health plans. This could *threaten* the market for healthcare clearinghouses and system vendors that do translation services.
- Standards should increase the efficiency in healthcare clearinghouses by allowing them to more easily link to multiple health plans. The

Five-Year Net Savings (in Billions of Dollars)

Costs and Savings	Yr 1	Yr 2	Yr 3	Yr 4	Yr 5	Total
Costs:						
Provider	1.3	1.3	1.1	0.0	0.0	3.6
Plan	0.8	0.8	0.7	0.0	0.0	2.2
Total	2.0	2.0	1.7	0.0	0.0	5.8
Savings from Claims Processing:						
Provider	0.0	0.1	0.3	0.4	0.6	1.4
Plan	0.0	0.1	0.2	0.4	0.5	1.2
Total	0.0	0.2	0.5	0.8	1.1	2.6
Savings from Other Transactions:						
Provider	0.0	0.2	0.4	0.7	1.1	2.4
Plan	0.0	0.2	0.4	0.6	0.8	2.0
Total	0.0	0.3	0.8	1.2	1.8	4.1
Savings from Manual Transactions:						
Provider	0.0	0.0	0.1	0.1	0.1	0.3
Plan	0.0	0.0	0.1	0.1	0.1	0.3
Total	0.0	0.1	0.1	0.2	0.2	0.6
Total Savings:						
Provider	0.0	0.3	0.6	1.0	1.5	3.4
Plan	0.0	0.3	0.7	1.2	1.6	3.9
Total	0.0	0.6	1.4	2.2	3.1	7.3
Net:						
Provider	(1.3)	(1.0)	(0.5)	1.0	1.5	(0.2)
Plan	(0.8)	(0.5)	0.0	1.2	1.6	1.7
Total	(2.0)	(1.4)	(0.3)	2.2	3.1	1.5

Table "Five-Year Net Savings": Again year 1 was 1998 in the computations.

increased efficiency in operations resulting from standards could, in effect, lower their overhead costs as well as attract new healthcare clearinghouse *opportunities* to offset any loss in market share that they might experience.

Another potential area of change is through *standardized code sets*. These standards may also lower costs and logistical barriers that discouraged some healthcare providers from doing their own coding and billing. As a result, some healthcare providers may choose an in-house transaction system rather than using a billing company as a means of exercising more control over information.

Healthcare clearinghouses may be able to operate more efficiently or at a lower cost based on their ability to gain market share. Some small billing companies may be consumed by healthcare clearinghouses that may begin offering billing services to augment their healthcare clearinghouse activities. However, many healthcare providers that use billing companies would probably continue to do so because of the comprehensive and personalized services these companies offer.

2.6.6 Qualitative Impacts

In addition to dollar savings, administration simplification produces *qualitative benefits*. WEDI suggests in its 1993 report that there will be a 'ripple-effect' of implementing an EDI infrastructure on the whole healthcare delivery system in that there would be a reduction in duplicate medical procedures and processes as a patient is handled by a continuum of healthcare providers during an episode of care. Administrative simplification promotes accuracy, reliability, and usefulness of the information shared.

The transaction formats enable patient financial service employees to educate patients about their coverage and negotiate with patients to develop strategies for resolving *out-of-pocket payments* (Gustafson, 2000). The result should be enhanced cash flow, reduced bad debt, and improved patient satisfaction.

The hundreds of different formats for claims transactions make it difficult for parties to exchange information electronically. At a minimum, it requires data to be translated from the sender's own format to the different formats specified by each intended receiver. Also, different approaches to uniquely identifying patients, healthcare providers and health plans make it difficult to compare services across healthcare providers and health plans. Standards will improve the ability to share information and deliver *quality care*.

The '837' format eliminates many nonstandard, local payer formats by standardizing the providers' and payers' claim submission and transfer processes (DISA, 2000). As a result, claims can be edited more effectively throughout the revenue cycle. Under the new format, erroneous data will be flagged automatically, allowing the patient financial services staff who collected the data to resolve the problems quickly without contacting and potentially upsetting patients at a later time, and thus also eliminating the need for post-service billing staff. Moreover, claims posing problems or involving exceptions will be easier to identify. The 837 enables payers to accelerate payment cycles.

By making all claims data available in a standard format, the '837' is expected to enhance payers' *fraud prevention* efforts. Government payers will be able to increase automatic claims screening, commercial payers will have easy access to historical claims and clinical data to more easily identify bogus injury and disability claims, and pharmacy management organizations will be able to screen more effectively for over-prescribing patterns and medication errors.

In addition, payers will be able to use the data included in the '837' to coordinate the processing of claims for patients with *multiple benefit plans*. Using the claims data set and the uniform health plan and provider identification numbers, payers will be able to automate coordination-of-benefits identification and claims processing without the need for additional contacts with providers and patients or policyholders. Time-consuming and costly manual efforts will be reduced for both providers and payers, and patients will receive clear information on their account status, thereby alleviating patient confusion and minimizing inquiries.

2.6.7 Review Questions

1. If 200 different standards for transactions existed, then how many translators would be needed. Show your reasoning. Explain the significance of this number relative to the number that would be needed, if only one standard is used.
2. What do the cost analyses show as the costs to health plans versus the costs to healthcare providers?
3. How many third-party healthcare claims vendors are there? What is the likely impact of HIPAA transaction standardization on them?
4. What qualitative impacts might accrue from EDI standards?

2.7 Implementation

Main Points

- The transactions are difficult to implement at one time and thus a sequencing schedule has been proposed.
- Testing that transactions are compliant is facilitated by a third-party certification service.
- The Administrative Simplification Compliance Act passed in December 2001 allows covered entities to submit a plan for how they will become compliant and thus earn a 1-year delay in the original compliance deadline.
- Providers need to assess their transaction status before choosing an implementation approach.
- Clearinghouses give providers a rapid start-up solution, but internal integration of a solution might facilitate long-term cost savings for a healthcare provider.

Implementing the HIPAA Transactions and Code Sets involves a massive national transformation. Not only must the workings within an organization be modified, but the workings among organizations have to change. Coordinating such a change calls for massive communication and decision-making at all levels.

2.7.1 Who is Doing What?

Payers and complex organizations (payer and provider in one) are expected to spend the most money on implementing changes to accommodate the HIPAA Transactions requirements (WEDI, 2001). The payers have to change their algorithms for adjudicating claims as the information in the claims has changed. Some payers, especially in the state Medicaid programs, will require new systems, because enhancing their existing systems may not be practical. For the states, this is further exasperated by the need to get funding from the states to make these acquisitions.

Providers expect changes to come from their vendors as part of their maintenance agreements or as part of enhancements that vendors offer. In addition, the unique payer identifiers and elimination of local codes will simplify their systems and many will not have to make changes to accommodate these modifications. On the other hand, the transactions will require that new data be collected for some transactions that were not previously collected. This will require database modifications and logic to collect and maintain the information.

Complex organizations have the worst of both worlds. Health plans and complex organizations are remediating based on internal efforts and translators. Providers are mixed between external solutions (vendors or clearinghouses) and internal remediation.

Vendors and clearinghouses will help other organizations remediate. For their internal use, vendors and clearinghouses will depend on their own resources.

2.7.2 Sequencing

Implementing each transaction will require time to analyze the

- systems involved,
- data content required, and
- system implications associated with collecting and maintaining new data, using new identifiers, and using new code sets.

Setting up each transaction will require testing and certification at many levels.

The transactions should be implemented in steps -- the "Big Bang" approach should be avoided. To allow effective use of resources and a method to move forward in small, controllable steps, a transaction schedule is proposed (WEDI, 2001). The sequencing allows the industry time to implement and test one or a few transactions at a time. For example, the claim and claim payment transactions are grouped together, because these two transactions will depend on data requirements from the other.

The WEDI-SNIP proposal identifies three significant implementation timeframes:

- In the Pilot Testing phase, a health plan would conduct pilot testing with a few selected providers.
- In the Health Plan Readiness phase, health plans begin accepting production HIPAA transactions from willing trading partners. This will begin the transition process, moving providers from the old formats to the new X12 transactions. During this phase, prior to accepting transactions in production, each trading partner would be expected to perform some initial testing to verify each entity is sending and receiving transactions properly. During this time health plans will continue to support current processes, until the transition is complete for all their customers.
- In the Migration Completion phase, all covered entities must complete their conversion to the HIPAA transaction standards.

Table "Deployment Sequence and Implementation Schedule": Groups in the columns and phases in the rows. This plan is the January 2002 one from WEDI-SNIP to go through October 2003 per the Administrative Simplification Compliance Act. Month 1 was April 2002 and Month 18 was October 2003.

Transactions in each Group	Group 1 837 and 835	Group 2 270/271 and 834	Group 3 276/277	Group 4 278	Group 5 820
Pilot Testing Start Dates	Month 1	Month 4	Month 7	Month 10	Month 12
Health Plan Readiness Start	Month 3	Month 6	Month 9	Month 12	Month 15
Migration Completion	Month 18	Month 18	Month 18	Month 18	Month 18

A table has been produced to give each transaction in each phase of implementation (see Table "Deployment Sequence and Implementation Schedule"). Factors that determined the schedule included:

- Implementing complex transactions may take longer (i.e., claims) than simple transactions, therefore complex transactions are early.
- Some transactions will have a positive impact on providers, reducing costs, improving efficiency, and improving core business processing. This coupled with what is believed to be a relatively easy development and implementation led to the decision to deploy the 270/271 transactions early in the schedule.
- Pilot availability due to mission-critical business events (i.e., open enrollment for health plans) led to an early deployment of the 834 transaction.

Converting to the new clinical code sets at the same time as converting to the X12 transaction may not be possible. Local codes may not translate easily to the new national code sets. While the transition from the current transaction to the new transaction occurs, not all transactions will be implemented for a provider or a health plan at the same time. Therefore, the new code sets cannot be utilized for those transactions not yet converted; leaving the requirement to translate between old and new code sets. This could prove unsupportable, if a one-to-one mapping between the old and new code sets is not practical.

2.7.3 Certification

Each organization will have to test internally that they are producing valid transactions that are meeting the specification requirements found in the X12N Implementation Guides. This process will require

- internal quality assurance testing,
- testing with a certification entity, and then
- additional assurance testing with selected trading partners.

Each organization will want to perform testing with each of its trading partners to verify that they

- are meeting the unique situational requirements that may exist between each trading partner and
- all coding decisions are consistent with each entity's interpretation of what is required.

Trading partner level testing will also insure that connections are working properly, security is working properly, and other submission requirements are being satisfied as required by each entity.

Health plans must test the standard transactions with a large number of submitters, and providers must test with all their health plans. This testing could overwhelm both health plans and providers. A third-party certification could reduce the cost of testing.

The different levels of testing within transaction certification systems include (WEDI, 2001a):

- Level 1: Integrity testing – validation of X12 syntax, and compliance with X12 rules.
- Level 2: Requirement testing – Testing for HIPAA implementation guide-specific requirements, such as repeat counts and used codes.
- Level 3: Balancing – Testing the transaction for balanced field totals, such as financial balancing of claims.
- Level 4: Situation testing – The testing of specific inter-segment situations. For example, if the claim is for an accident, the accident date must be present.
- Level 5: Code Set testing – Testing for valid code set values to make sure the usage is appropriate for any particular transaction.
- Level 6: Type of Service testing – Specialized testing is required by certain healthcare

specialties. For example, ambulance, chiropractic, podiatry, home health, nutrition, durable medical equipment, psychiatry, and other specialties have specific requirements that must be tested before putting the transaction in production.

This testing does not address the testing of the adjudication systems. These systems must be tested to ensure that data elements are not truncated or ignored, but such testing is outside the scope of the preceding 6-level certification.

2.7.4 One-Year Delay

The President signed into law at the end of December 2001 a Congressional Act entitled *Administrative Simplification Compliance Act*. The Act extended the deadline for compliance with the 'Transactions Rule' by one year, to Oct. 16, 2003, if covered entities submitted to federal officials a summary explaining how they would use the extra year to reach compliance.

The plan was expected to include:

- An analysis reflecting the extent to which, and the reasons why, the entity is not in compliance;
- A budget, schedule, work plan, and implementation strategy for achieving compliance;
- Whether the entity plans to use or might use a contractor or other vendor to assist in achieving compliance
- A timeframe for testing that begins not later than April 16, 2003

If an entity failed to submit a compliance plan or fails to be in compliance by October 16, 2002, the Centers for Medicare and Medicaid Services (CMS) would have the option of excluding the entity from participating in the Medicare plan. However, DHHS also said that no judgment will be made as to whether the plans are good or bad, but rather any submitted application automatically earned the submitter an extension. If an entity failed to submit a compliance plan or failed to be in compliance by October 16, 2002, the Centers for Medicare and Medicaid Services (CMS) would have the option of excluding the entity from participating in the Medicare plan.

In March 2002, DHHS released an application form which is 600-words long. The entity simply completes 26 multiple choice or fill-in-the-blank questions. The first question is a fill-in-the-blank and is:

"1. Name of Covered Entity: ______"

The tenth question asks for the reason for the delay:

10. Please check the reason(s) that your organization will not be in compliance with the HIPAA standard for Electronic Transactions and Code Sets by October 16, 2002. Multiple boxes may be checked.

Need more money
Need more staff
Need to buy hardware
Need more information about the standards
Waiting for vendor(s) to provide software
Need more time to complete implementation
Waiting for clearinghouse/billing service to update my system
Need more time for testing
Problems implementing code set changes
Problems completing additional data requirements
Need additional clarification on standards
Other

DHHS also said that no judgment will be made as to whether the answers are good or bad, but rather any submitted application automatically earns the submitter an extension.

The Act does not require electronic transmission of claims and related transactions, with one exception. The bill requires most Medicare claims be submitted electronically and lists limited exclusions.

The Act is also significant because it includes authorization to appropriate $44.2 million to the Department of Health and Human Services for implementation of HIPAA's Administrative Simplification provisions. Further, the National Committee on Vital and Health Statistics is to do an analysis of a sample of compliance plans and produce a report containing effective compliance solutions.

2.7.5 Provider Approach

The effective use of a tool in change management involves

- business and technology architecture and
- organizational change.

These solutions depend heavily on existing information and processes in the organization, and due to their disruptive nature are not practical to integrate into current workflows without some level of business process redesign.

2.7.5.1 Planning Documents

The first step in implementing the Transactions Rule is the establishment of a Project Management Office.

The Project Management Office coordinates documentation activities and initiates change management throughout the organization. This Office houses five roles that together design and implement the organizational change (see Table "Roles and Responsibilities of Transactions Project Management Office").

Assessment of transaction options may be different for providers, clearinghouses, and providers. The Provider Project Management Office should develop these inventories (Rada, et al, 2002):

1. 'Impacted Application' by Application/ Vendor/ Department/ Application Use/ Priority Ranking
2. 'Transaction Requirements' by Business Area/ Application/ Vendor/ Transaction/ Upgrade Availability
3. Clearinghouse and Payer Abilities' by X12 transactions/ anticipated date of transaction acceptance/ partner contact information/ messaging options.

Based on these inventories, the Office should determine the technical capabilities of systems to support HIPAA-related transactions. The next steps are:

1. Mapping of transactions to X12 standards to support future field-by-field conversion and to establish required and recommended fields to actively pursue with payers.
2. Identification of protected health information data elements by application or department that generates the data element.

The 'mapping of transactions to X12 standards' delineates each unique field, whether the field is fixed or optional, and its relative value to an organization. Fields are usually populated with sample data elements. In addition, the value of capturing additional or optional data elements should be addressed with business office personnel. Consultants have a set of recommended elements that are a part of a 'best practice' approach to implementing the HIPAA Transactions.

Table "Roles and Responsibilities of Transactions Project Management Office"

Role	Responsibilities
project manager	organizational change
information systems manager	information systems architecture
operations manager	claims, eligibility, referral and patient accounting
business office expert	document current workflows and new workflows for automated solution
human resource representative	recruit people for new roles and train these people

Finally, financial and staffing plans are made and involve a:

1. 'return on investment' analysis of automation affects and
2. 'current versus future workflow' map to delineate affected staff within targeted departments.

For the 'Return on Investment' analysis, a semi-automated tool may help a provider evaluate the revenue enhancement and cost reduction opportunity in automating the transactions. The entity first collects data about net revenue, claim volume, current ratios of electronic and manual processes, and current staffing numbers. The data collected are validated through interviews with the Director of Patient Accounts and Director of Registration Services. The tool will then show for each X12 transaction standard:

- Reduced write-offs,
- Interest on accelerated payment,
- Reduced re-work,
- Reduced time per transaction, and
- One-time cash acceleration.

This output facilitates the prioritization and sequencing of the rollout by payer and transaction.

2.7.5.2 Connectivity Options

From the provider perspective, there are three basic components of transactions with payers:

1. Translation of the transaction from the format produced in the provider's system to a HIPAA compliant transaction.
2. Transmission of the transaction to the payer.
3. Translation of the payer response into a format the provider's core systems can understand.

Providers will have to decide from the following connectivity options which approach is best suited to its needs.

The four main provider-health plan connectivity models are the collaborative, the clearinghouse, the payer-specific, and the internal integration (Hebert, 2001):

- In the collaborative model**,** providers and health plans agree to participate in a consortium with set HIPAA standards for data exchange. Start-up cost is usually low, and expenses are equally shared across the business partners within the consortium. An example of a collaborative commerce model is the New England Healthcare EDI Network (NEHEN). If a collaborative commerce model already exists in the entity's market and fulfills its connectivity requirements with 80% of its payers, this option should produce the quickest and most positive results.

- In the clearinghouse model, providers send all transactions through a clearinghouse, which converts the data into the acceptable HIPAA compliant formats for each respective health plan. The clearinghouse approach is the predominant approach utilized by providers. While easy to implement, long-term costs can be substantial. Clearinghouses usually charge on a per transaction basis and may also have an annual membership fee and start-up fees. In addition, response time is often too slow to undertake real-time validation of eligibility. Examples of clearinghouses include WebMD and MedUnite.
- In the payer-specific model**,** a payer offers its own unique solutions by which providers can directly connect. The access devices employ swipe cards, dummy terminals, or interactive voice recognition and have a tendency to be expensive and add additional steps to the patient registration and billing process. Other drawbacks include that providers must support multiple systems and must require registration or billing staff to re-key the information into their own source systems.
- In the internal integration model**,** providers utilize enterprise application integration (EAI) solutions to wrap their application infrastructure within an EAI environment. The EAI architecture will support messaging to and from payers in EDI, XML, and other formats within the EDI gateway. The gateway will support the aggregation, transformation and transliteration of incoming and outgoing data packets into acceptable messaging formats for storage within a provider's logical application environment. The EAI is sometimes not as cost effective as other models depending on a provider's transaction volumes but allows for the greatest amount of integration. In an ideal internally integrated solution, the transaction would flow seamlessly from the provider's legacy system to the payer's system and back again with no human intervention or re-keying.

The potential for Return-on-Investment is limited by the amount of integration a provider is willing to undertake. Providers must assess their current technical and business infrastructure against available connectivity options to determine the level of integration and implementation costs their organization can sustain to reduce costs and increase revenues.

If consortia and single-payer models are not a viable option, clearinghouse options may be the quickest and easiest to implement. However, each encounter with a patient will generate five transactions at a fixed cost per transaction, and each patient will return approximately three times. Thus, the overall processing cost per patient must be tripled across all five transactions. On the other hand, the first-year cost to implement an internal solution would be depreciated over time as part of asset management. The key decision is what level of integration can an entity sustain, not what method of connectivity will it acquire. Integration drives the level of efficiency and impact on revenue cycle outcomes.

2.7.6 Case Studies

Understanding how entities are implementing compliance with the transactions rule is aided by studying examples of what specific entities are doing. To that end, this subsection provides two case studies.

2.7.6.1 John Muir/Mt Diablo

John Muir/Mt Diablo Health System is a not-for-profit, multi-entity, integrated health system in the San Francisco Bay Area. It includes two acute care hospitals, a psychiatric hospital, a home health agency, ambulatory surgery centers, outreach laboratory services, several outpatient service entities, and a Health Maintenance Organization. Its HIPAA Transactions Project began with inventory and audit of transactions systems and manual processes. This assessment found fifteen applications that generate claims, but no other transactions (Halberg and Saff, 2002).

The HIPAA Project elected to centralize the EDI function rather than continue to have 15 separate applications performing this function. A *Central EDI Service* supports

- Claims batch load from the billing system,
- Claims editing and rejection,
- Aggregation of claims by payer for transmission,
- Transmission of claim batches to payers,
- Receipt of application acknowledgement, and
- Inventory and auto-tracking of sent claims.

Organizational responsibility for development and hosting was placed in Information Technology Services and is coordinated through the HIPAA Project Office. Organizational responsibility for the clinical editor application is in the Health System's Corporate Finance Department, and is managed by the business office. Responsibility for contact with payers and development of the trading partner agreements is shared between Finance and the Project Office. Operational responsibility for the data in claims remains with the individual business functions.

2.7.6.2 MEGA Life and Health

The *MEGA Life and Health Insurance Company* provides insurance (primarily health) to niche consumer and institutional markets. In 2000, the 500,000 people insured by *MEGA Life and Health Insurance Company* MEGA submitted more than two million claims, resulting in $300 million in paid benefits. MEGA says (HealthAxis, 2002):

> Even before the HIPAA deadline began to draw near, we were looking to EDI as a driver for automation and cost savings. We originally had this in our strategic plan as an 18 month project, to be completed in two phases: first becoming EDI-enabled, followed by an additional effort to achieve HIPAA transaction compliance. The [commercial translator software] for HIPAA enabled us to bring MEGA from paper-based processing to significant HIPAA transaction compliance in only ten weeks, and without any modifications to MEGA's existing mainframe claims processing systems.

The 10-week process went from envisioning to planning to development to deployment (see Table "MEGA Schedule").

Table "MEGA Schedule"

Weeks	Activity	Phase
1	Consultant Kick Off	Envisioning
2	Client Kick Off	Envisioning
3	Analysis	Planning
4-6	Mapping and Workflow	Development
7	Changes	Development
8	Testing	Development
9	Install Production System	Deployment
10	Sign Off	Deployment

The vision statement that resulted from the first two weeks was (Bass et al, 2002):

> Deploy translator software for HIPAA as key integration component, allowing for the client's claim system to accept and process X12 837 transaction sets. This Solution would then be utilized to deploy the remaining transaction sets into and out of the appropriate legacy systems.

The functional specification was that trading partners would send 837 transactions to the new gateway and the gateway would communicate with MEGA's legacy systems. The gateway in turn was designed as a 4-step process:

1. receive and save 837 transaction from trading partner
2. generate and send acknowledgement to trading partner
3. convert 837 to the common gateway internal format in an XML-marked-up representation
4. connect with the different workflows of the legacy system

One of the most difficult pieces of the project was the data mapping. The *legacy systems* were difficult to interpret. The second hardest part was representing the workflows around the legacy system and connecting that to the gateway. This involved a data warehouse, data mapping, maps to the imaging system, data enhancements, and maps to the claims adjudication system.

Finally, the project was put into full production mode. Some new equipment was installed. All production code was loaded and tested. MEGA then completed its own review and evaluation before *project sign-off*.

2.7.7 Review Questions

1. What types of organizations are likely to depend on vendors for their transactions compliance?
2. Why does the implementation of the transactions standards essentially require a sequencing strategy?
3. Relate the levels of certification to the technical characteristics of the X12 standards and the HIPAA Implementation Guides.
4. What are the roles in a Project Management Office for achieving compliance with the transactions standard?
5. Why is an enterprise application integration approach able to save a large organization money in the long-run?

2.8 Conclusion

Historically, a plethora of provider-payer forms have been used. This has contributed to an enormous overhead in administration in the healthcare system. For entities to agree to a standard and implement it is an enormous challenge.

2.8.1 Administrative Simplification

HIPAA's Administrative Simplification requires that DHHS adopt standards for transactions between providers and payers. These standards must include the format of the messages and the values that go into the fields in the forms. These values are codes sets and identifiers.

The government must use existing standards wherever practical. The intention is to build on and work with the private sector to adopt or adapt the standards favored by the marketplace. DHHS has devised various criteria to help assess the suitability of various standards and also engaged in numerous, consensus-building exchanges.

Standards are a dime a dozen but compliance with standards is precious. HIPAA has the force to select good standards and then to oblige entities to comply with the standards.

2.8.2 Transactions

Electronic Data Interchange (EDI) has been important for decades. The prominent American standards development organization for EDI is Accredited Standards Committee X12 (commonly referred to simply as X12). X12 specifies an envelope structure for messages. The information on the envelope is used in routing messages through the electronic networks. Various Committees of X12 work on implementation guides to specify in some detail how the content of the envelope might be standardized to carry information most useful to a given industry.

The Healthcare Task Force of the Insurance Committee of X12 has developed several *Implementation Guides* that DHHS has adopted as the standard for HIPAA transactions. These Implementation Guides cover:

- enrollments of individuals in health plans,
- eligibility inquiries,
- claim submissions, and
- payment advice.

For each Implementation Guide the transaction has a relatively simple hierarchical structure culminating in particular values from code sets or identifiers. The message is transmitted as a string of bits. X12 creates a language for authoring the message that people can understand and that is rigorous enough that a computer program can encode and transmit it and another computer program can receive and decode it.

Standardization of transactions has practical value:

- Forms with erroneous data will be readily recognized and returned to the sender to fix.
- Fraud surveillance will be facilitated.
- Claims that need to go to multiple health plans can be automatically routed.
- Eligibility inquiries should be readily answered automatically, and providers could thus avoid long delays and high costs of making eligibility inquiries by phone.

The list of benefits to standardized transactions is long.

Software exists for healthcare information systems that will generate the HIPAA transactions in the appropriate form. For systems that generate transactions in other than HIPAA-compliant forms, other software exists or must be created that will translate the information from the one format to the other.

Some *clearinghouses* have already implemented the X12 formats. Envoy is the largest clearinghouse, and its experiences with the transition from hundreds of different formats to one format reveal some of the challenges:

- The providers may not be prepared to provide some of the information required by the new forms and may want to continue providing some information that the new forms do not accept.
- The rules for transactions and code sets are final, but some necessary identifiers have not been finalized. Awkward temporary measures need to be invoked while waiting for the final ruling about the identifier from DHHS.

These problems should, however, be short-term.

2.8.3 Codes

A key component of the values to put into the fields of the transactions are the codes. A code is a representation assigned to a term, and a listing of terms and their associated codes is a code set. Examples of code sets include

- the simple code set for sex of M for Male or F for Female and
- the complex code set for diseases of the International Classification of Diseases.

The simple code sets are part of the implementation guidance coming from the standards organization, primarily X12 that developed the transaction standards. The *complex code sets* include the:

- International Classification of Diseases, 9th Edition, Clinical Modification, (ICD-9-CM), Volumes 1, 2, and 3,
- National Drug Codes (NDC),
- Code on Dental Procedures and Nomenclature,
- Health Care Financing Administration Common Procedure Coding System (HCPCS), and
- Current Procedural Terminology, Fourth Edition (CPT-4).

Local codes that traditionally have been allowed as the 3rd level of HCPCS are not allowed in the Transaction Standards. Problems with the existing code sets are acknowledged. Each code set is undergoing revision and these revisions, such as ICD-10-CM, are expected to replace their predecessors in the transactions.

2.8.4 Identifiers

Some of the fields in the transactions are filled with values from identifiers. The 'National Provider Identifier' has been proposed, and the 'National Employer Identifier' have been finalized. However, the 'Personal Identifier' has proven so highly contentious that no proposal for it exists.

Currently, no *healthcare provider identifier* is a national standard. This leads to communication problems among entities in trying to resolve the identity of providers. An extensive review of existing candidate identifiers revealed weaknesses with all but one candidate identifier. The identifier systems that were rejected include the Unique Physician Identification Number, the Health Industry Number, the National Association of Boards of Pharmacy Number, the Social Security Number, and the Drug Enforcement Administration Number. DHHS proposes that its National Provider System is the best.

The National Provider System has two different parts:

- National Provider Identifier and
- National Provider File.

The National Provider Identifier is simply an 8-position alphanumeric identifier. It contains no intelligence about the character of the provider and is simply an arbitrary string assigned uniquely to the provider.

The *National Provider File* is by contrast loaded with intelligence. It has dozens of fields that go from simple checkboxes about race of individuals to information about the licenses held by the provider and the location of the provider. Obtaining and maintaining reliable information about licenses and locations is not a trivial matter.

DHHS estimates a cost of about $50 per provider to achieve an entry in the National Provider System. About one million providers would need initially to be included in the system.

The *Employer Identifier* is simpler than the Provider Identifier. The Employer Identifier is the Employer Identification Number assigned by the Internal Revenue Service. No support files are required.

At the moment different entities use different methods of identifying individuals. When the public learned that the government was developing standard personal health identifiers, various protests ensued that were magnified by the media. In the end the government ordered a moratorium on work to produce a Personal Identifier.

2.8.5 Impact Analysis

One argument for standard's benefit is combinatorial. When people speak n different languages, n times n translators are needed. As n grows, 'n times n' grows faster. When n is 400, then 'n times n' is 160,000. However, when one language is spoken, no translators are needed.

Extensive analyses have been done of the *dollar costs and benefits* of the transaction and code set standards. In the first year, the cost is greater than the benefit to all concerned. By the fifth year, the payers are saving $1.7 billion per year, and the providers are saving $1.5 billion per year. However, for the providers the first three years are losses and added over the 5-year period, the providers actually experience a net loss. That loss will be, however, overturned by the sixth year when all participants show total cumulative benefit.

The new regulations mean initially that clearinghouses and billing services get extra work to help their clients come to grips with the legislation. In the long run, the clearinghouses and billing services may find that their traditional offerings are less needed as providers and payers increasingly directly communicate. The clearinghouses and billing services should offer new services that standardization makes practical.

The *qualitative benefits* of standardization include improved patient care and generally more reliable and useful data. Overall, the healthcare system should become more efficient and effective. These benefits of standard transactions are common across industry groups.

2.8.6 Implementation

Given that multiple entities are exchanging transactions, the standardization effort needs to be coordinated. WEDI-SNIP has proposed a national schedule that implements the prominent transactions first. Part of the coordination effort is testing of the compliance of a transaction with the standard, and to this end a 6-level certification test is described.

Providers, health plans, and clearinghouses face different challenges in adjusting their workflow and information flow to accommodate standardization of transactions. The steps that a provider might take highlight a careful inventory of current processes followed by a financial and technical assessment of options. The clearinghouse option is a fast solution but entails steady, substantial, long-term costs. The option of internally integrating standardization into the provider offers particular long-term efficiencies.

2.8.7 Epilogue

Initially, only a handful of transactions are standardized, and they emphasize claims and payments. However, the transactions that are initially standardized are the tip of the iceberg. For the payer-provider relation more transactions will be formalized over the coming years and will progressively cover other aspects of the communication between payers and providers.

Payer-provider transactions include *claims attachments*. When a payer wants to know why a provider requests a certain payment, the ultimate source of information is sometimes the entire medical record and that record becomes then a claims attachment. The proposed standardization of the claims attachments simply provides an envelop over the medical record. However, progress in standardizing the medical record format and content will have enormous, positive ramifications for the administration of healthcare.

Standardized transactions are the currency of quality management and the endowment for continuous quality improvement of patient care. Only by capturing clinical data from healthcare providers in a way that the data can be applied to healthcare decisions for individuals and to policy decisions for populations can the goal of high-quality, affordable healthcare be achieved. HIPAA’s administrative simplification represents a giant step towards such *standardization*.

3 Privacy

Target

Learning Objectives

- Diagram the flow of patient health information and show how privacy concerns reflect power concerns.
- Identify the need for acknowledgment of notice of privacy practices in the initial encounter as distinct from the need for authorization for subsequent disclosure for non-routine purposes.
- Construct a roles-to-information map that supports minimum necessary use.
- Demonstrate how business associate contracts and de-identification permit an entity to share information without a patient authorization.
- Classify certain exceptions to the rule as 'opportunity to object' or 'no opportunity to object'.
- Describe what an entity must do to serve patient rights.
- Identify the key administrative requirements of the Privacy Rule.
- Place the HIPAA Privacy Rule in the context of other laws and regulations.
- Estimate the costs for each type of activity required to achieve compliance with the Privacy Rule.
- Predict the struggles over information.

Main Points

- Privacy is very important to people.
- The Privacy Rule requires an acknowledgment of a notice of privacy practices for routine use of health information and a signed authorization form for other uses.
- For some information uses the entity need only give the patient an opportunity to object, while for certain, very special uses the entity may use the information whether or not the patient objects.
- Patients have a right to a copy of their medical record, to request an amendment to it, and to know the history of disclosures.
- Entities have great flexibility in how they implement the privacy regulations, but they are expected to have a privacy officer, train staff, and document policies.
- Other regulations of various governments have complex interactions with the Privacy Rule.
- The Privacy Rule is considered expensive to implement.

Administrative Simplification first asks for standardizing electronic transactions between healthcare providers and payers. This standardization should increase the flow of electronic information and the ability of various organizations to take advantage of the information therein. To insure that the information is not misused, HIPAA also calls for security and privacy. The ensuing material presents the principles and related information of the Privacy Rule.

3.1 Introduction

Main Points

- The history of privacy runs wide and deep.
- Privacy is first and foremost about power.
- Privacy standards are needed for many reasons.
- In a well-coordinated organization, privacy is built into the routine operation.
- The Privacy Rule applies to all health information in a covered entity that transmits any health information electronically.

The Privacy Rule has two major purposes:

- to protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information and
- to improve the efficiency and effectiveness of healthcare delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individuals.

The Rule may bring the patient closer to the healthcare process by more closely connecting the patient with the patient's record.

3.1.1 History of Privacy

Hippocrates was an ancient Greek physician whose writings not only had a great impact on the content of Greek medical thought but also on the privacy of patient information. He said (Staden, 1996):

> About whatever I may see or hear in treatment, or even without treatment, in the life of human beings -- things that should not ever be blurted outside -- I will remain silent, holding such things to be sacred, and not to be divulged

Physicians take a variant of this oath to this day.

In 1766 the British Parliament debate on search warrants included (Cooley, 1883):

> The poorest man may, in his cottage, bid defiance to all the forces of the Crown. The cottage may be frail; its roof may shake; ... but the King of England may not enter.

The American right to privacy is rooted in part in the *Fourth Amendment* to the United States Constitution. This Amendment states:

> The right of the people to be secure in their person, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Warrren and Brandeis (1890) said:

> In very early times, the law gave a remedy only for physical interference with life and property, for trespasses vi et armis. Then the 'right to life' served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. ... Gradually the scope of these legal rights broadened; and now the right to life has come to mean ... the right to be let alone ... and the term 'property' has grown to comprise every form of possession -- intangible, as well as tangible. ... Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone". Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops".

The same Brandeis (1928), but as a member of the U.S. Supreme Court four decades later, wrote:

> The makers of our Constitution ... conferred, as against the Government, the right to be let alone -- the most comprehensive of rights and the right most valued by civilized man.

The recent concerns for privacy are not that an official will physically enter and search someone's house nor that the newspaper will take photographs of private events. Rather the concern is for the use of records, particularly in computers.

3.1.2 Power

In the mid-19th century, three quarters of the adult population worked for themselves on farms or in small towns. Attendance at the village schoolhouse was not compulsory. Record keeping about individuals was limited and local in nature. Few individuals had insurance of any kind. A patient's medical record typically existed only in the doctor's memory. Now, by contrast, fewer than 10% of people are self-employed, and their employers often keep extensive records on them. Insurance is common, and medical care is institutionalized. Acquiring insurance or medical care requires the individual to divulge information, and usually leads to some evaluation of him based on information about him that some other *record keeper* has compiled.

Each individual plays a dual role in organizational record keeping (Privacy, 1977):

- as an object of information gathering and
- as a consumer of the benefits and services that depend on it.

While Americans claim to treasure their privacy, they are willing to share information about themselves when they see a concrete advantage to be gained by it.

Some people assert that a person does not object to organizational record-keeping practices "if the person has nothing to hide". However, whether or not an individual has something to hide is a matter of opinion and depends on who wants to do what with what information. The *balance* is delicate between an organization's need for information and each individual's desire to be fairly treated.

As computerized record collection and distribution by organizations continues to supplant *face-to-face* collection and distribution of information, the individual loses control to the organization. The individual is less well positioned to monitor what happens to information about the individual in the hands of a

- a computerized, global organization than
- another individual in the same community.

The information could be quickly spread widely by a global organization before the individual had any evidence of such privacy invasion.

What two people divulge about themselves when they meet for the first time depends on how much personal revelation they believe the situation warrants and how much confidence each has that the other will not misinterpret or misuse what is said. If they meet again, and particularly if they develop a relationship, their self-revelation may expand both in scope and detail. Throughout this process, each person may

- correct any misperception that develops and
- judge whether the other is likely to misuse the personal revelations.

Should either suspect that the other has violated the trust, he can sever the relationship or alter its terms, perhaps by refusing thereafter to discuss certain topics. Such relationships are the threads of which the fabric of society is woven. The situations are inherently social and not private in that the disclosure of information about oneself is expected.

An individual's relationship with a *record-keeping organization* has some of the features of individual face-to-face relationships, as it arises in an inherently social context, depends on the individual's willingness to divulge information, and carries some expectation of the practical consequences. Beyond that, however, the resemblance fades.

Typically, the organization decides what information must be divulged at what rate. The individual might theoretically take his business elsewhere when dealing with private organizations (but not when dealing with the government). Yet, organizations tend to have similar *information gathering requirements*, the differences among them are poorly understood, and the individual often has little opportunity to meaningfully pick and choose.

Once an individual establishes a relationship with a record-keeping organization, he loses some of the control that he has in face-to-face relationships, and this control or power goes to the organization. The individual faces challenges in trying to

- check on the accuracy of the information the organization develops,
- correct any errors that may exist in the information,
- know the full extent of uses of the information,
- know the disclosures of the information, or
- sever the relationship with the organization.

Having power is in a certain sense the ability to invade someone else's privacy. Information, in the hands of people who know how to use it, is power. Privacy is first and foremost about power.

Power and its converse *privacy* fascinate people in all socioeconomic classes, geographical regions, and political parties. Stores, homes, and workplaces buzz with lively and colorful rumors about what friends, relatives, and employers both possess and lack. People are born to seek power over others and privacy for themselves. Yet a tense silence surrounds the fact. People are often reluctant to acknowledge their attitudes towards power and privacy. This taboo against candor arises from the popular myths that power is evil and powerlessness is righteous and likewise that the desire for privacy is evil and openness is righteous.

The politics of privacy is a never-ending battle over who will control the record (Bacard, 1995). Who will get paid how much for which data bits? Who will be able to censor which records?

3.1.3 A Flow Scenario

The flow of information in healthcare may go beyond what people expect. The National Research Council has described the complex flow of personal health information in the following *scenario* (Committee, 1997):

> Rosa is in her late 20s, married, and employed by a small company. Her husband Ray is employed by a large firm. Ray's company offers its employees a choice of health benefit plans via a preferred provider organization (PPO). Differences in the ways their health records may be stored and controlled are not outlined in the program descriptions, and Rosa and Ray do not consider this factor in their decision.
>
> On her first visit to a prospective primary physician, who is a member of a small group practice, Rosa is asked to fill out a medical history form and specify how she will pay for her care in the future. She indicates that she will use the health insurance benefits available to her through her husband's job. Since Rosa specifies that some of her charges will be covered by a party other than herself, she is also given a form to sign that authorizes the physician's office to send information to the insurer for payment of claims. This release covers all future visits Rosa makes to this practice.
>
> Rosa's records for her initial examination are recorded on paper and held in the physician's office. Blood samples taken from her during the visit, however, are sent to an outside laboratory for analysis. Automated analysis equipment records the laboratory results and prints a paper copy that is returned to the physician; the laboratory bills Rosa for the service. The laboratory also retains a record of the test and of Rosa's identity. Through the third-party administrator used by Ray's firm to manage health care benefits, Ray's firm receives a claim from Rosa for the office visit and the blood test and approves payment.
>
> The following year, Rosa's annual checkup reveals hypertension. The physician prescribes medication, and Rosa fills the prescription at a local pharmacy. The pharmacy's charges are reimbursed through a pharmacy benefits program connected with the health insurance option selected by Ray. The pharmacy records Rosa's name and address, reads her pharmacy benefits card, notifies the benefits program, and is reimbursed. Parts of Rosa's health record now reside with the retail pharmacy and the pharmacy benefits provider, as well as her care provider.
>
> Ray's company, feeling competitive pressures, considers ways to save money and increase productivity. Since Ray's company is self-insuring, it asks the third-party administrator to provide it with claims information pertaining to its employees. The third-party administrator has no legal basis on which to refuse the request and, wanting to maintain good relations with its client, provides the information to Ray's employer. Since her claims are paid by Ray's company, Rosa's record, as well as Ray's, is also forwarded. Rosa's company, under similar pressure, initiates a company clinic on-site and a wellness program. Although she continues to be insured by Ray's company, Rosa uses the clinic occasionally and, on her first visit, provides the clinic with her history, including a list of medications she is taking.
>
> After the birth of their first child, Ray and Rosa realize that they need life insurance. Rosa applies for coverage with a large, respected firm, which will provide the coverage she wants if she passes a physical examination. The life insurance company will pay for the examination, but she must sign a release permitting the results of the examination to be forwarded to the Medical Information Bureau (MIB). The life insurance company decides to accept the risk of insuring her but forwards the hypertension results to the MIB in accordance with the industry's practices because her hypertension, although under control, may potentially affect her longevity.
>
> The group practice Rosa uses is purchased by a managed care firm, which installs its automated records program. Results of Rosa's office visits are now stored on a local computer system. The managed care firm, facing the same competitive pressures as Ray's company, periodically reviews records from each of its many groups to ensure both the quality and the appropriateness of the care provided.

The managed care firm denies a request from another patient within the practice to consult a specialist for a condition similar to the one for which Rosa was treated. The patient subsequently sues the practice, and her lawyers request disclosure of records from similar cases within the practice. The court grants a subpoena for the records involved, including Rosa's, and the practice is compelled to provide copies of the records to lawyers. Rosa's name is removed from the record.

Parts of Rosa's health record are held by a wide variety of organizations:

- her primary care physician's practice,
- a clinical laboratory,
- the local pharmacy,
- the pharmacy benefits provider,
- her husband's employer,
- her life insurance company,
- the Medical Information Bureau,
- the outcomes researcher, and
- various lawyers.

Most of these organizations have information that specifically identifies Rosa. She has explicitly consented access to some of these holders but not others.

If Rosa had developed an expensive, chronic condition as a complication of her pregnancy, Ray's self-insured employer could be made aware of that fact through its review of billing data (which contain detailed diagnostic codes). Ray's employer could use such information to influence a decision about Ray's continued employment. Managers in Ray's company might well argue that Ray's high health insurance bills make him too expensive to keep on the payroll. No legal standard prevents Ray's old employer from discussing Rosa's condition with a potential new employer or prevents some entrepreneur from establishing a clearinghouse of data on employees with *high insurance costs*.

As Rosa's story shows, the types of organizations that collect, process, and store health information include not only other members of the health care provider teams, such as laboratory technicians, but also groups such as third-party payers and a growing *health information services industry*. These various organizations have historically developed separate policies with regard to the protection of information in these records. These separate privacy policies reflect the different perceptions of individual stakeholders regarding the proper trade-off between Rosa's privacy interests and their use of the data.

3.1.4 Authorized Abuse

The press has many reports of privacy abuses. However, these are typically of the sensational, isolated, unauthorized category. Reports of unauthorized use of medical records include:

- A database created by the state of Maryland in 1993 to keep the medical records of all its residents for cost containment purposes was used by a banker to call in the loans of those bank customers whom the banker thus discovered had cancer (Gunter, 1996).
- While visiting her mother at the hospital at which she worked, the 13-year old daughter accessed the hospital's online patient files. The girl then phoned female patients and told them they were infected with HIV or were pregnant. After receiving such a call, one teenage victim attempted suicide (Davis, 1995).
- When Nydia Velazquez was running for Congress in 1992 in New York, someone obtained her hospital records detailing her 1991 suicide attempt and forwarded them to the press (Gorman, 1996). The New York Post published the story and Velazquez had to acknowledge publicly what she had not even shared with her family.

Many other such instances have been publicized. These incidents are

- isolated acts,
- committed by a single person,
- violate policies and ethics of institutions in which the incident occurred, and
- sometimes violate the law.

These unauthorized uses have consequences that are less significant than the consequences of the use that occurs by business of medical records. Most violations of privacy of medical records are the result of the unconcealed, systematic flow of medical information from the physician-patient-health insurer to other non-healthcare parties, including employers:

- In 1996, 35% of the Fortune 500 companies acknowledged that they drew on personal health information from insurance companies in making employment decisions (EPIC, 1996).
- A 1996 study by Harvard and Stanford Universities documented 206 cases of genetic discrimination against asymptomatic individuals. The individuals suffered loss of employment, loss of insurance coverage, or ineligibility for insurance based on their genetic potential for disease (Stipe, 1996).

In these situations, the employers did not misappropriate medical information -- their access to it was contractual and legal.

Marketing-type uses are also rampant:

- Metromail has a medical database of 15 million names. For about thirty cents per name, large drug companies can pitch their products directly to angina sufferers, diabetics, or others (Editor, 1994)
- IMS America buys for resale patient records with personal identifying information attached outright from state governments, medical clinics, and drugstore chains.
- The Medical Information Bureau (MIB) is a clearinghouse of medical information whose members include 680 life insurance companies. These records include medical information like a history of high blood pressure, as well as other information affecting insurance, such as a reckless driving record. Whenever an individual applies for insurance, the MIB members get the record from MIB.

These violations of privacy constitute a macroscopic problem.

3.1.5 Public Opinion

A Wall Street Journal/ABC poll asked Americans what concerned them most in the 21st century. '*Loss of personal privacy*' was the first or second concern of 29 percent of respondents. All other issues, such a terrorism, world war, and global warming had scores of 23 percent or less. At the same time, these same people want to be able to use a cellular phone to get their banking details online instantly across all their accounts, to find someone's address based on his or her phone number, and so on.

The Gallup Organization did a survey on the privacy of medical records (Gallup, 2000). A national cross-section from 1,000 households was systematically *interviewed*. Results showed:

- About eight in ten adults feel it is very important that their medical records be kept confidential. Less than half feel it is very important that their employment history be kept confidential, and fewer than one-third feel it is very important that their educational history be kept confidential.
- The majority of adults oppose allowing access to their medical records without their authorization to any group. Nine of ten oppose giving government agencies access. Eight of ten oppose employers being allowed to see their medical records. Seven in ten oppose giving doctors access to their medical records without permission. Medical researchers would be denied access too.
- While controlling access to their medical records is important to many, only one of five have heard or read anything recently about new federal regulations that would change the rules regarding access to medical records. Only one in ten would support a plan that requires every American to be assigned a medical identification number.

Patients want their information protected! Individuals who provide information to healthcare organizations are concerned about how their information is used. Patients want to know that their sensitive information will be *protected* not only during the course of their treatment but also in the future.

3.1.6 Applicable

The Privacy Rule applies to healthcare plans, providers, and clearinghouses that transmit health information in electronic form. Because DHHS does not have the authority to apply these standards directly to any entity that is not a *covered entity*, the rule does not directly cover some entities that obtain identifiable health information from covered entities. Any provider who maintains a solely paper information system would not be subject to these privacy standards.

If an entity transmits any individually identifiable health information in electronic form, then all individually identifiable health information in any form, electronic or non-electronic, is covered by this Privacy Rule. This includes information in *paper* records that never has been electronically stored or transmitted. If a hospital submits bills electronically and has a ward for which all information is on paper, then that paper information must be handled according to the Privacy Rule.

The Privacy Rule does not directly cover some entities that obtain identifiable health information from covered entities. Examples of entities that receive this information include workers compensation carriers, life insurance issuers, employers and marketing firms. DHHS also does not have the authority under HIPAA to directly regulate some of the persons that covered entities hire to perform administrative, legal, accounting, and similar services on their behalf, and who would obtain health information in order to perform their duties. This inability to directly address the information practices of these groups leaves a *gap in the protections* provided by the HIPAA Privacy Rule (DHHS, 1997). To cover this gap DHHS requires agreements between covered entities and their business associates such that the business associate is also obligated to maintain privacy. Additional legislation to broaden the applicability of the privacy legislation to cover any organization using any medium has been proposed in Congress but has not been accepted.

3.1.7 Review Questions

1. What is the relationship between power and privacy?
2. Why are privacy standards needed?
3. To what entities is the Privacy Rule applicable? To what entities is it not applicable?

3.2 Notice of Privacy Practices

Main Points

- The Notice of Privacy Practices captures the essences of the privacy policy as that policy pertains to patients.
- The provider must seek acknowledgment from the patient that the patient has read the Notice of Privacy Practices
- The Partners HealthCare System has a 'Notice for Patients' that add various particulars and takes a somewhat different approach than DHHS.

DHHS has extensively described a Notice of Privacy Practices. The healthcare provider will post for or send to patients this notice. The notice describes how covered healthcare providers and health plans use and disclose protected health information, and the individual's rights with respect to that information.

3.2.1 Content

The entity's privacy 'practices' are distinct from its 'policies'. An entity's 'policies' are a detailed documentation of all of the entity's privacy practices. For example, entities must have policies implementing the requirements for 'minimum necessary' use and disclosure of protected health information, but these policies need not be reflected in the entity's 'notice of privacy practice'. Similarly, entities must have policies for assuring individuals access to protected health information about them. While such *policies* will need to include documentation of the designated record sets subject to access, who is authorized to determine when information will be withheld from an individual, and similar details, the notice need only explain generally that individuals have the right to inspect and copy information about them, and tell individuals how to exercise that right.

The requirements for the content of the notice are not intended to be exclusive. As with the rest of the rule, DHHS specifies minimum requirements, not best practices. Entities may want to include more detail.

Entities may produce more than one notice. For example, an entity that conducts business in multiple states with different laws regarding the uses and disclosures that the entity is permitted to make may be required to produce a different notice for each state. An entity that conducts business both as part of an organized healthcare arrangement and as an independent enterprise (e.g., a physician who sees patients through an on-call arrangement with a hospital and through an independent private practice) may want to adopt different privacy practices with respect to each line of business. Entities must produce notices that accurately describe the privacy practices that are relevant to the individuals receiving the notice.

Entities may utilize a *layered notice* to implement the Rule's provisions. For example, a covered entity may satisfy the notice provisions by providing the individual with both a short notice that briefly summarizes the individual's rights, as well as other information; and a longer notice, layered beneath the short notice, that contains all the elements required by the Privacy Rule. Covered entities, however, while encouraged to use a layered notice, are not required to do so. Nothing in the final modifications relieve a covered entity of its duty to provide the entire notice in plain language so the average reader can understand it.

3.2.2 Provision of Notice

All covered entities that are required to produce a *notice* must provide the notice upon request of any person. The requestor does not have to be a current patient or enrollee. The notice is a public document that people can use in choosing between covered entities.

Health plans must provide the notice to all health plan enrollees as of the compliance date. After the compliance date, health plans must provide the notice to all new enrollees at the time of enrollment and to all enrollees within 60 days of a material revision to the notice. *Health plans* must notify enrollees no less than once every three years about the availability of the notice and how to obtain a copy.

Practical, effort-saving steps are appropriate in the distribution of notices. Examples for health plans follow:

- If a named insured and one or more dependents are covered by the same policy, the health plan can satisfy the distribution requirement with respect to the dependents by sending a single copy of the notice to the named insured.
- If an employee of a firm and her three dependents are all covered under a single health plan policy, then that health plan can satisfy the initial distribution requirement by sending a single copy of the notice to the employee rather than sending four copies, each addressed to a different member of the family.
- If a health plan has more than one notice, it satisfies its distribution requirement by providing the notice that is relevant to the individual or other person requesting the notice. For example, a health insurance issuer may have contracts with two different group health plans. One contract specifies that the issuer may use and disclose protected health information about the participants in the group health plan for research purposes without authorization (subject to the requirements of this rule) and one contract specifies that the issuer must always obtain authorizations for these uses and disclosures. The issuer accordingly develops two notices reflecting these different practices and satisfies its distribution requirements by providing the relevant notice to the relevant group health plan participants.

Patients must receive the relevant notice.

The distribution requirements vary according to whether the healthcare provider has a direct treatment relationship with an individual or not:

- Providers that have direct treatment relationships with individuals must provide the notice to such individuals as of the first service delivery after the compliance date. This requirement applies whether the first service is delivered electronically or in person. Providers may satisfy this requirement by sending the notice to all of their patients at once, by giving the notice to each patient as he or she comes into the provider’s office or facility or contacts the provider electronically, or by some combination of these approaches. Providers that maintain a physical service delivery site must prominently post the notice where it is reasonable to expect individuals seeking service from the provider to be able to read the notice. The notice must also be available on site for individuals to take on request. In the event of a revision to the notice, the covered provider must promptly post the revision and make it available on site.
- Healthcare providers that have indirect treatment relationships with individuals are only required to produce the notice upon request.

An entity that maintains a web site describing its services must make its privacy notice prominently available through the web site. An entity may satisfy the applicable distribution requirements described above by providing the notice to the individual *electronically*, if the individual agrees to receive materials from the covered entity electronically and the individual has not withdrawn his or her agreement. If the entity knows that the electronic transmission has failed, the covered entity must provide a paper copy of the notice to the individual.

If an individual's first service delivery from a provider occurs electronically, the provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. For example, the first time an individual requests to fill a prescription through a covered *Internet pharmacy*, the pharmacy must automatically and contemporaneously provide the individual with the pharmacy's notice of privacy practices. An individual that receives a covered entity's notice electronically retains the right to request a paper copy of the notice. This right must be described in the notice.

3.2.3 Acknowledgment

A health care provider with a direct treatment relationship with an individual must make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice. Other covered entities, such as health plans, are not required to obtain this acknowledgment from individuals, but may do so if they choose. The requirement provides individuals with an opportunity to request any additional restrictions on uses and disclosures of their health information or confidential communications, as permitted by the Rule.

The Rule requires, with one exception, that a covered direct treatment provider make a good faith effort to obtain the written acknowledgment no later than the date of first service delivery, including service delivered electronically, that is, at the time the notice is required to be provided (GCD, 2002). During emergency treatment situations, the final Rule delays the requirement for provision of the notice until reasonably practicable after the emergency situation, and exempts health care providers from having to make a good faith effort to obtain an individual's acknowledgment in such emergency situations.

The Rule requires only that the acknowledgment be in writing (including electronic writing), and does not prescribe other details such as the form that the acknowledgment must take or the process for obtaining the acknowledgment. For example, the final Rule does not require an individual's signature to be on the notice. Instead, a covered health provider is permitted, for example, to have the individual sign a separate sheet or list, or to simply initial a cover sheet of the notice to be retained by the provider. Alternatively, a pharmacist is permitted to have the individual sign or initial an acknowledgment within the log book that patients already sign when they pick up prescriptions, so long as the individual is clearly informed on the log book of what they are acknowledging and the acknowledgment is not also used as a waiver or permission for something else (such as a waiver to consult with the pharmacist). For notice that is delivered electronically as part of first service delivery, DHHS believes the provider's system should be capable of capturing the individual's acknowledgment of receipt electronically. In addition, those covered health care providers that choose to obtain consent from an individual may design one form that includes both a consent and the acknowledgment of receipt of the notice. Covered health care providers are provided discretion to design the acknowledgment process best suited to their practices.

While DHHS believes that the notice acknowledgment process must remain flexible, DHHS does not consider oral acknowledgment by the individual to be either a meaningful or appropriate manner by which a covered health care provider may implement these provisions. The notice acknowledgment process is intended to provide a formal opportunity for the individual to engage in a discussion with a health care provider about privacy. At the very least, the process is intended to draw the individual's attention to the importance of the notice. DHHS believes these goals are better accomplished by requiring a written acknowledgment.

If an individual refuses to sign or otherwise fails to provide an acknowledgment, a covered health care provider is required to document its good faith efforts to obtain the acknowledgment and the reason why the acknowledgment was not obtained. Failure by a covered entity to obtain an individual's acknowledgment, assuming it otherwise documented its good faith effort, is not a violation of the Rule. Such reason for failure simply may be, for example, that the individual refused to sign the acknowledgment after being requested to do so. A covered entity is required to document compliance with these provisions by retaining copies of any written acknowledgments of receipt of the notice or, if not obtained, documentation of its good faith efforts to obtain such written acknowledgment.

3.2.4 Plain Language

Recipients who cannot understand the entity's notice would miss important information about their privacy rights and how the entity is protecting health information about them. One of the goals of this rule is to create an environment of *open communication* and transparency with respect to the use and disclosure of protected health information. A lack of clarity in the notice could undermine this goal and create misunderstandings.

The notice must be in plain language. A covered plan or provider could satisfy the plain language requirement by:

- organizing material to serve the needs of the reader;
- writing sentences in the active voice;
- using 'you' and other pronouns;
- using common, everyday words in sentences;
- writing in short sentences; and
- dividing material into short sections.

Since the content of the notice should be communicated to all recipients, the covered entity should consider various means of communicating with various populations. Any covered entity that is a recipient of federal financial assistance is obligated under Title VI of the Civil Rights Act of 1964 to provide material ordinarily distributed to the public in the primary languages of persons with limited *English proficiency* in the recipients' service areas.

DHHS encourages covered entities to be attentive to the needs of individuals who cannot read. For example, an employee of the entity could read the notice to individuals upon request or the notice could be incorporated into a *video* presentation that is played in the waiting area.

Entities must include prominent and specific language in the notice that indicates the importance of the notice. The header must read:

> THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

This is the only specific language entities must include in the notice.

3.2.5 Uses and Disclosures

Entities must separately describe each purpose for which they are permitted to use or disclose protected health information under this rule without authorization, and must do so in sufficient detail to place the individual on notice of those uses and disclosures. With respect to uses and disclosures to carry out treatment, payment, and healthcare operations, the description must include at least one example of the types of *uses and disclosures* that the covered entity is permitted to make. This requirement is intended to inform individuals of all the uses and disclosures that the covered entity is legally required or permitted to make under applicable law, even if the covered entity does not anticipate actually making such uses and disclosures.

The Notice could be the same for every covered entity of a particular type within a state or other locale. DHHS encourages states, state professional associations, and other organizations to develop model language to assist covered entities in preparing their notices. This recommendation for *models*, if implemented, will expedite the implementation of these notices.

While the Privacy Rule requires entities to describe all of the types of uses and disclosures permitted or required by law (not just those that the covered entity intends to make), entities may include optional elements that describe the actual, more limited, uses and disclosures they intend to make without authorization. Some entities will want to *distinguish* themselves on the basis of their more stringent privacy practices. For example, healthcare providers who routinely treat patients with particularly sensitive conditions may wish to assure their patients that, even though the law permits them to disclose information for a wide array of purposes, the healthcare provider will only disclose information in very specific circumstances, as required by law, and to avert a serious and imminent threat to health or safety.

3.2.6 Rights, Duties, Contact

Entities must describe individuals' rights under the rule and how individuals may exercise those rights with respect to the entity. Entities must describe each of the following rights, as provided under the rule:

- the right to request restrictions on certain uses and disclosures, including a statement that the covered entity is not required to agree to a requested restriction;
- the right to receive confidential communications of protected health information;
- the right to inspect and copy protected health information;
- the right to amend protected health information; and
- the right to an accounting of disclosures of protected health information.

Additionally the notice must describe the right of an individual, including an individual that has agreed to receive the notice electronically, to obtain a paper copy of the notice upon request.

Entities must state in the notice that they are required by law to

- maintain the privacy of protected health information,
- provide a notice of their legal duties and privacy practices, and

- abide by the terms of the notice currently in effect.

Upon revision of the notice, the Privacy Rule requires only that the direct treatment provider make the notice available upon request on or after the effective date of the revision, and, if he maintains a physical service delivery site, to post the revised notice in a clear and prominent location in his facility. As the Rule does not require a health care provider to provide the revised notice directly to the individual, unless requested by the individual, a new written acknowledgment is not required at the time of revision of the notice.

An entity's notice must inform individuals about how they can lodge complaints with the covered entity if they believe their privacy rights have been violated. The notice must also state that individuals may file complaints with DHHS. Additionally the notice must include a statement that the individual will not suffer retaliation for filing a *complaint*. The notice must identify a point of contact where the individual can obtain additional information about any of the matters identified in the notice.

The notice must include the date the notice went into effect. The effective date cannot be earlier than the date on which the notice was first printed or otherwise published.

3.2.7 Revisions to the Notice

Entities are required to adhere to the terms of the notice currently in effect. When an entity materially changes any of the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices described in its notice, the entity must promptly revise its notice accordingly. Except when required by law, a *material change* to any term in the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

An entity that wishes to change its practices over time without *segregating its records* according to the notice in effect at the time the records were created must reserve the right to do so in its notice. Two examples are provided:

- A hospital that states in its notice that it will only make public health disclosures required by law, and that does not reserve the right to change this practice, is prohibited from making any discretionary public health disclosures of protected health information created or received during the effective period of that notice. If the covered hospital wishes at some point in the future to make discretionary disclosures for public health purposes, it must revise its notice to so state, and must segregate its records so that protected health information created or received under the prior notice is not disclosed for discretionary public health purposes. This hospital may then make discretionary public health disclosures of protected health information created or received after the effective date of the revised notice.
- If a second hospital states in its notice that it will only make public health disclosures required by law, but does reserve the right to change its practices, it is prohibited from making any discretionary public health disclosures of protected health information created or received during the effective period of that notice. If this hospital wishes at some point in the future to make discretionary disclosures for public health purposes, it must revise its notice to so state, but need not segregate its records. As of the effective date of the revised notice, it may disclose any protected health information, including information created or received under the prior notice, for discretionary public health purposes.

Entities may do well to reserve the right to make changes.

3.2.8 Notice for Patient

In its Notice of Proposed Rule Making (NPRM), DHHS provided a model 'Notice of Information Practices'. This notice was the precursor to the 'Notice of Privacy Practices' in the Final Rule. The *NPRM Notice* has been slightly modified by this author and reproduced here. This version no longer has the blessing of DHHS and is not presented as a legally accurate reflection of what is required by the Final Rule.

PROVIDER NOTICE

OF INFORMATION PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Uses and disclosures of health information

We may use or disclose identifiable health information about you without your authorization for several reasons. Subject to certain requirements, we may give out health information without your authorization for public health purposes, for

> auditing purposes, for research studies, and for emergencies. We provide information when otherwise required by law, such as for law enforcement in specific circumstances. In any other situation, we will ask for your written authorization before using or disclosing any identifiable health information about you. If you choose to sign an authorization to disclose information, you can later revoke that authorization to stop any future uses and disclosures.
>
> We may change our policies at any time. Before we make a significant change in our policies, we will change our notice and post the new notice in the waiting area and in each examination room. You can also request a copy of our notice at any time. For more information about our privacy practices, contact the person listed below.
>
> Individual rights
>
> In most cases, you have the right to look at or get a copy of health information about you that we use to make decisions about you. If you request copies, we will charge you $0.08 (8 cents) for each page. You also have the right to receive a list of instances where we have disclosed health information about you for reasons other than treatment, payment or related administrative purposes. If you believe that information in your record is incorrect or if important information is missing, you have the right to request that we correct the existing information or add the missing information.
>
> Complaints
>
> If you are concerned that we have violated your privacy rights, or you disagree with a decision we made about access to your records, you may contact the person listed below. You also may send a written complaint to the U.S. Department of Health and Human Services. The person listed below can provide you with the appropriate address upon request.
>
> Our legal duty
>
> We are required by law to protect the privacy of your information, provide this notice about our information practices, and follow the information practices that are described in this notice.
>
> *If you have any questions or complaints,*
> *please contact:*
> *Office Administrator*
> *111 Main Street, Anytown, OH 41111*
> *Phone: (111) 555-6789*
>
> Email: admin@docshop.com
>
> ………………………………………………
>
> Acknowledgment of receipt of Notice of Privacy Practices:
>
> Please sign your name and print your name and date on this acknowledgment form. Then detach the form from the Notice along the dotted line and return your signed acknowledgment to the receptionist or to the address above.
>
> Signature: ______________________
>
> Printed name: ______________________
>
> Date: ____________________

Many longer privacy notice forms are available, and any given organizations should be able to find some thing close to its needs and tailor that.

3.2.9 Partners' Notice for Patients

Partners HealthCare System was established in 1994 to oversee the affiliation of Brigham and Women's Hospital, Massachusetts General Hospital, and North Shore Medical Center. Partners has a 'policy on confidentiality for patients' that was prepared prior to HIPAA but indicates features that an entity might include in its 'Notice'.

Partners' 'Notice for Patients' emphasizes trust with the patient:

> Partners HealthCare System and Partners Community HealthCare are committed to providing you with high quality healthcare and to forming a relationship with you that is built on trust. That means respecting your privacy and confidentiality of you medical information. We protect your privacy and confidentiality rights by creating and putting into practice policies and procedures that allow access to your personal medical information only for legitimate reasons.

While the DHHS document notes the legal requirement for the notice, Partners goes further and explains how Partners assures privacy, including its *employee disciplinary practice*:

> Partners has put in place detailed policies regarding access to medical records by our staff and employees and has carefully

> outlined the circumstances under which your medical information may be released to parties outside the hospital or physician practice. These policies conform to state and federal law and are designed to safeguard your privacy.
>
> Our staff and employees are trained in the appropriate use of medical information and know that it is available to them only to continue to provide care to you or for other limited but legitimate reasons. A violation of confidentiality or the failure of an employee to protect your information from accidental or unauthorized access will not be tolerated. This may include the employee being fired from his or her job.

Whereas the DHHS notice does not indicate specific types of information that would require special permission (aside from a footnote about psychotherapy), the Partners' Notice lists several categories of information that must be treated in a special way, as follows:

> We do not allow others outside Partners to access your medical information unless we have the appropriate authorization to do so. We will request your authorization to release information at your first visit or admission. In addition, some laws prevent certain types of patient information from being released without specific patient permission. Examples include, but are not limited to:
>
> Confidential details of:
>
> - Psychotherapy (from a psychiatrist, licensed psychologist or psychiatric clinical nurse specialist)
> - Other professional services of a licensed psychologist
> - Social Work Counseling
> - Domestic Violence Victims' Counseling
> - Sexual Assault Counseling
> - HIV test results (Patient authorization required for each release request)
>
> Records pertaining to Sexually-Transmitted Diseases
>
> Alcohol and Drug Abuse Records that are protected by Federal Confidentiality Rules

The Partners notice concludes with information about special requirements for release of information by other agencies, with needs for research, and with an invitation for the patient to ask questions.

3.3 Authorization

Covered entities must obtain the individual's written permission as an 'authorization' for uses and disclosures of protected health information that are not otherwise permitted or required under the rule.

3.3.1 Principles

An authorization gives covered entities permission to use specified protected health information for specified purposes, which are generally other than treatment, payment, or healthcare operations, or to disclose such information to a third party specified by the individual.

Authorizations are appropriate in many situations of which two examples follow:

- *Eligibility determinations*. For example, if an individual applies for new coverage with a health plan in the non-group market and the health plan wants to review protected health information from the individual's healthcare providers before extending an offer of coverage, the individual first must authorize the providers to share the information with the health plan. If the individual applies for renewal of existing coverage, however, the health plan would not need to obtain an authorization to review its existing claims records about that individual, because this activity would come within the definition of healthcare operations and be permissible.
- *Employment determinations*. For example, a healthcare provider must obtain the individual's authorization to disclose the results of a pre-employment physical to the individual's employer.

When individuals initiate authorizations**,** they are more likely to understand the purpose of the release and to benefit themselves from the use or disclosure. When a covered entity asks the individual to authorize disclosure, the entity should make clear what the information will be used for, what the individual's rights are, and how the covered entity would benefit from the requested disclosure.

The Privacy Rule essentially identifies one situation in which otherwise routine information cannot be shared with the healthcare team -- that is for *psychotherapy* notes. The rationale for such a special treatment of psychotherapy notes is provided later.

Covered entities may use one authorization form for all purposes. The following are the core elements for a valid authorization:

- a description of the information to be used or disclosed,
- the identification of the persons or class of persons authorized to make the use or disclosure of the protected health information,
- the identification of the persons or class of persons to whom the covered entity is authorized to make the use or disclosure,
- a description of each purpose of the use or disclosure,
- an expiration date or event,
- the individual's signature and date, and
- if signed by a personal representative, a description of his or her authority to act for the individual.

An authorization that does not contain all of the core elements does not meet the requirements for a valid authorization. Additionally, an authorization is not valid unless it contains all of the following:

- a statement that the individual may revoke the authorization in writing, and either a statement regarding the right to revoke, and instructions on how to exercise such right or, to the extent this information is included in the covered entity's notice, a reference to the notice,
- a statement that treatment, payment, enrollment, or eligibility for benefits may not be conditioned on obtaining the authorization if such conditioning is prohibited by the Privacy Rule or, if conditioning is permitted, a statement about the consequences of refusing to sign the authorization, and
- a statement about the potential for the protected health information to be re-disclosed by the recipient.

Although the notification statements are not included in the paragraph on core elements an authorization is not valid unless it contains both the required core elements, and all of the required statements. The required statements must be written in a manner that is adequate to place the individual on notice of the substance of the statements.

Covered entities are required to obtain an authorization to use or disclose protected health information for marketing purposes, and to disclose in such authorizations any direct or indirect remuneration the covered entity would receive from a third party as a result of obtaining or disclosing the protected health information. However, a statement concerning remuneration is not a required notification for other authorizations.

3.3.2 Individual Initiation

Individuals may seek disclosure of their health information to others in many circumstances, such as

- when applying for life or disability *insurance*,
- in seeking certain *job* assignments where health is relevant, and
- in *tort litigation*, where an individual's attorney needs individually identifiable health information to evaluate an injury claim and asks the individual to authorize disclosure of records relating to the injury to the attorney.

The authorization should include a precise description of the information to be used. For example, the authorization could include a description of "laboratory results from July 1998" or "all laboratory results" or "results of MRI performed in July 1998." The covered entity would then use or disclose that information and only that information.

The requirements make it unlikely that an individual could actually initiate a proper authorization, because few individuals would know to include all of the required elements in a request for information. In most instances, individuals authorize release of health information by completing a form provided by another party, either the ultimate recipient of the records (who may have a form authorizing them to request the records from the record holders) or a healthcare provider or health plan holding the records (who may have a form that documents a request for the release of records to a third party).

Individuals may face reluctance on the part of covered entities that receive authorizations requiring them to classify and *selectively disclose* information when they do not benefit from the activity. Individuals would need to consider this when specifying the information in the authorization. Covered entities may respond to requests to analyze and separate information for selective disclosure by providing the entire record to the individual, who may then select and release the information to others.

3.3.3 Valid or Defective

An authorization containing the required elements is valid. A *valid authorization* may contain additional, non-required elements, provided that these elements are not inconsistent with the required elements. Covered entities are not required to use or disclose protected health information pursuant to a valid authorization, but a covered entity that uses or discloses protected health information pursuant to an authorization meeting the applicable requirements will be in compliance with this rule.

An authorization may expire upon a certain event or date. For example, a valid authorization may state that it expires upon acceptance or rejection of an application for insurance or upon the termination of employment (for example, in an authorization for disclosure of protected health information for fitness-for-duty purposes) or similar event. The *expiration event* must, however, be related to the individual or the purpose of the use or disclosure. An authorization that purported to expire on the date when the stock market reached a specified level would not be valid. If the expiration event is known by the covered entity to have occurred, the authorization is defective.

An authorization that the covered entity knows has been revoked is not valid. Although an authorization must be revoked in writing, the covered entity may not always 'know' that an authorization has been revoked. For example, a government agency may obtain an individual's authorization for "all providers who have seen the individual in the past year" to disclose protected health information to the agency for purposes of determining eligibility for benefits. The individual may revoke the authorization by writing to the government agency requesting such revocation. DHHS cannot require the agency to inform all covered entities to which it has presented the authorization that the authorization has been revoked. If a covered entity does not know of the revocation, the covered entity will not violate this rule by acting pursuant to the authorization. At the same time, if the individual does inform the covered entity of the revocation, even orally, the covered entity 'knows' that the authorization has been revoked and can no longer treat the authorization as *valid* under this rule. Thus, in this example, if the individual tells a covered entity that the individual has revoked the authorization, the covered entity 'knows' of the revocation and must consider the authorization defective.

Entities may not condition treatment or payment on individual authorization, except under certain circumstances. Two examples follow:

- Permitting use of protected health information is part of the decision to receive care through a clinical trial, and healthcare providers conducting such trials should be able to condition research-related treatment on the individual's willingness to authorize the use or disclosure of his or her protected health information for research associated with the trial.
- When a covered entity provides treatment for the sole purpose of providing information to a third party, the covered entity may condition the treatment on the receipt of an authorization to use or disclose protected health information related to that treatment. For example, a covered healthcare provider may have a contract with an employer to provide fitness-for-duty exams to the employer's employees. The provider may refuse to conduct the exam if an individual refuses to authorize the provider to disclose the results of the exam to the employer.

Other *exceptions* exist, but the general rule is that authorization is needed.

3.3.4 Authorization Form

A sample authorization form follows.

AUTHORIZATION for RELEASE of INFORMATION

I hereby authorize the use or disclosure of my individually identifiable health information as described below. I understand that this authorization is voluntary. I understand that if the organization authorized to receive the information is not a health plan or healthcare provider, the released information may no longer be protected by federal privacy regulations.

Patient name: ___________________

ID number: ________________

Persons/organizations providing the information: _____________________

Persons/organizations receiving the information: _____________________

Specific description of information (includes dates): ____________________

What is the purpose of the use or disclosure? ___________________________________

If the use or disclosure is for marketing purposes, will the health plan or provider receive financial or in-kind compensation in exchange for using or disclosing the health information described above? yes no

The patient or the patient's representative must read and initial the following statements:

I understand that my healthcare and the payment for my healthcare will not be affected if I do not sign this form. Initials: ___

I understand that I may see and copy the information described on this form if I ask for it, and that I get a copy of this form after I sign it. Initials: ___

The patient or the patient's representative must read and initial the following statements:

I understand that this authorization will expire on __/__/__ (DD/MM/YR) Initials: ____

I understand that I may revoke this authorization at any time by notifying the providing organization in writing, but if I do it won't have any affect on any actions they took before they received the revocation. Initials: ___

Signature of patient or patient's representative: ____________________

Date: _________________

Printed name of patient's representative: __________________

Relationship to the patient: ___________________

- You may refuse to sign this authorization
- You may not use this form to release information for treatment or payment except when the information to be released is psychotherapy notes or certain research information.

END of AUTHORIZATION

3.4 Uses and Disclosures

Main Points

- Policies for minimum necessary use and disclosure should respect the traditional patterns of the roles in healthcare.
- Business associates are not directly covered by HIPAA but the Privacy Rule allows covered entities to share information with business associates.
- De-identification converts protected health information into unprotected health information.

Uses and *disclosures* are foundational concepts in the Privacy Rule. Their meanings are (see Figures "Use" and "Disclosure"):

- 'Use' means the employment, application, utilization, examination, or analysis of protected information within an entity that maintains the information.
- 'Disclosure' means the release, transfer, provision of access to, or divulging in any other manner of protected health information outside the entity holding the information.

In short, 'use' occurs inside an entity, and

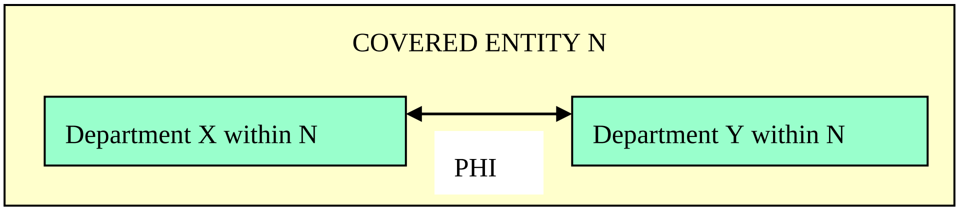


Figure "Use": Department X within the covered entity N is sharing protected health information (PHI) with another Department Y inside the same covered entity -- this is 'use'.

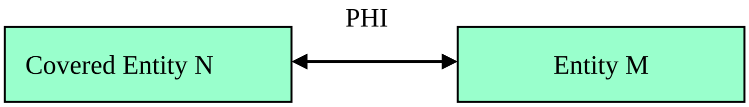


Figure "Disclosure": Covered entity N sends PHI to entity M -- that is 'disclosure'.

'disclosure' occurs outside an entity.

3.4.1 Minimum Necessary Standard

To maximize privacy one wants to control information flow. In some ways this control may be seen as minimizing the flow to that necessary. DHHS requires covered entities to implement policies and procedures for 'minimum necessary' uses and disclosures. Implementation of such policies and procedures is required in lieu of making the 'minimum necessary' determination for each separate use or disclosure. Covered entities can disclose protected health information for the treatment and payment activities of another covered entity or any health care provider, and for certain health care operations of another covered entity. Uses or disclosures for treatment purposes are not subject to the 'minimum necessary' standard.

3.4.1.1 Policy

The *'minimum necessary' standard* has essentially three components:

- first, it does not pertain to certain uses and disclosures including treatment-related exchange of information among healthcare providers;
- second, for disclosures that are made on a routine and recurring basis, such as insurance claims, a covered entity is required to have policies and procedures for governing such exchanges (the rule does not require a case-by-case determination); and
- third, providers must have a process for reviewing non-routine requests on a case-by-case basis to assure that only the minimum necessary information is disclosed.

The policy must generalize the rules about the flow of information.

The Minimum Necessary Standard requires behavior similar to the current practice of many providers. For standard disclosure requests, for example, providers generally have established procedures for determining how much health information is released. For non-routine disclosures, providers currently ask questions to discern how much health information is necessary for such disclosure. To comply with the Minimum Necessary Standard, entities will have to be more thorough in their policies and procedures and more vigilant in their oversight of them.

Entities should establish policies and procedures to limit:

- the *amount of protected health information* used or disclosed to the minimum amount necessary to meet the purpose of the use or disclosure, and
- access to protected health information only to those people who need *access* to the information to accomplish the use or disclosure.

Such limiting of access of course means that the flow of information is constrained.

The responsibility for determining what disclosure is the 'minimum necessary' is on the covered entity making the disclosure. The exception would be for health plan requests for information from healthcare providers for auditing and related purposes. Health plans are responsible for requesting the minimum necessary information. Since the provider is not in a position to negotiate with the payer, the duty would be shifted to the *payer* to request the 'minimum necessary' information for the purpose. Whenever a health plan requests a disclosure, it would be required to limit its requests to the information to achieve the purpose of the request. For example, a health plan seeking protected health information from a provider or other health plan to process a payment should not request the entire health record unless it is actually necessary.

Entity's policies and procedures must provide that disclosure of an entire medical record will not be made except pursuant to policies that specifically justify why the entire medical record is needed. For instance, disclosure of all protected health information to an accreditation group would not necessarily violate the regulation, because the entire record may be the 'minimum necessary' for its purpose; covered entities may establish policies allowing for and justifying such a disclosure. Disclosure of the entire medical record absent such documented justification is a presumptive violation of this rule.

An entity may rely on the assertion of a requesting entity that it is requesting the minimum protected health information necessary for the stated purpose. An entity may also *rely on the assertions* of a professional (such as an attorney or accountant) who is a member of its workforce or its business associate regarding what protected health information he or she needs in order to provide professional services to the covered entity when such person represents that the information requested is the minimum necessary. Covered entities making disclosures to public officials may rely on the representation of a public official that the information requested is the minimum necessary.

3.4.1.2 Roles to Information

An entity should have an organizational manual that indicates the functions of the entity. On any particular day, certain people perform certain

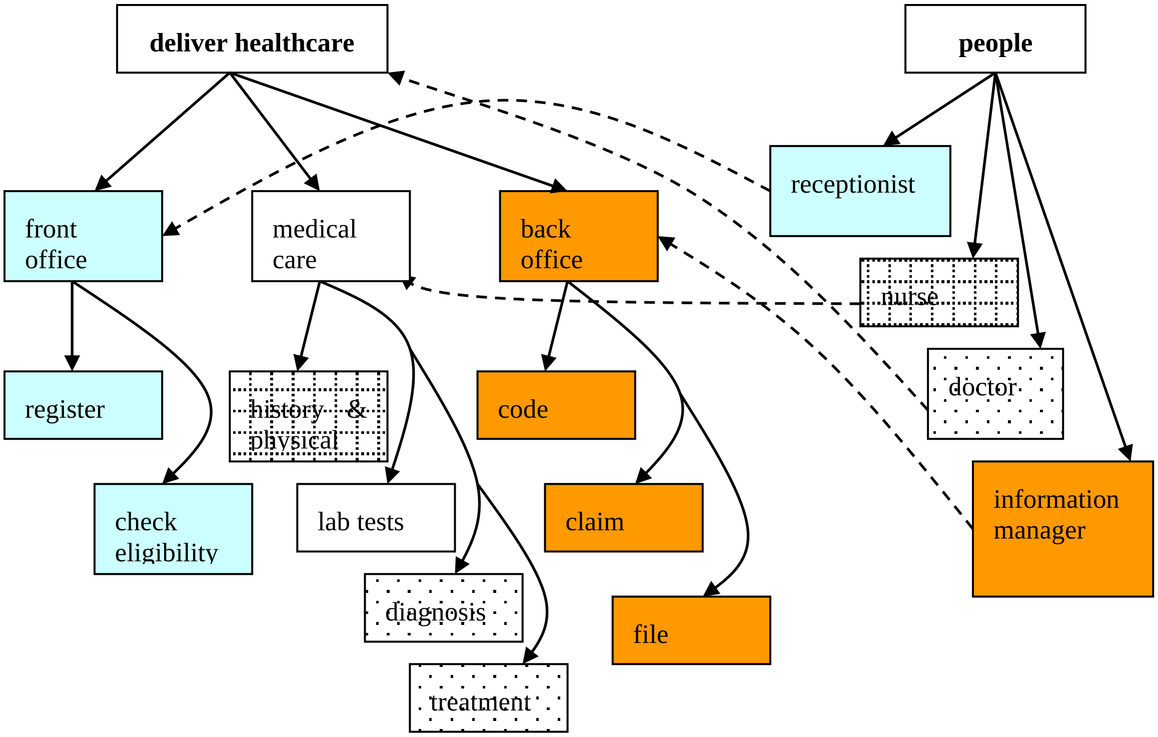


Figure "Roles to Information": The functions of the medical clinic are depicted in the left-hand tree -- three major functions of 'front office', 'medical care', and 'back office' are shown. The roles of the people are shown in the right-hand of the diagram. Each person in a role is expected to use certain types of information.

functions (see Figure "Roles to Information"). This mapping of people to functions is integral to implementing the minimum necessary standard.

An entity must implement policies and procedures to identify the

- persons or classes of persons in the entity's workforce who need access to protected health information to perform their duties,
- categories of protected health information to which such persons or classes need access, and
- conditions, as appropriate, that would apply to such access.

People are grouped or classified according to the functions they serve. In other words, people fill roles. Information is also categorized. Then roles are mapped to information categories. Entities must implement policies and procedures to limit access to only the identified persons, and only to the identified protected health information.

The policies and procedures must be based on reasonable determinations regarding the *roles* that require protected health information, and the nature of the *health information* they require, consistent with their job responsibilities. For example, a hospital could implement a policy that permitted nurses access to all protected health information of patients in their ward while they are on duty. A health plan could permit its underwriting analysts unrestricted access to aggregate claims information for rate setting purposes, but require documented approval from its department manager to obtain specific identifiable claims records of a member for the purpose of determining the cause of unexpected claims that could influence renewal premium rate setting.

For any type of disclosure that is made on a *routine*, recurring basis, an entity must implement policies and procedures that permit only the disclosure of the minimum protected health information reasonably necessary to achieve the purpose of the disclosure. Individual review of each disclosure is not required. For example, a covered entity may decide to participate in research studies and require researchers requesting disclosure of data contained in paper-based records to review the paper records on-site and to abstract only the information relevant to the research. For another example, a standard protocol could describe the subset of information that may be disclosed to medical transcription services.

For *non-routine disclosures*, a covered entity must develop reasonable criteria for limiting disclosure to the minimum amount of protected health information necessary to accomplish the purpose of the disclosure. The entity must implement procedures for reviewing non-routine requests for disclosures on an individual basis. Disclosures to healthcare providers for treatment purposes are not subject to these requirements.

3.4.1.3 Mechanism

Large entities face tougher requirements than small entities. The decisions for determining what would be the minimum necessary information to accomplish an allowable purpose should include the reasonable ability of covered entities to delimit the amount of individually identifiable health information in otherwise permitted uses and disclosures. For example, a *large enterprise* that makes frequent electronic disclosures of similar data would be expected to remove identifiers or to limit the data fields that are disclosed to fit the purpose of the disclosure. An individual *physician's office* would not be expected to have the same capabilities to limit the amount of information disclosed, although, in the cases of disclosures involving a small number of records, such an office could be expected to hide identifiers or to limit disclosures to certain pages of the medical record that are relevant to the purpose of the disclosure.

For paper records, traditional methods may adequately limit disclosure. Two approaches are illustrated:

- One approach relates to *copying*. 'Minimum necessary' disclosure could be accomplished by the selective copying of relevant parts of protected health information or the use of order forms to convey the relevant information. These techniques are already in use in the healthcare environment today, not because of privacy considerations, but because of the risk of losing access to the full medical record when needed for clinic or emergency visits.
- Another approach keeps the medical record under the eye of the entity. For example, if a health researcher wants access to relatively discrete parts of medical records that are presently maintained in paper form for a large number of patients with a certain condition, it could be financially prohibitive for the covered entity to isolate the desired information. However, it could be reasonable for the covered entity to allow the researcher to review the records *on-site* and to abstract only the information relevant to the research. Much records research is done today through such abstracting, and this could be a good way to meet the 'minimum necessary' principle. By limiting the physical distribution of the record, the covered entity would have effectively limited the scope of the disclosure to the information necessary for the purpose.

Minimum necessary disclosure may require removing identifiers. The 'minimum necessary' determination would include a determination that the purpose of the use or disclosure could not be reasonably accomplished with information that is not *identifiable*. Each covered entity would be required to have policies for determining when information must be stripped of identifiers before disclosure. If identifiers are not removed simply because of inconvenience to the covered entity, the 'minimum necessary' rule would be *violated*.

Limiting disclosure is easier with electronic records than with paper records. Technological mechanisms to limit the amount of information available for a particular purpose, and make information available without identifiers, are an important contribution of technology to personal privacy**.** For example, the fields of information that are disclosed can be limited, and identifiers (including names, addresses, and other data) can be removed. Where reasonable (based on the size, sophistication and volume of the covered entity's electronic information systems), covered entities would configure their record systems to allow selective access to different portions of the record, so that, for example, *administrative personnel* get access to only certain fields, and *medical personnel* get access to other fields. This selective access to information would be implemented using the access control technology discussed in the proposed security regulation.

Each covered entity should document the policies and procedures that it will use to meet the privacy requirements. With respect to the 'minimum necessary' standard, such procedures would have to describe how the covered entity will make minimum necessary determinations, the person or persons who will be responsible for making such determinations, and the process in place to periodically review uses and disclosures in light of new technologies or other relevant changes. Proposed uses or disclosures would have to be reviewed by persons who have an understanding of the entity's privacy policies and practices, and who have sufficient expertise to understand and weigh the relevant factors. For large enterprises, the documentation of policies and procedures might identify the general *job descriptions* of the people that would make such decisions throughout the organization.

Routine use does not create a bright line test for determining the minimum necessary amount of protected health information appropriate for most uses or disclosures. Because of this lack of precision, DHHS considered eliminating the requirement altogether. DHHS also considered merely requiring covered entities to address the concept within their internal privacy procedures, with no further guidance as to how each covered entity would address the issue. These approaches were rejected because minimizing both the amount of *protected health information* used and disclosed within the healthcare system and the number of persons who have access to such information is vital to the confidentiality of people's personal health information.

3.4.1.4 Coordination

The Rule on Transactions and Code Sets helps define a common language for healthcare information systems. The Minimum Necessary Standard presents recipes for decision-making. This combination of common language and *decision-making* is the basis of coordination.

Coordination theory says that organizations strive as a top objective to be coordinated (Malone, 1987). Coordination depends first on a common language and then on decision-making. Decision-making depends on an organizational manual and a role hierarchy. The organizational manual describes all the standard processes of the organization. The role hierarchy describes the various roles in the organization and the functions associated with each role. Roles operate on documents in processes that achieve the goals of the organization.

The Rule on Transactions and Code Sets plus the Rule on Privacy are closer than anything else in the United States to a national plan for a coordinated healthcare information system. Such a national plan has long been advocated by certain people as the key to improved efficiency and effectiveness in the American healthcare system. However, prior to now no one has had simultaneously the will to create such a plan and the *power* to implement it.

3.4.1.5 Incidental

The Privacy Rule does not require that all risk of incidental use or disclosure be eliminated. The Privacy Rule explicitly permits certain incidental uses and disclosures that occur as a result of a use or disclosure otherwise permitted by the Privacy Rule. An incidental use or disclosure

- is a secondary use or disclosure that cannot reasonably be prevented,
- is limited in nature, and
- occurs as a by-product of an otherwise permitted use or disclosure.

An incidental use or disclosure is permissible only to the extent that the covered entity had applied reasonable safeguards and implemented the minimum necessary standard. However, an incidental use or disclosure that occurs as a result of a failure to apply reasonable safeguards or the minimum necessary standard, where required, is not a permissible use or disclosure and, therefore, is a violation of the Privacy Rule. For example, a hospital that permits an employee to have unimpeded access to patients' medical records, where such access is not necessary for the employee to do her job, is not applying the minimum necessary standard and, therefore, any incidental use or disclosure that results from this practice would be an unlawful use or disclosure under the Privacy Rule.

The *incidental provision* does not obviate the need for medical staff to take precautions to avoid being overheard, but rather, will only allow incidental uses and disclosures where appropriate precautions have been taken. The provision applies to an incidental use or disclosure to any person, and not just to incidental uses and disclosures resulting from treatment communications or only to communications among health care providers or other medical staff. For example, a provider may instruct an administrative staff member to bill a patient for a particular procedure, and may be overheard by one or more persons in the waiting room. Assuming that the provider made reasonable efforts to avoid being overheard and reasonably limited the information shared, an incidental disclosure resulting from such conversation is permissible under the Rule.

3.4.2 Business Associate

On the one hand, the Privacy Rule says that if an entity wants to disclose protected information, then it needs an authorization. On the other hand, getting authorization for every disclosure would be too burdensome. Thus, the Privacy Rule allows the covered entity to send for certain 'healthcare-serving' purposes 'protected information' to a non-covered entity. However, when protected information is disclosed for 'healthcare-serving' purposes to a non-covered entity, the two entities must have a 'business associate contract' to prevent further disclosure of the information.

3.4.2.1 Conditions

To visualize the 'business associate' concept recall that routine use of protected health information (PHI) among covered entities is allowed with only an acknowledgement of receipt of a Privacy Notice (see Figure "Routine Use"). Under normal circumstances, an authorization is required to share PHI with non-covered entities (see Figure "Authorization Required"). However, under two conditions, PHI can be sent to a non-covered entity without an authorization from the patient -- those two conditions are (see Figure "Business Associate"):

- the PHI will be used for certain healthcare serving purposes (detailed in the Privacy Rule) and
- a business associate contract is agreed between the covered entity sending the PHI and the non-covered entity receiving the PHI.

A business associate uses protected health information of a covered entity. In more detail, a business association occurs when the right to use or disclose the protected health information belongs to the covered entity, and another person is using or disclosing it to perform a function on behalf of the covered entity. 'Business associate' services include (but are not limited too) legal, actuarial, accounting, consulting, management, administrative accreditation, data aggregation, and financial services. Business associate relationships occur in those cases in which the covered entity is disclosing information to someone or some organization that will use the information on behalf of the covered entity. A *business associate* cannot be part of the covered entity's workforce.

Where a physician or other provider has *staff privileges* at an institution, neither party to the relationship is a business associate based solely on the staff privileges because neither party is providing functions or activities on behalf of the other. However, if a party provides services to or for the other, such as where a hospital provides billing services for physicians with staff privileges, a business associate relationship may arise with respect to those services.

Oversight agencies are not business associates. Covered entities are permitted to disclose protected health information to oversight agencies that act to provide oversight of federal programs and the healthcare system. These *oversight agencies* are not performing services for or on behalf of the covered entities and so are not business associates of the covered entities. Therefore the federal agency that administers Medicare is not required to enter into a business associate contract in order to disclose protected health information to the DHHS's Office of Inspector General.

While a business associate may be a covered entity, the mere fact that two covered entities participate in an organized healthcare arrangement does not make either of the covered entities a business associate of the other covered entity. The fact that the entities participate in *joint healthcare operations* or other joint activities, or pursue common goals through a joint activity, does not mean that one party is performing a function on behalf of the other.

A covered entity is not required to enter into a business associate contract with a person or organization that acts merely as a *conduit for protected health information* (e.g., the US Postal Service or certain private couriers). A financial institution is not acting on behalf of a covered entity, and therefore no business associate contract is required, when it clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for compensation for healthcare.

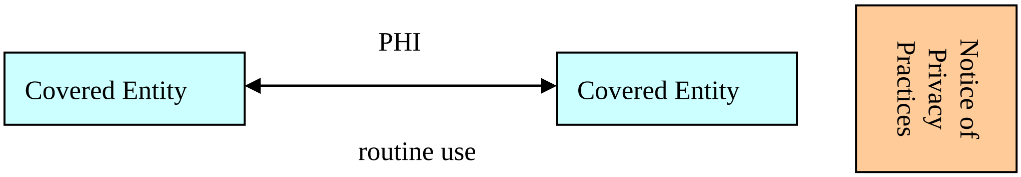


Figure "Routine Use": PHI is protected health information. Covered entities can share PHI for routine use (payment, treatment, and healthcare operations) after the patient acknowledges receipt of a Notice of Privacy Practices.

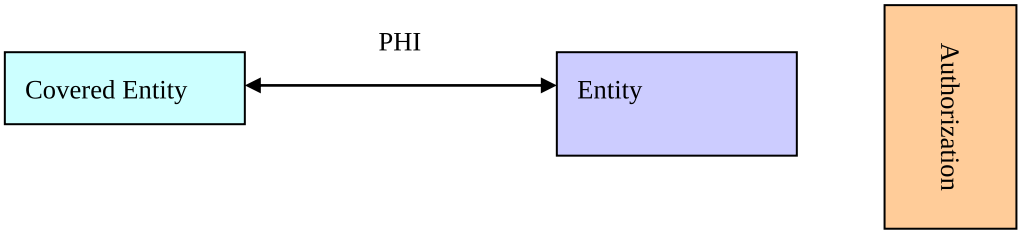


Figure "Authorization Required": A covered entity can send PHI to another entity with an authorization.

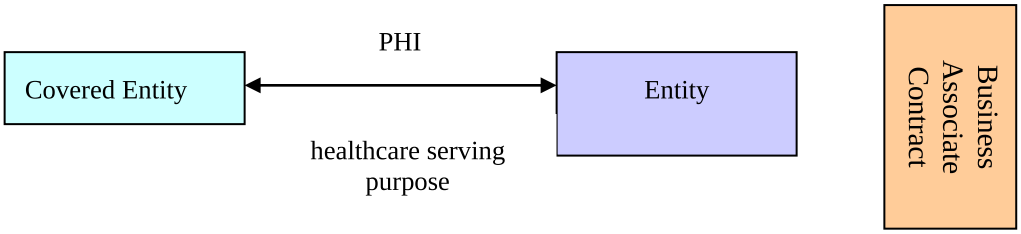


Figure "Business Associate": A covered entity can send PHI to any other entity for certain healthcare serving purposes when a 'business associate' contract has been signed.

Data aggregation services may give rise to a business associate relationship. *Data aggregation* is where a business associate of one covered entity combines the protected health information of such covered entity with protected health information received by the business associate in its capacity as a business associate of another covered entity in order to permit the creation of data for analyses that relate to the healthcare operations of the respective covered entities. For example, a state hospital association could act as a business associate of its member hospitals and could combine data provided to it to assist the hospitals in evaluating their relative performance in areas such as quality, efficiency, and other patient care issues. The business associate contracts of each of the hospitals would have to permit the activity, and the protected health information of one hospital could not be disclosed to another hospital.

3.4.2.2 Contracts

A contract between the covered entity and a business associate must provide that the business associate will:

- Not use or further disclose the information other than as permitted or required by the contract or as required by law;
- Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;
- Ensure that any agents, including a subcontractor, to whom it provides the protected health information agrees to the same restrictions that apply to the business associate;
- Make its internal practices, books, and records relating to the use and disclosure of the protected health information available to DHHS for purposes of determining the covered entity's compliance with this subpart.
- At termination of the contract, if feasible, return the protected health information.

Covered entities have certain responsibilities relative to their business associates. The covered entity is subject to *sanctions*, if it has knowledge of a business associate's wrongful activity and fails to address the wrongdoing. If a business associate maintains the medical records or manages the claims system of a covered entity, the covered entity must ensure that individuals who are the subject of the information can have access to it.

The Business Associate Contract is a major concern for large covered entities that engage in multiple contracts with vendors. To lessen the effort expected of any particular entity, a sample contract is provided next.

THIS CONTRACT is entered into on this _________ day of _________ between ______________ ("ENTITIY") and ______________ ("ASSOCIATE").

WHEREAS, ENTITY will make available to ASSOCIATE certain Information that is confidential and must be afforded special treatment and protection.

WHEREAS, ASSOCIATE will have access to and/or receive from ENTITY certain Information that can be used or disclosed only in accordance with this Contract and the HHS Privacy Regulations.

NOW, THEREFORE, ENTITY and ASSOCIATE agree as follows:

1. The term of this Contract shall commence as of ______ (the "Effective Date"), and shall expire when all of the Information provided by ENTITY to ASSOCIATE is destroyed or returned to ENTITY.

2. The Parties hereby agree that ASSOCIATE shall be permitted to use and/or disclose Information provided or made available from ENTITY for the following stated purposes:

   ____
   ____
   ____

3. ASSOCIATE OBLIGATIONS:

   a. ASSOCIATE hereby agrees that the Information provided or made available by ENTITY shall not be further used or disclosed other than as permitted or required by the Contract or as required by law and that appropriate safeguards will be in place
   b. ASSOCIATE hereby agrees that it shall report to ENTITY within two (2) days of discovery any use or disclosure of Information not provided for or allowed by this Contract.
   c. ASSOCIATE hereby agrees that anytime Information is provided or made available to any subcontractors or agents, ASSOCIATE must enter into a subcontract with the subcontractor or agent that contains the same terms, conditions and restrictions on the use and disclosure of Information as contained in this Contract.
   d. ASSOCIATE hereby agrees to make available and provide a right of access to Information by an Individual, to make Information available for amendment and to incorporate any amendments to Information, and to provide an accounting of disclosures in accordance with the Privacy Rule.
   e. ASSOCIATE hereby agrees to make its internal practices, books, and records relating to the use or disclosure of Information received from, or created or received by ASSOCIATE on behalf of the ENTITY, available to HHS for purposes of determining compliance with the HHS Privacy Regulations.
   f. ASSOCIATE agrees to have procedures in place for mitigating, to the maximum extent practicable, any deleterious effect from the use or disclosure of Information in a manner contrary to this Contract or the HHS Privacy Regulations.

4. ASSOCIATE agrees that ENTITY has the right to immediately terminate this Contract and seek relief if ENTITY determines that ASSOCIATE has violated this Contract.

IN WITNESS WHEREOF, ASSOCIATE and ENTITY have caused this Contract to be signed and delivered by their duly authorized representatives, as of the date set forth above.

ASSOCIATE

By:________________

Print Name:________________

Title:______________________

ENTITY

By:____________________

Print Name:_______________

Title:____________________

3.4.3 De-identification

The Privacy Rule applies to 'individually identifiable health information' and not to de-identified information. The statute defines individually identifiable health information as certain health information:

- Which identifies the individual, or
- With respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

De-identified information may be valuable for various purposes. Difficulties arise because, even after removing obvious identifiers (e.g., name, social security number, address), there is some probability that information about an individual can be attributed to that individual.

3.4.3.1 Safe Harbor

The de-identification method can use a statistically-sound technique or the Safe Harbor specifications. In further detail:

- One way is if a person with appropriate experience applying generally accepted statistical and scientific methods makes a determination that the risk is very small that the information could be used, either by itself or in combination with other available information, to identify a subject of the information. The covered entity must also document the analysis that justifies the determination.
- The other method is the safe harbor. Under the safe harbor, a covered entity is considered to have met the standard, if it has removed all of a list of enumerated identifiers.

The safe harbor allows age, some geographic location information, and some demographic information to be included in the de-identified information. All dates directly related to the subject of the information must be removed or limited to the year, and zip codes must be removed or aggregated (in the form of 3-digit zip codes) to include at least 20,000 people. Extreme ages of 90 and over must be aggregated to a category of 90+ to avoid identification of very old individuals. These identifiers must be *removed*:

- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- License numbers;
- Vehicle identifiers;
- Device identifiers;
- Web Universal Resource Locators;
- Internet Protocol address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code.

The safe harbor provides a means to produce de-identified information that could be used for many purposes with a very small risk of privacy violation. The safe harbor involves a minimum of burden and conveys a maximum of certainty that the rules have been met with an easily followed, cookbook approach.

Covered entities may use codes to mark records so that they may later be re-identified, if the code does not contain information about the subject of the information. For example, the code may not be a derivative of the individual's social security number. The covered entity is prohibited from disclosing the mechanism for *re-identification*.

3.4.3.2 Limited Data Set

To some the de-identification safe harbor of the Privacy Rule is too restrictive. DHHS addressed this concern by permitting the creation and disclosure of a *limited data set*. The use or disclosure of any such limited data set is restricted to research, public health, and health care operations purposes only. The implementation specifications do not delineate the data that can be released through a limited data set. Rather, the Rule specifies the direct identifiers that must be removed for a data set to qualify as a limited data set. From the de-identification safe harbor list of identifiers, the following direct identifiers have to be removed from any limited data set: name, street address, telephone and fax numbers, e-mail address, social security number, certificate/license number, vehicle identifiers and serial numbers, URLs and IP addresses, and full face photos and any other comparable images. The limited data set could include the following identifiable information: admission, discharge, and service dates; date of death; age (including age 90 or over); and five-digit zip code.

DHHS does not include in the list of direct identifiers the *catch-all* category from the de-identification safe harbor of 'any other unique identifying number, characteristic or code." While this requirement is essential to assure that the de-identification safe harbor does in fact produce a de-identified data set, it is difficult to define in advance in the context of a limited data set. The goal in establishing a limited data set is not to create de-identified information.

To support privacy, the covered entity must enter into a *data use agreement* with the intended recipient which

- establishes the permitted uses and disclosures of such information by the recipient, consistent with the purposes of research, public health, or health care operations,
- limits who can use or receive the data, and
- requires the recipient to agree not to re-identify the data or contact the individuals.

In addition, the data use agreement must contain adequate assurances that the recipient use appropriate safeguards to prevent use or disclosure of the limited data set other than as permitted by the Rule and the data use agreement, or as required by law. These adequate assurances are similar to the requirements for business associate agreements.

3.4.4 Review Questions

1. Why might a mapping of roles to information responsibilities and enforcing of the mapping achieve the effect of 'minimum necessary use'?
2. What must be contained in a contract between a business associated and a covered entity?
3. What is the 'safe harbor' for de-identification of patient information?

3.5 Special Opportunities

Main Points

- Despite the general guidance of the Notice of Privacy Practices and authorizations, individuals do have opportunities to object to the general guidance and to achieve another result.
- The default inclusion of some information in facility directories can be voided, the passing of information to guardians can be changed, and psychotherapy notes have a special category.
- The opportunity to object does not exist in some other circumstances. Military members may have their records shared with superiors, research may be done with records when approved by a review board, and certain marketing is allowed.

The Privacy Rule creates general categories of protected health information, including:

- Routine use;
- Authorization required;
- No authorization required, but an individual has a chance to object; and
- No authorization required, and there is no opportunity to object.

3.5.1 Opportunity to Object

Special opportunities to object to a default process are explained next.

3.5.1.1 Facility Directories

Healthcare providers may include patient information in their directory only if:

- they inform incoming patients of their policies regarding the directory; or
- they give patients a meaningful opportunity to opt-out of the directory listing or to restrict its uses and disclosures.

A patient must be allowed, for example, to have his or her name and condition included in the *directory* while not having his or her religious affiliation included. The provider's notice and the individual's opt-out or restriction may be oral.

Subject to the individual's right to object, a covered healthcare provider (also known as a 'facility' in the context of a directory) may disclose the following information to persons who inquire about the individual by name:

- the individual's general condition in terms that do not communicate specific medical information about the individual (e.g., fair, critical, stable, etc.); and
- location in the facility.

Provisions for disclosure of directory information to clergy are slightly different from those that apply for disclosure to the general public. Subject to the individual's right to object or restrict the disclosure, the rule permits an entity to disclose to a member of the *clergy*:

- the individual's name;
- the individual's general condition in terms that do not communicate specific medical information about the individual;
- the individual's location in the facility; and
- the individual's religious affiliation.

A disclosure of directory information may be made to members of the clergy even if they do not inquire about an individual by name. The rule in no way requires a healthcare provider to inquire about the religious affiliation of an individual, nor must individuals supply that information to the facility. Individuals are free to determine whether they want their religious affiliation disclosed to clergy through facility directories.

Directory disclosures are allowed when patients are incapacitated or in emergency treatment circumstances. For example, when a patient is conscious and capable of making a decision, but is so seriously *injured* that asking permission to include his or her information in the directory would delay treatment, health facilities can make decisions about including the patient's information in the directory.

3.5.1.2 Other Persons

Entities may disclose information to a person involved in the patient's healthcare. The Privacy Rule includes separate provisions for situations in which the patient is *present* and for when the patient is not present at the time of disclosure. When the patient is present and has the capacity to make his or her own decisions, an entity may disclose protected health information only if the entity:

- obtains the patient's agreement to disclose to the third parties involved in their care;
- provides the patient with an opportunity to object to such disclosure and the patient does not express an objection; or
- reasonably infers from the circumstances that the patient does not object to the disclosure.

Situations in which providers may infer a patient's agreement to disclose protected health information include, for example, when a patient brings a spouse into the doctor's office when treatment is being discussed, and when a colleague or friend has brought the individual to the emergency room for treatment.

Entities may notify family members, personal representatives, or other persons responsible for an individual's care with respect to an individual's location, condition, or death. These provisions allow, for example, entities to notify a patient's adult child that the *parent* has suffered a stroke and to tell the person that the parent is in the hospital's intensive care unit.

3.5.1.3 Restriction

Entities must permit individuals to request that uses and disclosures of protected health information for treatment, payment, and healthcare operations be restricted and must adhere to restrictions to which they have agreed. An entity is not required to agree to a *restriction*. For example, if an individual requests that an entity never disclose protected health information to a particular family member, and the entity agrees to that restriction, the entity is prohibited from disclosing protected health information to that family member, even if the disclosure would otherwise be permissible. An entity should consider the need for access to protected health information for treatment purposes when considering a request for a restriction, discuss this need with the individual making the request for restriction, and agree to restrictions that should not impede the individual's treatment.

An entity must document a restriction to which it has agreed. DHHS does not require a specific form of documentation; a note in the medical record or similar notation is sufficient. The *documentation* must be retained for six years from the date it was created or the date it was last in effect, whichever is later.

Restrictions may be terminated in two ways:

- An entity may terminate a restriction with the individual's written or oral agreement. If the individual's agreement is obtained orally, the covered entity must document that agreement. A note in the medical record or similar notation is sufficient documentation. If the individual agrees to terminate the restriction, the entity may use and disclose protected health information as otherwise permitted under the rule.

- If the entity wants to terminate the restriction without the individual's agreement, it may only *terminate the restriction* with respect to protected health information it creates or receives after it informs the individual of the termination. The restriction continues to apply to protected health information created or received prior to informing the individual of the termination. That is, any protected health information that had been collected before the termination may not be used or disclosed in a way that is inconsistent with the restriction, but any information that is collected after informing the individual of the termination of the restriction may be used or disclosed as otherwise permitted under the rule.

Emergencies may over-ride the exception. In emergency treatment situations, an entity that has agreed to a restriction may use or disclose to a healthcare provider, restricted protected health information that is necessary to provide the emergency treatment. If the entity discloses restricted protected health information to a healthcare provider for *emergency treatment purposes*, it must request that the provider not further use or disclose the information.

3.5.1.4 Psychotherapy

The general principle is that all information is equally sensitive. The Privacy Rule generally would not require covered entities to vary the level of protection of protected health information based on the sensitivity of such information. Psychotherapy notes are an exception.

'Psychotherapy notes' document conversation during a counseling session led by a mental health professional. Such notes can be used only by the therapist who wrote them, have to be maintained separately from the medical record, and can not be involved in the documentation necessary for healthcare treatment, payment, or operations. *Psychotherapy notes* do not include medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, or summaries of diagnoses.

Psychotherapy notes are subject to unique rules of disclosure. Psychotherapy notes are of primary value to the specific provider, and the promise of strict confidentiality helps to ensure that the patient will feel comfortable disclosing very personal information essential to successful treatment. Unlike information shared with other healthcare providers for the purposes of treatment, psychotherapy notes are more detailed and *subjective*.

As the *Judicial Conference Advisory Committee* observed in 1972 when it recommended that Congress recognize a psychotherapist privilege as part of the Proposed Federal Rules of Evidence, a psychiatrist's ability to help a patient

> is completely dependent upon [the patients'] willingness and ability to talk freely. This makes it difficult if not impossible for [a psychiatrist] to function without being able to assure . . . patients of confidentiality and, indeed, *privileged communication*. . . . there is wide agreement that confidentiality is a sine qua non for successful psychiatric treatment. ...

Protecting confidential communications between a psychotherapist and a patient from involuntary disclosure is important.

Use of psychotherapy notes by other than the psychotherapist requires specific permission. A healthcare provider is not permitted to disclose psychotherapy notes for treatment, payment, or healthcare operations unless a *specific authorization* is obtained from the individual. In addition, an entity is not permitted to condition treatment of an individual on a requirement that the individual provide a specific authorization for the disclosure of psychotherapy notes. An authorization is not required for use or disclosure of psychotherapy notes when required for enforcement purposes; when mandated by law; when needed for oversight of the healthcare provider who created the psychotherapy notes; when needed by a coroner or medical examiner; or when needed to avert a serious and imminent threat to health or safety.

3.5.2 No Opportunity to Object

Privacy is surrendered in some situations. Entities may use protected health information without individual authorization for certain categories of uses to permit and promote *national healthcare priorities*. Entities are permitted to use or disclose an individual's protected health information:

- when required by law;
- for public health activities;
- about victims of abuse, neglect, or domestic violence;
- for health oversight activities;
- for judicial and administrative proceedings;
- for law enforcement purposes;
- about decedents;
- to comply with workers' compensation laws;

- for donation of organs, eyes, or tissues;
- to avert a serious threat to health or safety;
- for research purposes;
- for specialized government functions (such as military personnel, and inmates in correctional facilities); and
- for certain marketing purposes.

Three cases (the last three in the preceding list) where information can be shared without authorization are detailed next. The reasoning behind and specifics of these cases are given, and the reader can infer some of the reasoning and specifics of the other cases from these three.

3.5.2.1 Research

Information may be disclosed to researchers through means other than a patient authorization. The authors of the Privacy Rule believe that

- important life-saving information comes from research that uses individually identifiable health information and
- researchers may not practically be able to obtain the authorization of every subject they should include within a study.

Often, thousands of records are involved and identification and contacting subjects to obtain authorization may not be practical. The rule allows entities to use information for research without individual authorization provided that the *researcher's protocol* has been approved by an Institutional Review Board (IRB) or a Privacy Board (the two terms will be combined henceforth in this section and simply called IRB). Absent such review, the information can only be used with the patient's prior authorization.

An IRB uses the following criteria to decide whether or not to grant a waiver of patient authorization:

- the use or disclosure of protected health information involves no more than minimal risk to the privacy of the individual;
- the research could not practicably be conducted without the waiver; and
- the research could not practicably be conducted without access to the protected health information.

In performing the *minimal privacy risk analysis*, IRBs must consider whether there is:

- an adequate plan to protect the identifiers from improper use or disclosure;
- an adequate plan to destroy the identifiers at the earliest opportunity, unless retention of identifiers is required by law or is justified by research or health issues; and
- adequate written assurance that the protected health information will not be used or disclosed to a third party except as required by law or permitted by an authorization.

This emphasis on privacy in IRB approvals did not exist prior to the Privacy Rule.

Authorizations also have special status for research which reduces, however, some control of patients:

- By way of an exception to the general rule forbidding compound authorizations, authorizations for research may be combined with an informed consent to participate in the research study, another authorization, or any other legal permission related to the research.
- Research authorizations may omit a date for the authorization expiring. 'No expiration date' or 'none' may be used in authorizations for any research study.
- While an individual may revoke his or her authorization that information be used and disclosed for research purposes, covered entities may continue to use or disclose information collected prior to the revocation as necessary to maintain the integrity of the research study. Examples of permitted disclosures include submissions of marketing applications to the FDA, reporting of adverse events, accounting of the subject's withdrawal from the study and investigation of scientific misconduct.

These relaxations of the authorization requirements for research facilitate research at the expense of patient privacy.

3.5.2.2 Military

The *military healthcare system*, like other federal and civilian healthcare systems, provides medical care to its beneficiary population. However, it also serves a critical national defense purpose, ensuring that the Armed Forces are in a state of medical readiness to permit the discharge of those responsibilities. The primary purpose of the healthcare system of the military services differs in its basic character from that of the healthcare system of society in general. The special nature of military service is acknowledged by the Constitutional provision for separate lawmaking for them. To address the special circumstances of the Armed Forces and their healthcare systems, military providers may disclose protected health information about soldiers for certain purposes.

In all environments, operational or otherwise, the Armed Forces may want to assure that its personnel are medically qualified to perform their responsibilities. Each and every person may perform a vital service upon which others must rely in executing a specified military requirement. Unqualified personnel not only *jeopardize* the possible success of an assignment or operation, but they pose a risk and danger to others.

To assure that such persons are *medically fit*, health information is provided to proper command authorities regarding military members performing certain critical functions for medical screening and other purposes so that determinations can be made regarding the ability of such military personnel to perform assigned duties. For example, health information is provided regarding:

- A pilot receiving medication that may affect alertness;
- An Armed Forces member with an intolerance for a vaccine necessary for deployment to certain geographical areas;
- Any significant medical or psychological changes in a military member who is a member of the Nuclear Weapons Personnel Reliability Program;
- A military recruit or member with an illness or injury which disqualifies him or her from military service; and
- Compliance with controlled substances policies.

The military and the Coast Guard obtain such information from their own healthcare systems, as well as from other agencies that provide *healthcare to service members*. Other healthcare providers could also provide information, for example, when a private sector physician treats a member injured in an accident.

3.5.2.3 Marketing

Any covered entity must obtain the individual's authorization before using protected health information for marketing. However, DHHS has defined 'marketing' so as to allow certain 'marketing communications'. Certain activities, such as communications made by an entity for the purpose of describing the products and services it provides, are not marketing. A covered entity may use or disclose protected health information to make a marketing communication (DWT, 2002):

- if communication occurs in a face-to-face encounter with the individual. This provision would permit a covered entity to discuss any services and products, including those of a third-party, without restriction during a face-to-face communication. A covered entity also could give the individual sample products or other information in this setting.
- if products or services have only nominal value. This provision ensures that covered entities do not violate the rule when they distribute calendars, pens and other merchandise that generally promotes the covered entity.
- for case management or care coordination, or to direct or recommend alternative treatments, therapies, health care providers, or care settings.

Covered entities may also use protected health information to communicate with members about health insurance products offered by the covered entity that could enhance or substitute for existing health plan coverage. For example, if a child is about to age out of coverage under a family's policy, this provision will allow the plan to send the family information about continuation coverage for the child. A health plan is also not engaging in marketing when communicating about health-related products and services available only to members that add value to, but are not part of, a plan of benefits. To qualify for this exclusion, a value-added item or service must meet two conditions. First, the value-added item or service must be health related. Second, it must add value to the plan's membership alone, rather than being a pass through of something available to the public at large.

The marketing provisions allow the use of health information for commercial communications that some consider marketing. For instance, the regulation permits pharmacies to receive money from drug manufacturers to data-mine patient prescriptions and to send to targeted patients' letters encouraging them to switch to the manufacturer's brand of drug. These communications are not necessarily based on a determination of what is medically best for the patient but are sent due to financial incentives. Since this activity is not defined as 'marketing' in the Privacy Rule, pharmacies do not have to obtain the patients' authorization (Health, 2002). The authorization requirement applies to materials that encourage the purchase or use of products and services that are not related to health care. Furthermore, in the above scenario, pharmacies never have to give patients an opportunity to be removed from the mailing list. Nor do they have to tell patients that the drug company is paying them to send the letters (see Table "Marketing versus Non-marketing").

DHHS defines fundraising on behalf of a covered entity to be a healthcare operation and not marketing. DHHS permits a covered entity to use protected health information without individual authorization for fundraising on behalf of itself, provided that it limits the information that it uses to demographic information about the individual and the dates that it has provided service to the individual. In addition, fundraising materials must explain how the individual may opt out of any further fundraising communications. DHHS permits a covered entity to disclose limited protected health information to a business associate for fundraising on the covered entity's behalf.

Table "Not Marketing versus Marketing": Advertising health related products is sometimes not considered marketing, as the first row illustrates. The second row shows an example of marketing.

Not Marketing Principle: Paid to recommend health-related product or service. Example: Drug company pays pharmacy to identify patients taking certain drugs and to send letters encouraging them to switch to drug company's brand. Requirements: • no authorization, • no opportunity to object, • no notification provided that covered entity is paid to encourage purchase, and • no identification of source of material.
Marketing Principle: Paid to recommend product or service not related to health. Example: Pharmacy is paid by third party to identify patients taking depression medication and to send them advertisements for vacation destinations. Requirements: Authorization

3.5.3 Review Questions

1. What options must a hospital give a patient concerning the listing of the patient in the facility directory?
2. What exceptions are granted in terms of routine use for reports on psychological 'diseases'?
3. In what sense may an 'Institutional Review Board' take the place of a patient authorization for a researcher?
4. What exceptions are granted to commander in the military as regards the privacy of the medical records of the troops reporting to the commander?

3.6 Patient Rights

Main Points

- Patients have a right to access their medical record.
- Patients may request that communications occur along confidential channels.
- Patients have a right to amend the medical record.
- Patients have a right to an accounting of the disclosures of their medical record.

The access, amend, and account provisions allow the patient to see and change the medical record. The access, amend, and account provisions may empower patients to become more involved in their healthcare. What are these provisions?

3.6.1 Access to Information

What rights does a person to have to see her own medical records? Under what conditions can a healthcare organization deny a person such access? In what forms may the access be expected?

3.6.1.1 Right of Access

The definition of the right of access is linked to the definition of a designated record set. What is a '*designated record set*'? A 'record' is 'any item, collection, or grouping of protected health information maintained, collected, used, or disseminated by a covered entity.' Designated record sets are any group of records that are used, in whole or in part, by or for a covered entity to make decisions about individuals. This information includes, for example, information used to make healthcare decisions or information used to determine whether an insurance claim will be paid. Two examples follow:

- For health plans, designated record sets include, at a minimum, the enrollment, payment, claims adjudication, and case or medical management record systems of the plan.
- For healthcare providers, designated record sets include, at a minimum, the medical record and billing record about individuals maintained by or for the provider.

Records that otherwise meet the definition of designated record set and which are held by a business associate of the covered entity are part of the covered entity's designated record sets.

Individuals have a right of access to any protected health information that is maintained in a designated record set. This right of access applies to health plans, healthcare providers, and healthcare clearinghouses that create or receive protected health information. Covered entities must provide *access* to individuals for as long as the protected health information is maintained in a designated record set.

Entities often incorporate the same protected health information into a variety of different data systems, not all of which will be utilized to make *decisions about individuals*. For example, information systems that are used for quality control or peer review analyses may not be used to make decisions about individuals. In that case, the information systems would not fall within the definition of designated record set. Entities do not need to grant an individual access to information systems not used to make decisions about individual patients.

For three types of information, individuals do not have a right of access, even if the information is maintained in a designated record set. They are:

- psychotherapy notes,
- information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding, and
- certain protected health information maintained by a covered entity that is subject to or exempted from the Clinical Laboratory Improvements Amendments of 1988.

Covered entities may, but are not required to, provide access to this information.

3.6.1.2 Denial of Access

An entity may deny access to protected health information under three circumstances. These circumstances occur when the *physical safety* of an individual is endangered:

- First, entities may deny individuals access to protected health information if a licensed healthcare professional has determined that the access requested is reasonably likely to endanger the physical safety of the individual or another person. The most commonly cited example is when an *individual* exhibits suicidal or homicidal tendencies. If a licensed healthcare professional determines that an individual exhibits such tendencies and that permitting inspection or copying of some of the individual's protected health information is reasonably likely to result in the individual committing suicide, murder, or other physical violence, then the healthcare professional may deny the individual access to that information. Under this reason for denial, entities may not deny access on the basis of the sensitivity of the health information or the potential for causing emotional or psychological harm.

- Second, entities may deny an individual access to protected health information if the information requested makes reference to someone other than the individual (and other than a healthcare provider) and a licensed healthcare professional has determined that the access requested is reasonably likely to cause serious harm to that *other person*. On some occasions when health information about one person is relevant to the care of another, a physician may incorporate it into the latter's record, such as information from group therapy sessions and information about illnesses with a genetic component. This provision permits an entity to withhold information in such cases if the release of such information is reasonably likely to cause substantial physical, emotional, or psychological harm.
- Third, entities may refuse to treat a personal representative as the individual, generally, if the entity has a reasonable belief that treating the personal representative as the individual may endanger the individual, and decides not to treat such person as the *personal representative*.

DHHS intends narrow exceptions to the right of access and expects entities to employ these exceptions rarely, if at all. Covered entities may only deny access for the reasons specifically provided in the Rule.

If the entity denies the request, the individual has the right to have the denial reviewed by a licensed healthcare professional. The *reviewer* is designated by the entity to act as a reviewing official and did not participate in the original decision to deny access. The entity must provide access in accordance with the reviewing official’s determination.

3.6.1.3 Provision

If an entity accepts a request, in whole or in part, it must notify the individual of the decision and provide the access requested. Individuals have the right both to *inspect* and to *copy* protected health information in a designated record set. The individual may choose whether to inspect the information, to copy the information, or to do both.

If the same protected health information is maintained in more than one designated record set or at more than one location, the covered entity is required to produce the information only once per request for access. Summary information and reports are not the same as the underlying information on which the summary or report was based. Individuals have the right to access both summaries and the underlying information. An individual retains the right of access to the underlying information even if the individual requests access to, or production of, a *summary*.

The entity must provide the information in the form or format requested, if it is readily producible in such form or format. For example, if the entity maintains health information electronically and the individual requests an electronic copy, the entity must accommodate such request, if possible. Additionally, if the information is not available in the *form* or *format* requested, the entity must produce a readily readable hard copy of the information or another form or format to which the individual and entity can agree. If the individual agrees, including agreeing to any associated fees, the entity may provide access to a summary of information rather than all protected health information in designated record sets. Similarly, an entity may provide an explanation in addition to the protected health information, if the individual agrees in advance to the explanation and any associated fees.

The entity must arrange for a mutually convenient time and place for the individual to inspect the protected health information or obtain a copy. If the individual requests that the entity mail a copy of the information, the entity must do so, and may charge certain fees for copying and mailing. Entities may discuss the request with the individual as necessary to facilitate the timely provision of access. For example, if the individual requested a copy of the information by mail, but the entity is able to provide the information faster by providing it *electronically*, the entity may discuss this option with the individual.

If the individual requests a copy of protected health information, an entity may charge a reasonable, cost-based fee for the copying, including the labor and supply costs of copying. If hard copies are made, this would include the cost of paper. If electronic copies are made to a computer disk, this would include the cost of the computer disk. If the individual requests the information to be mailed, the *fee* may include the cost of postage.

Entities may not charge any fees for retrieving or handling the information or for processing the request. The inclusion of a *fee for copying* is not intended to impede the ability of individuals to copy their records. Rather, it is intended to reduce the burden on entities. If the cost is excessively high, some individuals will not be able to obtain a copy. Entities should limit the fee for copying so that it is within reach of all individuals.

Access must be provided:

- within 30 days of receiving the request if the information is accessible on-site or
- within 60 days of receiving the request if the information is not accessible on-site.

If the entity is unable to act on a request within the applicable deadline, it may extend the deadline by no more than 30 days by providing the individual with a written statement of the reasons for the delay and the date by which the entity will complete its action on the request. This written statement describing the extension must be provided within the standard deadline. An entity may only extend the *deadline* once per request for access. This provision permits an entity to take a total of up to 60 days to act on a request for access to information maintained on-site and up to 90 days to act on a request for access to information maintained off-site.

3.6.2 Confidential Communications

Entities must permit an individual to request a confidential communication channel. The requirement applies to communications from the entity to:

- the individual, and
- the named insured of an insurance policy that covers the individual as a dependent of the named insured.

Individuals may request that the entity send such communications by alternative means or at alternative locations. For example, an individual who does not want his or her family members to know about a certain treatment may request that the provider communicate with the individual about that treatment at the individual's place of employment, by mail to a designated address, or by phone to a designated phone number. Similarly, an individual may request that the provider send communications in a closed envelope rather than a post card, as an *alternative means*.

Health plans must accommodate all administratively feasible requests, if the individual states that the disclosure of the protected health information could endanger the individual. For example, if an individual requests that a health plan send explanations of benefits about particular services to the individual's work rather than home address because the individual is concerned that a member of the individual's household (e.g., the named insured) might read the explanation of benefits and become abusive towards the individual, the health plan must accommodate the *request*.

The administrative feasibility of a request must be determined by an entity on the basis of the administrative difficulty of complying with the request. A healthcare provider or health plan *cannot refuse* to accommodate a request based on its perception of the merits of the individual's reason for making the request. A healthcare provider may not require the individual to provide a reason for the request as a condition of accommodating the request.

3.6.3 Right to Amend

The individual may request to amend protected health information about the individual for as long as the covered entity maintains the information.

3.6.3.1 Amending

Entities may specify the form and content of the amending request. If an entity informs individuals of such requirements in advance, the entity may require individuals to make *requests for amendment* in writing and to provide a reason to support a requested amendment. If the entity imposes such a requirement and informs individuals of the requirement in advance, the entity is not required to act on an individual's request that does not meet the requirements.

Entities must act on a request for amendment within 60 days of receipt of the request. The entity must inform the individual that the request has been either accepted or denied, in whole or in part. If the entity is unable to meet the deadline, the entity may extend the deadline by no more than *30 days*.

If an entity accepts an individual's request for amendment, it must make the appropriate *amendment*. At a minimum, the entity must identify the records that are affected and must append the amendment (or otherwise provide a link to the location of the amendment). Entities are not required to expunge any protected health information. Entities may expunge information, if doing so is consistent with other applicable law and the entity's record keeping practices.

The entity must provide a copy of the amendment to:

- persons the individual identifies as having received protected health information about the individual and needing the amendment; and

- persons, including business associates, that the entity knows have the unamended information and who may have relied, or could foreseeably rely, on the information to the detriment of the individual.

If an entity receives a *notification of amended protected health information* from another entity, the entity must make the necessary amendment to health information in designated record sets it maintains. In addition, entities must require their business associates who receive such notifications to incorporate any necessary amendments to designated record sets maintained on the entity's behalf.

3.6.3.2 Denying the Amendment

An entity may deny a request for amendment, if the

- entity did not create the protected health information or record that is the subject of the request for amendment. However, if the individual provides a reasonable basis to believe that the originator of the protected health information is no longer available to act on the requested amendment, the covered entity must address the request for amendment as though the entity had created the information.
- protected health information that is the subject of the request for amendment is not part of a designated record set or would not otherwise be available for inspection
- information in dispute is accurate and complete.

This right is not intended to interfere with medical practice or to modify standard business record keeping practices. Perfect records are not required. Instead, a standard of *reasonable accuracy* and completeness should be used. In addition, this right is not intended to provide a procedure for substantive review of decisions such as coverage determinations by payers. It is intended only to affect the content of records, not the underlying truth or correctness of materials recounted therein. Attempts under the Privacy Act of 1974 to use this mechanism as a basis for collateral attack on agency determinations have generally been rejected by the courts. The same results are intended here.

If an entity denies a request for amendment, it must provide the individual with a statement of denial written in plain language. The *written denial* must include

- the basis for the denial,
- how the individual may file a written statement disagreeing with the denial, and
- how the individual may make a complaint to the entity and DHHS.

The entity must inform individuals of their options with respect to future disclosures of the disputed information in order to ensure that an individual is aware of his or her rights. The written denial must state that if the individual chooses not to file a statement of disagreement, the individual may request that the entity include the individual's request for amendment and the entity's denial of the request with any future disclosures of the health information that is the subject of the requested amendment.

The entity must permit the individual to submit a written statement disagreeing with the denial and the basis of such disagreement. The entity may reasonably limit the length of a statement of disagreement and may prepare a written rebuttal to the individual's statement of disagreement. If the entity prepares a rebuttal, it must provide a copy to the individual. The entity must identify the health information that is the subject of the disputed amendment and *append* or otherwise link the following information to the designated record set:

- the individual's request for amendment,
- the covered entity's denial of the request,
- the individual's statement of disagreement (if any), and the covered entity's rebuttal (if any).

If the individual submits a written statement of disagreement, all of the appended or linked information, or an accurate summary of it, must be included with any subsequent disclosure of the protected health information to which the disagreement relates.

3.6.4 Accounting of Disclosures

An individual has a right to receive an accounting of disclosures of protected health information made by an entity in the *six years* prior to the date on which the accounting is requested. However, this account is only for exceptional disclosures. No accounting is expected for disclosures:

- made pursuant to an individual's authorization.
- that are part of a limited data set.
- that are merely incidental to another permissible use or disclosure.
- that occurred prior to the compliance date for the entity.
- to business associates that are for any exempt purpose (such as treatment, payment, or health care operations).
- that are made by business associates or by others who receive protected health information from the covered entity.

Other less frequent categories of disclosure for which accounting is not required include those

- for national security or intelligence purposes and
- to correctional institutions or law enforcement officials.

Examples of disclosures that may have occurred without a patient-signed authorization and that the covered entity should record for an ‘accounting of disclosures’ are a report of:

- gun shot wounds to police,
- child abuse to social services, and
- positive tuberculosis test result to a public health agency.

The covered entity must provide the individual with a *written accounting* that includes for each disclosure:

- the date of the disclosure;
- the name of the entity or person who received the protected health information and, if known, the address of such entity or person;
- a brief description of the protected health information disclosed; and
- a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.

If, during the period covered by the accounting, the entity has made multiple disclosures of protected health information to the same person or entity for a single purpose, or pursuant to a single authorization, the accounting may, with respect to such multiple disclosures, provide the:

- information required for the first disclosure during the accounting period;
- frequency, periodicity, or number of the disclosures made during the accounting period; and
- date of the last such disclosure during the accounting period.

The entity must act on the individual’s request for an accounting no later than 60 days after receipt of such a request. If the entity is unable to provide the accounting within that time, the entity may extend the time to provide the accounting by no more than 30 days, provided that:

- The entity provides the individual with a written statement of the reasons for the delay and the date by which the entity will provide the accounting; and
- The entity may have only one such extension of time for action on a request for an accounting.

The entity must provide the first accounting to an individual in any 12-month period without charge. The entity may impose a reasonable, *cost-based fee* for each subsequent request for an accounting by the same individual within the 12 month period, provided that the entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee. The entity must also retain a copy of any accounting provided and must document the titles of the persons or offices responsible for receiving and processing requests for an accounting.

3.6.5 Review Questions

1. What is the relationship between the ‘designated record set’ and the right of a patient to access?
2. Under what conditions can an entity deny a patient access?
3. What costs of providing access is an entity allowed to charge directly to the patient requesting the access?
4. If an entity wants to deny a patient’s request to amend the record, then what steps must the entity take?
5. What accounting of disclosures must an entity be prepared to provide to a patient?

3.7 Administration

Main Points

- The Privacy Rule is flexible so that an entity can choose the approach best suited to itself.
- The Rule requires entities to have a privacy official, to document their policies, to train staff, to safeguard information, to accept complaints, and to sanction privacy violators.
- The federal enforcement of the Privacy Rule includes possible imprisonment of chief executives of guilty covered entities.

The Privacy Rule can be seen as a blueprint for the flow of information in healthcare. What does the Rule say about how entities should operate so as to best implement the Rule? How much flexibility is there? What staffing, documentation, and training are required? What sanctions exist?

3.7.1 Flexible

DHHS requires that each affected entity assess its own needs. The standards do not impose particular mechanisms or procedures that covered entities must adopt to implement the standards. Instead, DHHS requires that each affected entity assess its own needs and devise, implement, and maintain appropriate privacy policies, procedures, and documentation to address its business requirements. How each privacy standard will be satisfied will require business decisions by each entity. Entities of a similar type are encouraged to work together to establish best practices for that entity type.

Because the privacy standards need to be implemented by all covered entities, from the *smallest provider* to the largest, *multi-state health plan*, a single approach to implementing these standards is neither economically feasible nor effective in safeguarding health information privacy. Examples for staffing are

- In a small physician practice, the office manager might be designated to serve as the privacy official as one of many duties.
- At a large health plan, the privacy official may constitute a full time position and have the regular support and advice of a privacy staff or board.

Examples for disclosures are:

- A large enterprise may make frequent electronic disclosures of similar data. In such a case, the enterprise would be expected to remove identifiers or to limit the data fields that are disclosed to fit the purpose of the disclosure. The process would be documented and perhaps even automated.
- A solo physician's office, however, would not be expected to have the same capabilities to limit the amount of information disclosed, although, in the cases of disclosures involving a small number of records, such an office could be expected to hide identifiers or to limit disclosures to certain pages of the medical record that are relevant to the purpose of the disclosure.

In taking this flexible approach, DHHS intends to strike a balance between the need to maintain the *confidentiality* of protected health information and the *economic cost* of doing so. Healthcare entities must consider both aspects in devising their solutions.

3.7.2 Requirements

Entities should develop a privacy compliance program. Although certain hospital departments, such as medical records, may have privacy policies, the Rule requires the institution as a whole to adopt privacy guidelines for all employees and departments. Covered entities are required to:

- Designate a privacy officer;
- Document their policies and procedures relative to privacy;
- Provide employees with training on health information privacy;
- Implement safeguards to protect health information from intentional or accidental misuse;
- Provide a means for individuals to lodge complaints about the organization's information practices and maintain a record of any complaints; and
- Develop a system of sanctions for employees and business associates who violate the organization's policies.

The Rule touches many aspects of the healthcare operation.

3.7.2.1 Privacy Official

Covered entities are required to designate a privacy official, responsible for the implementation and development of the entity's privacy policies and procedures. Entities must also designate a contact person to receive complaints about privacy and provide information about the matters covered by the entity's notice. The *contact person* could be, but is not required to be, the person designated as the privacy official. Implementation details are left to the discretion of the entity. Implementation may vary widely depending on the size and nature of the entity, with small offices assigning this as an additional duty to an existing staff person, and large organizations creating a full-time privacy official.

If a subsidiary is defined as a covered entity, then a separate privacy official and contact person is required for that covered entity. This approach is also recommend by JCAHO (1999):

> accountability is enhanced by having focal points that are responsible for assessing compliance with policies and procedures...

If several *subsidiaries* are designated as a single covered entity, then together they need have only a single privacy officer and contact person. If several covered entities share a notice for services provided on the same premises, that notice need designate only one privacy official and contact person for the information collected under that notice.

3.7.2.2 Documentation

DHHS requires covered entities to develop and document their policies and procedures for implementing the requirements of the Privacy Rule. This requirement is intended as a tool to

- facilitate entities' efforts to develop appropriate policies to implement this rule,
- ensure that the members of its workforce and business associates understand and perform expected privacy practices, and
- assist entities in developing a notice of information practices.

The size of the policies developed should be consistent with the size of the covered entity.

Small entities can have small documents. For example, a small health plan could develop policies restricting access to health plan information to one designated employee, empowering that employee to deny release of the information to corporate executives and managers unless required for health plan administration. A *solo practitioner's* documentation of his policies and procedures could provide relatively straightforward statements, such as:

> This practice does not use or disclose any protected health information that is not authorized. A staff registered nurse reviews all individually authorized requests for disclosures to ensure they contain all required elements and reviews the copied information to ensure only authorized information is released. Information requests that would require extensive redaction will be denied.

Large entities have large documents. Large entities with many functions and business relationships and who are subject to *multi-state* reporting and record-keeping requirements would need to develop and document extensive policies. Large employers could have policies that include using contractors for any function that requires access to protected health information or requiring all reports they receive for plan administration to be de-identified unless individual authorization is obtained. A health plan may determine that Underwriting Department employees must provide a written request, approved by a team leader, to access any identifiable claims information; that such requests must be retained and reviewed every quarter for appropriateness; and the *Underwriting Department* must destroy such information after use for an approved activity.

Entities must maintain information. Entities must modify in a prompt manner their policies and procedures to comply with changes in relevant law. The policies and procedures must be maintained in writing. Any other communication, action, activity, or designation that must be documented under the Rule must be documented in writing. 'Writing' includes electronic storage; paper records are not required. Entities must retain any required documentation for at least *six years* (the statute of limitations period for the civil penalties) from the date of the creation of the documentation.

This documentation approach is consistent with JCAHO (1999) recommendation:

> Managed Care Organizations should have clearly defined policies and procedures for dealing with confidentiality issues.

More generally, good business sense requires documentation.

3.7.2.3 Training

An entity must train all members of its workforce on the policies and procedures with respect to protected health information, as necessary and appropriate for the members of the workforce to perform their function within the entity. A covered entity must provide training that meets these requirements:

- To each member of the covered entity's workforce by no later than the compliance date for the entity;

- Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the entity's workforce; and
- To each member of the entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart, within a reasonable period of time after the material change becomes effective.

Entities are responsible for implementing policies and procedures to meet these *training requirements* and for documenting that training has been provided.

Entities would determine the most effective means of communicating with their workforce. For example, in a *small physician practice* the training requirement could be satisfied by

- providing each new member of the workforce with a copy of the practice's information policies and
- requiring members of the workforce to acknowledge that they have reviewed the policies.

A *large health plan* could provide for a training program with live instruction, video presentations, or interactive software programs (Rada, 2001). The small physician practice's solution would not protect the large plan's data, and the large plan's solution would be neither economically feasible nor necessary for the small physician practice.

3.7.2.4 Safeguards

Entities must have administrative, technical and physical safeguards to protect the privacy of health information. Entities must *safeguard* protected health information from accidental or intentional use or disclosure that is a violation of the Rule. Limitations on access to protected health information by the entity's workforce will also be covered by the policies and procedures for 'minimum necessary' use of protected health information. These provisions work in tandem.

DHHS does not prescribe the particular measures that entities must take to meet this standard, because the nature of the required policies and procedures will vary with the size of the entity and the type of activities that the entity undertakes. As with other provisions of this rule, this requirement is 'scalable'. Examples of appropriate safeguards include requiring that

- documents containing protected health information be shredded prior to disposal, and
- doors to medical records departments (or to file cabinets housing such records) remain locked and only certain personnel are authorized to have the key.

This is intended to be a common sense, *scalable standard*.

Entities are not required to guarantee the safety of protected health information against all assaults. Theft of protected health information may or may not signal a violation of this Rule, depending on the circumstances and whether the covered entity had reasonable policies to protect against theft. Organizations such as the Association for Testing and Materials (ASTM) and the American Health Information Management Association (AHIMA) have developed a body of *recommended practices* for handling of protected health information that covered entities may find useful. The proposed HIPAA Security Standards would require covered entities to safeguard the privacy and integrity of health information. For electronic information, compliance with both regulations will be required.

The requester's identity and authority should be verified:

- When the request for disclosure of protected health information is from a person with whom the covered entity does not routinely do business, the covered entity should *verify* the identity of the requestor, such as via a driver's license.
- For certain categories of disclosures, covered entities would also be required to verify the requestor's legal authority to make the request.

For example, public health agencies may contract with a nonprofit agency to collect and analyze certain data. In such cases the covered entity would be required to verify the requestor's identity and authority through examination of reasonable documentation that the requestor is acting on behalf of the government agency. Reasonable evidence would include a written request provided on *agency letterhead* that describes the legal authority for requesting the release and states that the person or entity is acting under the agency's authority, or other documentation, including a contract, a memorandum of understanding, or purchase order that confirms that the requestor is acting on behalf of the government agency. Reasonable reliance on verbal representations would be appropriate in certain situations, such as emergencies.

3.7.2.5 Complaints

Entities must have a mechanism for receiving complaints from individuals regarding the health plan's or provider's privacy practices. They must receive complaints concerning violations of the covered entity's privacy practices, not just violations of the rule. For example, a covered entity must have a mechanism for receiving a *complaint* that patient information is used at a nursing station in a way that it can also be viewed by visitors to the hospital, regardless of whether the practices at the nursing stations might constitute a violation of this rule.

The health plan or provider does not need to develop a formal appeals mechanism, nor must 'due process' or any similar standard be applied. Additionally, there is no requirement to respond in any particular manner or time frame. The entity is, however, required to maintain a *record of the complaints* that are filed and a brief explanation of their resolution, if any.

The entity could implement the complaint mechanism based on its size and capabilities. For example, a *small practice* could assign a clerk to log written or verbal complaints as they are received. One physician could review all complaints monthly, address the individual situations, and make changes to policies or procedures as appropriate. The clerk would log results of the physician's review of individual complaints. A large entity could choose to implement a formal appeals process.

Sometimes an individual not otherwise involved in law enforcement uncovers evidence of wrongdoing, and wishes to bring that evidence to the attention of appropriate authorities -- this is a whistleblower. Whistleblowers may use protected health information. Important evidence of unlawful activities may be available to employees of covered entities, such as billing clerks or nurses. Sometimes only identifiable information will suffice to demonstrate that an allegation of wrongdoing merits the investment of legal or investigatory resources. For instance, a billing clerk who suspects that a hospital has engaged in fraudulent billing practices may need to use billing records for a set of specific cases to demonstrate the basis of his suspicion to an oversight agency. An entity would not be held in violation because a member of its workforce or a business associate appropriately discloses protected health information that such person believes is evidence of a civil or criminal violation. An appropriate disclosure is made to relevant oversight or law enforcement agencies or an attorney. The *attorney* would determine whether a violation of criminal or civil law has occurred or assess the remedies that may be available to the person disclosing the information.

3.7.2.6 Sanctions

All covered entities must develop and apply sanctions for failure to comply with policies or procedures of the covered entity or with the requirements of the HIPAA Privacy Rule. All members of the workforce who have regular contact with protected health information should be subject to sanctions, as would the entity's business associates. The *sanction* applied would vary depending on factors such as the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicates a pattern or practice of improper use or disclosure of protected health information. Sanctions could range from a warning to termination.

Entities must respond to breaches of contract terms. For example, an entity that becomes aware that a *business associate* has improperly disclosed protected health information could require that business associate to take steps to retrieve the disclosed information. The covered entity also could require that business associate to adopt new practices to better assure that protected health information is appropriately handled.

Covered entities generally would not be required to monitor the activities of their business associates, but would be required to take steps to address problems of which they become aware. Where the *breach* is serious or repeated, the covered entity must monitor the business associate's performance to ensure that the wrongful behavior has been remedied. For example, the covered entity could require the business associate to submit reports or subject itself to audits to demonstrate compliance with the contract terms required by this rule. *Termination* of the arrangement would be required, if it becomes clear that a business associate cannot be relied upon to maintain the privacy of protected health information provided to it.

A covered entity must have written policies and procedures for the application of appropriate sanctions for violations of the Privacy Rule and document those sanctions. Sanctions would be more formally described in large entities than in small ones. Small entities would be given more latitude and *flexibility* than large entities.

Covered entities have a duty to mitigate any harmful effect of a use or disclosure of protected health information that is known to the covered entity. The duty is to *mitigate* a violation of the covered entity's policies and procedures, not just a violation of the Privacy Rule. This duty is on covered entities for harm caused by either members of their workforce or by their business associates.

An example of a form that can be used by employees to indicate their agreement to operate in accordance with sound practices for privacy is available from CPRI-HOST (CPRI-HOST, 2000). Any individual who is permitted access to a healthcare provider's information system should be required to sign an agreement documenting his understanding of his responsibilities in preserving the confidentiality and security of information. The form can be used for employees, volunteers, or students. It begins with this paragraph:

> Security and confidentiality is a matter of concern for all persons who have access to (HEALTHCARE ENTITY) information systems. Each person accessing (HEALTHCARE ENTITY) data and resources holds a position of trust relative to this information and must recognize the responsibilities entrusted in preserving the security and confidentiality of this information. Therefore, all persons who are authorized to access data and resources, both through enterprise information systems and through individual department local area networks and databases, must read and comply with (HEALTHCARE ENTITY) policy.

The CPRI Employee Form then has three paragraphs about the general principles of confidentiality and security as regards employee behavior. After that eighteen requirements are listed for all employees. Two of these requirements are reproduced here by way of example:

> Respect the privacy and rules governing the use of any information accessible through the computer system or network and only utilize information necessary for performance of my job.
>
> Understand that my obligations under this Agreement will continue after termination of my employment. I understand that my privileges hereunder are subject to periodic review, revision, and if appropriate, renewal.

The CPRI Employee Form defines roles. It includes a 500-word attachment that defines the responsibilities of three roles, namely:

- Health Information Trustees,
- Custodians, and
- Users.

The *Trustee* determines privacy policy, the *Custodian* implements the policy, and the *User* follows the policy.

The form calls for the signature of the employee that appears as follows:

> Those who cannot accept these standards of behavior may be denied access to the relevant computer systems and networks. Violators also may be subject to penalties, including disciplinary action, under policies of (HEALTHCARE ENTITY) and under laws of the State of (STATE NAME) or the United States of America to the extent applicable. By signing this, I agree that I have read, understand and will comply with the Agreement.
>
> ____________________________________
>
> Signature/Date
>
> ____________________________________
>
> Printed Name
>
> ____________________________________
>
> Area/Department/Phone Number

While the CPRI form predates HIPAA, its content goes in the direction of what might be used by an organization wanting to comply with HIPAA requirements.

3.7.2.7 Transition Provisions

In certain circumstances, an entity may continue to rely upon authorizations obtained prior to the *compliance date*, even if these authorizations do not meet the requirements set forth in the Privacy Rule. To ensure that important functions of the healthcare system are not impeded, previously obtained authorizations continue under a grandfather clause. This means that uses or disclosures of individually identifiable health information made prior to the compliance date of this regulation are not subject to sanctions. Entities are not required to rely upon these authorizations and may obtain new authorizations that meet the applicable requirements of the Privacy Rule.

Covered entities may operate under existing contracts with business associates for up to one year beyond the April 14, 2003 compliance date. This transition period is available to a covered entity if it has an existing contract or other written arrangement with a business associate, and the contract is not renewed or modified prior to April 14, 2003.

3.7.3 Enforcement

How is the Privacy Rule enforced by the government?

3.7.3.1 Three Approaches

The statute has three distinct approaches to achieve compliance:

- filing complaints,
- compliance review, and
- contracts.

Individuals have the right to file a complaint with DHHS, if they believe that a covered entity has failed to comply with the Privacy Rule. Because individuals would have received notice of the uses and disclosures that the entity could make and of the entity's privacy practices, they would have a basis for making a realistic judgment as to when a particular action or omission would be improper. The notice would also inform individuals how they could file such *complaints*.

The DHHS procedures are modeled on those used by DHHS's Office for Civil Rights. DHHS will require complainants to identify the entities and describe the acts or omissions alleged to be *non-compliant*. Individuals must file such complaints within 180 days of those acts or omissions. The requirements for filing complaints are as minimal as possible, to facilitate use of this right. DHHS would also attempt to keep the identity of complainants confidential.

DHHS would try to resolve complaints on an informal basis wherever possible. Where a resolution could not be reached, the Secretary could make a formal finding of noncompliance. DHHS could also refer the matter to the *Department of Justice* for prosecution.

The second method of enforcement is compliance review. DHHS may conduct compliance reviews to determine whether the covered entity or business associate is complying with the rules. To be in compliance, the entity must:

- have records adequate to allow DHHS to determine whether the entity has been complying;
- cooperate with DHHS in reviewing procedures in the entity;
- permit access to all information that might be pertinent to ascertaining compliance; and
- not intimidate, discriminate against, or take any retaliatory action against any individual who collaborates with DHHS in investigating compliance.

DHHS will assume in this way an increased *policing role*.

Complaints by individuals and compliance reviews by DHHS are the 1st and 2nd enforcement mechanisms. The 3rd enforcement mechanism is contractual. DHSS has enlisted each covered entity to police compliance by its *business associates*. An entity is in violation of the regulations, if it reasonably should have known of a breach by a business associate of the privacy requirements in its contractual agreement and fails to take reasonable steps to remove the problem.

3.7.3.2 Civil and Criminal Penalties

Civil and criminal penalties apply. HIPAA grants DHHS the authority to impose civil monetary penalties against covered entities and also establishes criminal *penalties* for certain wrongful disclosures of protected health information.

HIPAA provides for civil penalties of $100 per violation of the privacy provisions. These civil fines are capped at $25,000 for each calendar year for each type of provision that is violated. DHHS cannot impose a *civil penalty*, if the act or omission is criminally punishable.

The criminal penalties are graduated, increasing if the offense is committed under false pretenses, or with intent to sell the information or reap other personal gain. The HIPAA legislation provides more precisely for a:

- fine of $50,000 and *one year in prison* for basic offenses,
- fine of $100,000 and *five years in prison* for offenses committed under false pretenses, and
- fine of $250,000 and *ten years in prison* for offenses committed with intent to use individually identifiable health information for gain or harm.

If the criminal penalties are enforced on a per violation basis, then they become even more of an incentive to comply (Owens, 2000).

3.7.3.3 Beyond

Some say that failure to protect health information should be punished by significant penalties and that any individual whose rights under the law have been violated should be permitted to bring an action for actual damages and equitable relief. In HIPAA, Congress did not provide such enforcement authority. Efforts since the passage of HIPAA to pass legislation that contained such individual right to action clauses have been highly controversial and did not pass. Nevertheless, state law may lead the way in establishing such individual right to action. For instance, the Ohio State Supreme Court concluded that there is a common law right for privacy and established the *independent tort* of unauthorized disclosure of medical information obtained under a physician-patient relationship.

The most significant exposure from HIPAA's Privacy Rule may result from HIPAA establishing a minimum floor for the protection of health information. A party that fails to implement the HIPAA Privacy Rule would risk tort lawsuits for breach of the *common law right of privacy*. Plaintiffs in those suits may point to the HIPAA Privacy Rule as the minimum reasonable level of protection. This

Rule then becomes the 'test' for adequate privacy to be applied to all entities and all health information -- not just the information and parties specifically covered by the HIPAA rules (Britten et al, 1999).

3.7.4 Review Questions

1. What does DHHS mean by its intent to be flexible in its requirements of entities complying with the Privacy Rule?
2. List the basic administrative requirements of the Privacy Rule.
3. What guidance does the Privacy Rule give about how much training needs to be offered how often?
4. What sanctions for privacy violations must an entity administer?
5. What are key features of the DHHS 'notice of privacy practices'?
6. What options does an entity have in terms of producing different 'notices of privacy practice' for different contexts and how would those be distributed to patients?
7. What is the relationship between the legislation (HIPAA) and the enforcement of privacy?

3.8 Other Regulations

Main Points

- The HIPAA Privacy Rule is consistent with other Federal rules germane to privacy.
- State laws on privacy present a maze of different conditions within a state, and across the states the differences are also great.
- States do not give the broad rights to patients that the HIPAA Privacy Rule does. States tend neither to require privacy notices nor to require that providers allow patients to see their medical records. The HIPAA Privacy Rule will pre-empt less stringent state rules.
- Various professional associations have privacy guidelines, but they are less patient-centric than the HIPAA Privacy Rule.
- JCAHO has privacy guidelines that hospitals will have to meet in order to be certified.
- The European Union has a privacy directive that is citizen-centric and much stronger than laws in the United States with the exception of HIPAA.

Many different laws, regulations, and guidelines exist. *Federal laws* and rules for privacy harmonize nicely with the HIPAA Rule. The situation elsewhere is not as simple. HIPAA requires that states have some priority in running their own affairs. The *states* have a very complex set of approaches to privacy. *Professional societies* may also have their own codes of conduct. In dealing with different countries, the difficulties of sharing information increases because the different countries have different rules, as shown at the end of this section in the European Union approach to privacy.

3.8.1 Federal Laws

Various Federal laws and regulations address privacy. Two examples of federal privacy legislation that apply to large components of the healthcare sector are described next, namely, the Privacy Act of 1974 and the Gramm-Leach-Bliley Act.

3.8.1.1 Privacy Act of 1974

An important step toward data protection was the development in 1973 of 'fair information principles' by the U.S. Department of Health, Education, and Welfare. The five fair information principles are the foundation of a privacy policy and follow:

- There must be no secret, personal-data, record-keeping system.
- There must be a way for individuals to discover what personal information is recorded about them and how it is used.
- There must be a way for individuals to prevent personal information obtained for one purpose from being used without their consent for another purpose.
- There must be a way for individuals to correct or amend information about them.
- An organization creating, maintaining, using, or disseminating records of identifiable personal data must ensure the reliability of the data for their intended use.

The U.S. Privacy Act of 1974 is based on the 1973 fair information principles. It applies only to federal agencies.

The Privacy Act of 1974 is widely seen as ineffective. The Privacy Act allows disclosure without the subject's consent whenever the purposes are compatible with the original purpose – this is called routine use. The *routine use* provisions have led to an ever-expanding loophole in the disclosure of information. Other weaknesses include (Summers, 1997):

- The burden of enforcement is placed entirely on the individual, who must file a civil suit to get an injunction or damages; and
- the penalties are inadequate.

Nevertheless, the *Privacy Act* provides Federal agencies with a framework for protecting privacy, and the HIPAA Privacy Rule builds on the Privacy Act framework. Basic management features, such as the provision of safeguards to protect the privacy of health information and training for employees -- which are required by the HIPAA privacy rule -- already are required by the Privacy Act. *Federal agencies* will be required to comply with both the Privacy Act of 1974 and the HIPAA Rule. The HIPAA Rule has been designed so that individuals will not have fewer rights than they have now under the Privacy Act. HIPAA may require that agencies obtain individual authorization for some disclosures that they now make without authorization but assume are routine use.

3.8.1.2 Gramm-Leach-Bliley

In 1999 Congress passed the Gramm-Leach-Bliley Act (GLB) and thus revamped the financial services industry by removing Depression-era restrictions on certain business activities of *financial institutions*. In giving financial institutions greater freedom to engage in multiple activities and create and share large databases, the Congress also tried to constrain the sharing of personal information to protect the interests of individuals.

GLB calls for privacy. Title V of GLB focuses on privacy protection for information concerning individual customers of financial institutions. The legislation mandates that each financial institution has an

> affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' non-public personal information.

GLB applies to health plans (Senate, 2001). A 'financial institution' is any company that engages in activities that are defined by the statute to be 'financial' in nature. In addition to traditional banking activities, this term also includes

> insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability or death, or providing and issuing annuities, and acting as principal, agent, or broker for those activities.

The reference to illness includes health insurance activities.

The GLB privacy provision covers a wider range of information than the HIPAA Privacy Rule (Nahra, 2000). The GLB privacy limitations apply to non-public personal information, which is defined as

> personally identifiable financial information that is provided by a customer to a financial institution, or information resulting from any transaction with the customer or any service performed for the customer or information otherwise obtained by the financial institution.

The meaning of the term 'financial' includes health information but is considerably broader. For instance, financial information about a person is also non-public, personal information.

The GLB privacy provision generally makes a crucial distinction between disclosures to 'affiliated' and 'nonaffiliated' companies. An 'affiliated' company is any company that controls, is controlled by, or is under common control with another company. A non-affiliated third party is any entity that is not an affiliate of the financial institution. According to a key provision of GLB, a financial institution may not

> directly or through any affiliate, disclose to a nonaffiliated third party any non-public personal information, unless the financial institution has provided to the consumer an

appropriate notice and gives the consumer the ability to ‘opt out’ of this disclosure.

The exchange of information between affiliated companies is essentially unrestricted.

In order to disclose information to nonaffiliated entities, health plans must disclose the health plan policies at the time of establishing a customer relationship and not less than annually during the continuation of such relationship.

The National Association of Insurance Commissioners approved a model Privacy of Consumer Financial and Health Information Regulation, to implement the insurance industry privacy obligations under GLB. The model states that compliance with the HIPAA requirements will constitute compliance with GLB.

To comply with GLB’s privacy provision, health plans should first do a privacy audit. This audit should:

- assess all of the sources of personal information used by the health plan, how that information is used by the company, and where this information is distributed and
- conduct a contract review (including insurance policies, employer contracts, vendor contracts, utilization review agreements, and reinsurance) to understand the company's information flow with business partners and the commitments that are being made in connection with these contractual relationships.

This audit is an essential roadmap to the other decisions to comply with the GLB privacy provisions.

3.8.1.3 Others

Organizations that operate specialized substance abuse treatment facilities and that either receive Federal assistance or are regulated by a Federal agency are subject to confidentiality rules established by the *Public Health Service Act*. These organizations will be subject both to that Act and to HIPAA. The HIPAA Privacy Rule should have little practical effect on the disclosure policies of these organizations, because the patient confidentiality statute governing information about substance abuse is generally more restrictive than the HIPAA Privacy Rule.

The HIPAA Privacy Rule applies to State Medicaid programs, which under HIPAA are considered health plans. Pre-existing Medicaid rules regarding disclosure of patient information are stricter than provisions of the HIPAA Privacy Rule. Therefore, Medicaid agencies simply will continue to follow the *Medicaid rules*.

In 1997, the Food and Drug Administration (FDA) announced a uniform approach to regulating electronic signature, record keeping and reporting practices for all business disciplines under its control. Dubbed *21 CFR Part 11*, this regulation has far-reaching implications for all businesses within the bio-pharmaceutical industry. These regulations provide criteria for acceptance by FDA of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. The FDA has authority to evaluate compliance practices during routine inspections, and companies are developing strategies to identify, remediate and validate non-compliant systems, as well as creating standards for new systems. The FDA has issued formal warnings to companies who are not in compliance or who have not made formal plans and schedules to be compliant. The regulations are intended to permit the widest possible use of electronic technology, compatible with FDA’s responsibility to promote and protect public health. The use of electronic records as well as their submission to FDA remains voluntary.

3.8.2 State Laws

States have adopted a number of laws designed to protect patients against the inappropriate use of health information. A recent survey of these laws indicates, however, that these protections are uneven and leave large gaps in their protection (Health, 1999). While harmonizing the HIPAA Privacy Rule with other Federal privacy rules seems straightforward, the situation as regards state rules or laws is complicated. Laws relating to health privacy can be found in obvious and obscure sections of a state’s code, buried in regulations, developed in case law, and detailed in licensing rules (Pritts et al, 1999). Florida, for example, has more than 60 statutes that address health privacy, and the state is not unique. Subsequent sections examine how these *state rules* vary by entity, by patient access rights, by disclosures, and by condition-specific requirements.

3.8.2.1 By Entity

To understand what confidentiality protections do exist at the *state level*, one must first begin by examining the laws applying to the different entities that use health information. Even states that attempt to handle health privacy in a comprehensive fashion typically establish unique rules for different entities. For example, physicians, schools, insurers, and state agencies each have a specific function in the state and a legal and regulatory structure specific to their roles. The statutory requirements for how they handle medical information are different.

The end result of this *legislating by entity* is that state laws – with a few notable exceptions – do not extend comprehensive protections to people's medical records. Thus, a state statute may impose privacy rules on hospitals but not dentists. The state may restrict the use and disclosure of information derived from a genetic test but not information obtained in a routine physical. Or just the opposite may be true in a neighboring state.

3.8.2.2 Patient Access

States vary widely in the rights they grant to patients to receive and copy their own medical records:

- On one end, some states have no statutory right of access, such as Kansas and North Dakota.
- On the opposite end, a few states – such as Connecticut and Minnesota – *grant access* to records maintained by nearly all of the potential sources of patient data, i.e. government agencies and entities, hospitals, physicians, insurers, schools, and even non-traditional healthcare providers such as naturopaths.

Most states fall somewhere in the middle of these two extremes and provide some rights of access, as follows:

- 33 states provide a right of access to hospital records;
- 13 states provide a right of access to HMO records; and
- 16 states provide a right of access to insurance records.

Many states have granted patients the right to amend or correct their medical information. In Illinois, New Jersey and Ohio, for example, the statute includes a detailed procedure for resolving a patient's challenge to the accuracy or completeness of the record. Where the provider and the patient disagree, for example, the patient may be able to *insert a statement* of his or her position in the record.

Most states allow an entity to charge patients for copies of their medical record. Some states specify a cost in the statute – in Kentucky, for example, a healthcare provider or hospital must provide a patient with a free copy of their medical record. A patient may be charged for additional copies, but not more than $1 per page. Other states require that the fee be waived, if the patient is contesting an adverse underwriting decision. The most common approach is to stipulate that an entity may charge a *reasonable fee*.

3.8.2.3 Restrictions on Disclosure

States vary widely in their restrictions on disclosures of medical information. They vary in the chain of trust agreements that they require, in the exceptions to requiring authorization to disclose, and in the conditions under which research can gather information.

Some states require chain of trust agreements, and some states do not. In other words, the *receiving entity* may or may not be under any legal obligation to adhere to the privacy rules imposed on the disclosing entity.

State statute typically requires that patient authorization be secured prior to health information being disclosed -- except for routine use but *routine use* is not defined. The statutes all specify numerous circumstances under which an entity may disclose information without patient authorization. The most common circumstances include

- purposes of treatment;
- securing payment for healthcare;
- quality assurance activities, and
- research purposes.

These circumstances reflect some of the most frequent demands on healthcare information anyhow.

Many state laws allow researchers broad access to patient records but not to registry data. What limits do exist for patient records usually speak only to specific information – such as genetic information or HIV/AIDS information. On the other hand, researcher access to patient data in government registries is often constrained.

Authorization forms and revocations vary. Some states specify in the legislation the format and content of the patient *authorization form*. Some states do not. Some states say patients may revoke authorizations, but some states do not.

3.8.2.4 Condition-specific

Nearly all states have laws that impose privacy requirements that are specific to a medical condition. These requirements often shield people with mental illness, communicable diseases, cancer, and other sensitive, stigmatized illnesses from broad disclosures. Many of these laws were passed to respond to public fear that certain health information would be widely disclosed and used to deny patients benefits or result in other harm. Where this fear acted as a barrier to seeking healthcare, treatment, or counseling, states have moved to bolster public trust and confidence in the healthcare system by enacting heightened privacy rules for these *specific conditions*.

Some condition-specific requirements allow for greater disclosure of the information. Some mental health statutes, for example, explicitly allow family members to access the *mental health records* of a family member who has been committed. Other statutes allow employers to share medical information about an employee, if it affects performance on the job.

Many condition-specific requirements that exist at the state level were enacted hand-in-hand with mandatory reporting laws. For instance, essentially all states require that healthcare providers report to governmental health authorities the identity of persons suspected or diagnosed as having specified contagious diseases, such as tuberculosis. Many states require providers to report the identity of children born with birth defects to a central registry. The statutes then limit how the health authorities or registry can use or disclose the information which has been collected. This tight control on registry information has a *historical basis*. Legislation created the registry. To calm the public's fear that this government-supported collection of health information would lead to a loss of privacy, the sponsoring legislation demands confidentiality of the registry content.

Most state health privacy statutes contain some form of remedies and penalties that are triggered by violations of the law. Commonly found are private right of action provisions that grant people the ability to bring *lawsuits* when the statute has been violated. A full range of damages, remedies, and attorney's fees and costs are usually available; however the monetary damages are often very low.

3.8.3 States versus HIPAA

What are the differences between state law and the HIPAA Privacy Rule? The HIPAA Privacy Rule preempts state law only when the state law is weaker. What does weaker mean?

3.8.3.1 Comparing

A comparison of State privacy law with the HIPAA Privacy Rule highlights numerous differences. Differences in notice publication, access restrictions, and entities to which the laws are applicable are sketched next. Many other *differences* can be found (Pritts et al, 1999).

No State law requires entities to make their privacy policies available to patients. Under HIPAA all covered entities that have direct contact with patients are required to prepare and *publish* a statement of their privacy policies. Thus entities will have to develop these notices, if they do not already have them in place.

HIPAA applies to both electronic and non-electronic information in the hands of covered entities. State laws typically assume the health information is on *paper*. The HIPAA rules may lead States to address electronic and paper forms in their privacy protections.

Approximately 100 million non-elderly persons who purchase health insurance are in States that do not provide patients a legal right to inspect or copy their records. The HIPAA Privacy Rule gives those 100 million patients the right to see their records.

State privacy laws do not always *apply to entities* covered by the HIPAA Privacy Rule. For example, State laws may provide strong privacy protection for hospitals and doctors but not for dentists or HMOs. State laws protecting particular types of genetic testing or conditions may be similarly problematic because they protect some types of sensitive information and not others. In some instances, a patient's right to inspect his or her medical record may be covered under State laws and regulations when a physician has the medical information, but not under State requirements when the information being sought is held by a health plan. Thus, the HIPAA Privacy Rule extends privacy requirements already applicable to some entities within a State to other entities that currently are not subject to State privacy requirements.

3.8.3.2 Preemption

HIPAA provides that contrary State laws that relate to the privacy of individually identifiable health information will not be preempted by the federal requirements, if state laws are *more stringent* than HIPAA. The statute directs this analysis by requiring the comparison of State law and federal regulation. Definitional questions arise in considering whether or not a State law is preempted:

- What is a State law?
- What State law "relates to the privacy of individually identifiable health information?"
- When is a provision of State law "more stringent than" the analogous provision of the federal regulations?

State law means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law. Much State "privacy law" – e.g., the law concerning the physician/patient privilege – is not found in statutes, but is rather in State common law. *Common law* is:

> the body of law developed from judicial decisions based on custom and precedent, unwritten in statute or code, and constituting the basis of state legal systems.

The determination of common law is highly subjective and complex. Yet state privacy laws are largely common law.

What is a law that "*relates to privacy*"? The Privacy Rule says:

> Relates to the privacy of individually identifiable health information means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

Despite such a seemingly straightforward definition of 'relates', the definition may be difficult to apply. The meaning of the term 'relates' has been extensively adjudicated in a somewhat similar context, the issue of the preemption of State laws by ERISA. The U.S. Supreme Court alone has decided over a dozen ERISA preemption cases, and there are numerous lower court cases. These cases suggest an approach that looks to the legislative history of HIPAA and seeks to determine what kinds of State laws Congress meant to leave intact in deciding which State laws "relate to" or are relevant to privacy and which do not. Determining for each question of relevancy the intention of the Congress is difficult. Decisions are bound to be subjective and political in character and subject to change over time.

When is an analogous provision *contrary*? One definition embodies the tests that the courts have developed to analyze "conflict preemption." In this analysis, the courts will consider a provision of State law to be in conflict with a provision of federal law where it would be impossible for a private party to comply with both State and federal requirements or where the provision of State law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."

What is the meaning of "*more stringent*"? The issue of when a provision of State law is "more stringent" than the comparable requirements, standards, or implementation specifications of the HIPAA Privacy Rule is not an easy one. In general, "more stringent" should mean "providing greater privacy protection" but, such an interpretation leads to somewhat different applications, depending on the context. For example:

- a State law that provided for fewer and more limited disclosures than the HIPAA Privacy Rule would be "more stringent", but
- a State law that provides for more or greater penalties for wrongful disclosures than does the HIPAA privacy regulation would also be "more stringent."

In the former case, "more stringent" means less or fewer, while in the latter case, "more stringent" means more or greater. Some situations are more difficult to characterize. For example, if the HIPAA Privacy Rule requires disclosure to the individual on request and a State law prohibits disclosure in the circumstance in question, which law is "more stringent" or "provides more privacy protection"?

A continuum of regulatory options is available to determine what "more stringent" means. The two ends of the spectrum are:

- one end of the continuum is the minimalist approach of not interpreting the term "more stringent" further, and leaving the specific applications to later case-by-case determinations.
- the other end of the continuum is the approach of specifying criteria for future determinations.

Using the latter approach, DHHS specifies criteria for determining what "more stringent" means. The DHHS criteria are extrapolated from the principles of fair information practices, and some of the *criteria* follow:

- Limiting disclosure of personal health information protects privacy; thus, the law providing for less disclosure is considered to be "more stringent."
- The access of an individual to his or her protected health information is considered to be central to enabling the individual to protect such information. Thus a law granting greater rights of access is "more stringent."
- Many State laws require patients to authorize or consent to disclosures of their health information for treatment and/or payment purposes. Individual authorization is generally more protective of privacy interests than the lack of such authorization, so such State requirements would generally stand as being "more stringent".

However, each criterion can become very complicated. For instance, a State law requiring individual authorization is on the surface strong but would be preempted if the State law also permits a provider to require, as a condition of treatment for healthcare, an individual to authorize disclosures for purposes other than routine use.

3.8.4 Associations

An association is an organization of persons having a common interest. Healthcare associations may have their own health information privacy rules. DHHS examined privacy statements issued by five professional associations, one 'electronic network' association, and a managed care association. All these *associations* subscribe to these themes:

- An individual's health information should be protected;
- Policies need to ensure the confidentiality of protected health information;
- Only the minimum necessary information should be released to accomplish the purpose for which the information is sought.

Beyond these principles, the associations differ with respect to the methods used to protect health information. Major differences between the DHHS rules and the association standards include that the associations do not address:

- the individual's right of access to health information in the covered entity's possession,
- exceptions for research purposes,
- relationships between contractors and covered entities, and
- entities making their privacy policies available to patients through a notice.

The first two of these differences are elaborated next.

Only two of the five professional associations state that patients have the *right to review* their medical records. One association declares this as a fundamental patient right, while the second association qualifies their position by stating that the physician has the final word on a patient's access to the patient's health information. This second association also recommends that its members respond to requests for access to patient information within ten days, and recommends that entities allow for an appeal process when patients are denied access. Because the DHHS Privacy Rule requires that patients have access to their health information, large numbers of providers may have to modify their current practices in order to allow patient access.

Only one association explicitly made reference to information released for legitimate research purposes. The DHHS Privacy Rule allows for the release of protected health information for *research* purposes without an individual's authorization, but only for research that is supervised by an Institutional Research Board or a Privacy Board. This research requirement may cause some groups to revise their disclosure authorization standards.

Each organization has, of course, its own perspective. For example:

- The statements of the *managed care association*, while endorsing the general principles of privacy protection, are vague on the release of information for purposes other than treatment. The managed care association suggests allowing the use of protected health information without the patient's authorization for health promotion or marketing.
- The standards from the *'electronic network' association* advocate the protection of private health information from disclosure without patient authorization and emphasize that encrypting information should be a principal means of protecting patient information.

Health promotion or marketing is a primary concern of the managed care association. Encryption is a primary concern of the electronic network association. Each organization advocates privacy in a way consistent with its own best interests.

3.8.5 JCAHO

The Joint Commission on the Accreditation of Healthcare Organizations (JCAHO) and the National Committee on Quality Assurance (NCQA), as accrediting organizations, can contribute to the development of a common framework to guide the protection of personal health information (JCAHO/NCQA, 1999). JCAHO and NCQA have incorporated requirements for the protection of patient information into their standards and practices for evaluating healthcare organizations. Accreditation standards address requirements for health organizations to:

- obtain patient consent for release of information;
- treat patient medical records as confidential;
- incorporate confidentiality requirements into contractual agreements with third parties; and
- inform patients of their rights regarding access to their medical record information.

JCAHO and NCQA plan to extend their requirements to further influence confidentiality through their accreditation standards. Their guidelines do not refer to 'covered entities' but rather to 'Managed Care Organizations' (MCOs). The guidelines are presented next in the words of the accrediting bodies:

> MCOs should have clearly defined policies and procedures for dealing with confidentiality issues. Accountability is enhanced by having focal points who are responsible for assessing compliance with policies and procedures, for example, a security officer and a data disclosure board.
>
> MCOs should have a program of periodic audits to ensure compliance by staff and contractors with MCO policies and procedures. MCOs must verify that personally identifiable health information

shared with external organizations is used only for the purposes that were specified in the Notice of Privacy Practices, and that the external organization will comply with the MCO's policies.

As MCOs acquire information systems, they should require capabilities that provide a high level of security and confidentiality protection, including encryption, detailed user access controls, transaction logs, and blinded files. MCOs should leverage the sophistication of technology to solve special privacy issues, such as restricted access. Existing technology can set levels of authorization for access to patient data according to the role the user plays in a patient's care.

MCOs should maintain and routinely analyze records of all accesses or modifications to personal health information. Modifications or changes to data should be disseminated in a timely way to all other legitimate users to ensure data accuracy. To the extent possible, this tracking should be incorporated into computerized systems.

MCOs should provide their members with a detailed understanding of what personally identifiable health information is maintained, how it is kept, how it is used, who has access to it for clinical, reimbursement, or for quality oversight purposes, and any releases of information that are required by law. MCOs should make their policies and procedures known at the time of marketing and enrollment and reinforce them at the time of care delivery. These efforts should be continuous and multi-pronged.

MCOs should inform their members of their rights to review and comment about their personal health information and to review transaction logs that record accesses or changes to their personally identifiable health information.

MCOs should routinely provide training to their employees and contracted providers on how to be sensitive to confidentiality concerns and how to comply with confidentiality policies.

JCAHO and NCQA are created for and run by healthcare professionals. *JCAHO* and *NCQA* strive to reflect the preferences of healthcare professionals and at the same time to follow whatever laws and regulations apply to the professions. Thus their criteria for accreditation are a good indication of what is practical.

3.8.6 European Union

The *European Privacy Directive* (the Directive) was passed in 1995 and took effect in 1998. The Directive seeks to promote the free flow of personal information within the European Union while assuring a common, high level of privacy protection. The Directive constrains the flow of personal information from the European Union to other countries. Personal information transfers underpin many routine business transactions. Hence, while the Directive focuses its attention on protection of individuals in Europe, many of its consequences affect international enterprises. The Directive expresses an expectation that third countries would change their privacy regimes to conform to European assumptions (Collman, 1999).

3.8.6.1 Europe

The Directive applies to 'personal data', a general category covering information about individual human beings without regard to the sector of its use. *Personal data* includes information relating to an identified person ('data subject'), using direct or indirect means such as an identification number or one or more factors specific to the data subject's physical, physiological, mental, economic, cultural or social identity. This definition intends to cover all 'reasonable and likely' means of identifying an individual, including advanced statistical methods that are making identifying an individual easier and easier with less and less information. The Directive applies to processing of personal data primarily using automated means. It applies to manual means, if used in a structured filing system that allows easy access to personal data. The Directive does not apply to:

- personal data for uses by purely domestic or personal purposes,
- activities outside the scope of EU law, and
- processing related to EU Members' public security, state security, defense or criminal law.

The Directive creates rights for Europeans that Americans do not have with respect to use of personal data. Data subjects have the following rights with respect to processing of personal data about themselves, namely the right to:

- know the controller, purpose, types and proposed recipient of the information processing;

- gain access to the data to verify its truth and legality;
- know the 'logic' of automated processing;
- rectify, erase, or block processing of inaccurate data;
- object to processing of data, especially for marketing purposes;
- not be subject to decisions based on automated data processing;
- have access to judicial remedy for failure to respect their privacy rights.

Before information about an EU citizen can be sent to someone in a non-EU country, the privacy laws in the non-EU country must be validated as having *'adequate' safeguards*. The Directive states that adequacy of privacy protection shall be assessed:

> in light of all the circumstances surrounding a single or set of data transfers such as the nature of the data, the purpose and duration of the data processing operations, the country of origin, the country of final destination, and the general and sectoral rules of law as well the professional rules and security measures effective in a third country.

When a finding of inadequacy occurs, the Directive permits EU Member States to take measures preventing data transfers or to begin negotiations to remedy the adverse finding. The United States could reasonably expect a finding of 'inadequacy' with respect to its privacy safeguards.

The starchiness of the Directive makes interpretation of its meaning difficult in the networked world. The Directive assumes a world dominated by mainframe or client-server network architectures and person-to-business transaction. It uses terms such as 'controller' and implies fixed, easily identifiable *points of authority*. In a web-enabled Internet world, however, users may not know the 'location' in real space of a particular web site's 'controller'. Moreover, laptop technology makes everybody more mobile. In the course of one business trip, personal data on a laptop hard disk may cross borders between EU and non-EU countries many times.

3.8.6.2 United States

Transactions in personal data lie deeply embedded in business and trade between EU Member States and the United States of America. Global corporations move personal data all over the world in the course of their business ranging from trade transactions, to clinical and pharmaceutical research, to routine human resource management. A finding of inadequacy *jeopardizes* these transactions when personal data must flow from the EU to the United States. The US faces a finding of inadequacy for many reasons, including a sectoral approach to privacy rule making, and a reputation for privacy practices that frequently do not meet EU requirements.

Companies can comply with a Safe Harbor agreement between the United States and Europe to demonstrate compliance with the European Directive and thus maintain flows of personal data from EU Member States to the USA (Commerce, 2000). Organizations *self-certify* to the Department of Commerce. Topics covered in the 'Safe Harbor' include notice, choice, security, access, and enforcement.

The Safe Harbor agreement does not reconcile basic differences in the European and American approaches to privacy. Tensions are likely to arise. The HIPAA Privacy Rule gives the American healthcare sector a rigor in privacy regulation that would make that sector compliant with the European Union concerns for trusted partners. The progress with HIPAA might serve as an *exemplar* to other industries in the US.

3.8.7 Review Questions

1. What are some laws that Federal agencies must already follow about privacy and how do they relate to HIPAA?
2. What do state laws specify about a patient's access to his or her healthcare information?
3. HIPAA provides that contrary State laws that relate to the privacy of individually identifiable health information will not be preempted by the federal requirements, if they are "more stringent" than those requirements. What are some of the difficult questions that need to be answered in determining what is or is not "more stringent"?
4. What did the DHHS survey of five professional associations reveal about their recommendations to their memberships on privacy policies?
5. What is JCAHO's role in privacy rule enforcement?
6. What is the significance of the European Union Privacy Direction for American healthcare organizations?

3.9 Costs

Costs are difficult to estimate for implementing sweeping administrative changes. The first challenge in estimating the costs is to determine the different categories of activity that have to be funded and then to estimate the cost of each. Different organizations have produced reasonably similar breakdowns of the cost categories. However, the cost associated with each category varies widely. In this section, are presented one set of DHHS estimates that total about *$18 billion* for 10 years and then estimates sponsored by Blue Cross Blue Shield that total about *$40 billion* over 5 years.

3.9.1 Method

An analysis of the costs of the Privacy Rule requires a baseline from which to measure the Rule's effects. For some regulations, the *baseline* is relatively straightforward. For instance, an industry might widely use a particular technology, but a new regulation may require a different technology, which would not otherwise have been adopted by the industry. In this example, the old and widely used technology provides the baseline for measuring the effects of the regulation. The costs and the benefits are the difference between keeping the old technology and implementing the new technology. Where the underlying technology and industry practices are rapidly changing, however, it can be far more difficult to determine the baseline and thereby measure the costs and benefits of a regulation. There is no simple way to know what technology industry would have chosen, if the regulation had never existed, nor how industry practices would have evolved.

The entities covered by the HIPAA Privacy Rule are in the midst of a shift from paper records to electronic records. As covered entities spend significant resources on hardware, software, and other information technology costs, questions arise about which of these costs are fairly attributable to the Privacy Rule as opposed to costs that would have been expended in the absence of the Rule. Industry practices generally are *rapidly evolving*.

New technological or other measures taken to protect privacy are in part attributable to the expected expense of shifting to electronic medical records, rather than being solely attributable to the new regulations. In addition, the existence of privacy rules in other sectors of the economy help set a norm for what practices will be considered good practices for health information. The level of privacy protection that would exist in the healthcare sector, in the absence of regulations, thus would likely be affected by regulatory and related developments in other sectors. In short, projecting a cost baseline for the HIPAA Privacy Rule is difficult.

The common security practice of using ‘firewalls’ illustrates how each of three baselines might apply:

- Under the first baseline, the *full cost* of implementing firewalls should be included in a Regulatory Impact Analysis for a rule that expects entities to have firewalls. Because current law has not required firewalls, a new rule expecting this security measure must include the full cost of creating firewalls. This approach, however, would seem to overstate the cost of such a regulation. Firewalls would seem to be an integral part of the decision to move to an on-line, electronic system of records. Firewalls are also being widely deployed by users and industries where no binding security or privacy regulations have been proposed.
- Under the second baseline, the touchstone is the *level of risk* of security breaches for individually identifiable health information under current practices. There is quite possibly a greater risk of breach for an electronic system of records, especially where such records are accessible globally through the Internet, than for patient records dispersed among various doctors' offices in paper form. Using the second baseline, the costs of firewalls for electronic systems should not be counted as a cost of the regulation except where firewalls create greater security than existed under the previous, paper-based system.
- Finally, the third baseline would require an estimate of the typical level of firewall protections that covered entities would adopt in the absence of regulation, and include in the Regulatory Impact Analysis only the *extra costs*, those attributable exclusively to the Privacy Rule.

The DHHS analysis uses this 3rd baseline approach.

To *estimate costs*, DHHS used information from published studies, trade groups and associations, public comments to the proposed regulation, and fact-finding by staff. The analysis focused on the major policy areas in the regulation that would result in significant costs. Given the vast array of institutions affected by this regulation and the considerable variation in practices, DHHS identified the ‘typical’ current practice for each of the major policy areas and estimated the cost of change resulting from the regulation. The major costs that covered entities will incur are one-time costs associated with implementation of the Rule and ongoing costs that result in continuous requirements in the Rule.

The costs of complying with the Privacy Rule is related to the number of affected entities and the number of affected transactions in each entity. There are approximately:

- 12,200 health plans (including self-insured employer and government health plans that are at least partially self-administered),
- 6,500 hospitals, and
- 630,000 non-hospital providers.

that will bear implementation costs under the Rule.

The cost of some provisions were estimated by using the Census Bureau's "Current Population Survey" wage data for the classes of employees affected by the Rule. The hourly wage of the type of employee assumed to be mostly likely responsible for compliance with a given provision was determined. Where a number of different types of employees might be responsible for complying with a certain provision, as is often expected to be the case, a weighted-average wage was determined based on the types of employees involved. Finally, assumptions were made regarding the number of person-hours per institution required to comply with the Rule. The estimates are averages across the entire class of non-hospital healthcare providers, hospitals, or health plans in question. Underlying all annual cost estimates are *growth projections*.

The DHHS cost estimates are interesting for the cost details but also as a *guide to implementation*. DHHS's cost estimates are based on details about what roles would be expected to spend how much time doing what. Thus DHHS's cost computations provide a blueprint for implementing the privacy regulations.

3.9.2 Biggest Budget Items

The largest costs are associated with the minimum necessary provision and the privacy official, which together constitute over half of the anticipated 10 year cost of compliance.

3.9.2.1 Privacy Official

The Privacy Rule requires entities to designate a privacy official who will be responsible for the development and implementation of privacy policies and procedures. Some costs for the privacy official, particularly in the initial years, are subsumed in other cost requirements. Nonetheless, the privacy official will have to address additional ongoing responsibilities, such as coordinating between departments, evaluating procedures and assuring compliance. To avoid double counting, the cost calculated here is only for the ongoing, operational functions of a *privacy official* (e.g., clarifying procedures for staff) that are in addition to other items, such as developing policy.

The privacy official role could be an additional responsibility given to an existing employee in the covered entity, such as an office manager in a small entity or a compliance official in a large institution. Any covered entity that handles individually identifiable health information has one or more people with responsibility for handling and protecting the confidentiality of such information. Non-hospital providers will need to devote, on average, an additional half hour per week of an official's time to compliance with the Privacy Rule for the first two years and one quarter hour per week for the remaining eight years. For hospitals and health plans, which are more likely to have a greater diversity of activities involving privacy issues, three hours per week for the first two years, and one and a half hours per week for the remaining eight years are predicted. Wages would be:

- $34 per hour for managers of non-hospital health,
- $79 for senior hospital planning officers, and
- $88 for claims executives at health plans.

Although individual hospitals and health plans may not necessarily select their *planning officers* or *claims executives* to be their privacy officials, they should be of comparable responsibility, and therefore comparable pay, in larger institutions. The initial year cost for privacy officials will be $700 million; the ten-year cost will be $5.9 billion.

3.9.2.2 Minimum Necessary

Beyond the policy for the overall entity approach to privacy and the privacy official role, the DHHS assessment allotted specific costs to a handful of other specific activities, such as implementing the '*minimum necessary*' requirement. To determine the policies for the minimum necessary requirement, each

- hospital would spend 160 hours,
- health plan would spend 110 hours, and
- non-hospital provider would spend 10 hours.

Once the policies are established, there will be costs resulting from implementing the new policies to restrict internal uses of protected health information to the minimum necessary. Implementing the 'minimum necessary standard' in the first year will require 560 hours for hospitals, 160 hours for health plans, and 10 hours for non-hospital providers. On an annual ongoing basis after the first year, hospitals will require 320 hours, health plans 100 hours, and non-hospital providers 10 hours to comply with this provision. The wage for healthcare providers is estimated at $47; and the wage for health plans is estimated to be $34. The total cost of the 'minimum necessary' provision over 10 years is $5.8 billion.

3.9.3 Other Internal Operations

Policy development and training are substantial internal operations both of which have a large start-up cost but may require continual attention.

3.9.3.1 Policy Development

The Privacy Rule imposes a variety of requirements for entities to develop policies to establish and maintain compliance. These include policies such as those for inspection and copying, amending records, and receiving complaints. To the extent practical, consistent with maintaining adequate protection of protected health information, the Rule is designed to encourage the development of policies that apply across all entities of a given type. Such generic models will *reduce costs* and will facilitate greater consistency across entities.

Trade and professional associations and other groups serving large numbers of members or clients will develop materials that can be used broadly. These materials will likely include

- the model privacy practice notice that all covered entities will have to provide patients;
- general descriptions of the regulation's requirements appropriate for various types of healthcare providers;
- checklists of steps entities will have to take to comply;
- training materials; and
- recommended procedures or guidelines.

Using Faulkner and Gray's *Health Data Directory 2000*, DHHS identified hundreds of associations that are likely to provide guidance to members. Some associations would provide hundreds of hours of legal analysis at $150 per hour, and hundreds of hours of senior analyst's time at $50 per hour.

The development of policies will occur at two levels:

- first, at the *association* level and
- second, at the *entity* level.

Covered entities will require some time for internal policy development beyond what is provided by associations or outside consultants. For most non-hospital providers, the external assistance will provide most of the necessary information. These non-hospital providers will need only eight hours to adapt these policies for their specific use. Hospitals and health plans, which employ more individuals and are involved in a wider array of endeavors, are likely to require more specific policies tailored to their operations to comply with the Privacy Rule. These entities will require an average of three hundred hours of policy development per institution.

3.9.3.2 Training

The Privacy Rule requirements provide covered entities with considerable flexibility in how to best fulfill the necessary *training* of their workforce. As a result, the actual practices may vary substantially based on such factors as the number of members of the workforce, the types of operations, worker turnover, and experience of the workforce. Training is estimated to cost $737 million over ten years. At the time of the effective date, approximately 6.7 million healthcare workers will have to be trained, and in the subsequent ten years, 7 million more will have to be trained because of worker turnover.

Covered entities will need to provide employees with varying amounts of training depending on each employee's responsibilities, but on average, each member of the workforce who is likely to have access to protected health information will require one hour of training in the policies and procedures of the covered entity. The initial training cost estimate is based on teacher training with an average class size of ten. After the initial training, some training (for example, new employees in larger institutions) will be done by videotape, videoconference, or computer, all of which are likely to be less expensive. Training materials are assumed to cost an average of *$2 per worker*.

3.9.4 Dealing with Patients

The following activities involve communication between the patient and the covered entity.

3.9.4.1 Notice

Healthcare providers with direct treatment relationships are required to provide a *notice of privacy practices* no later than the date of the first service delivery to individuals after the compliance date for the covered healthcare provider. For most types of healthcare providers (such as physicians, dentists, and pharmacists) one notice would be distributed to each patient during his or her first visit following the compliance date for the covered provider, but not for subsequent visits. For hospitals, however, a notice would be provided at each admission, regardless of how many visits an individual has in a given year. In subsequent years, non-hospital providers would only provide notices to their new patients, because it is assumed that providers can distinguish between new and old patients, although hospitals will continue to provide a notice for each admission. The total number of notices provided in the initial year is estimated to be 800 million. In years 2004 through 2012, 5.3 billion notices will be provided. Health plans might include their privacy policy in the annual mailings they make to members, such as by adding a page to an existing information booklet.

The printing cost of the policy is estimated to be $0.05. At $0.05, the total cost of the initial notice is $50 million. Using a standard growth rate for patients, the total cost for producing and distributing notices is estimated to be $400 million for the ten-year period. The costs of soliciting, obtaining, and storing acknowledgments of having seen the Notice might add another $230 million to the costs.

3.9.4.2 Inspection and Copying

Records are routinely copied as part of treatment or when patients change providers. In addition, copying occurs as part of legal proceedings. Nine hundred million pages of medical records are copied each year in the United States. The average medical record is 31-pages long. Only 10 percent of all requests are made directly from patients, and of those, most are for transfer to another provider, not for purposes of individual *inspection*. Twenty-five percent of direct patient requests to copy medical records are for purposes of inspecting their accuracy (i.e., 2.5 percent of all copy requests) or 850,000 in 2003 if the current practice remained unchanged.

As patients gain more awareness of their right to inspect and copy their records, more requests will occur. A 10 percent increase in the number of requests to inspect and copy medical records over the current baseline would amount to a little over 85,000 additional requests in 2003 at a cost of $1 million. The total cost for the ten-year period would be $17 million.

The Privacy Rule allows a provider to deny an individual the right to inspect or obtain a copy of protected health information in a designated record set under certain circumstances, and that the patient can request the denial to be reviewed by another licensed healthcare professional. DHHS estimates there will be about 12 million requests for inspections over the ten-year period. If one-tenth of one percent of these requests results in a *denial* in accordance with the rule, the result would be 12,000 cases. Not all these cases would be appealed. If 25 percent were appealed, the result would be 3,000 cases. If a second provider were to spend a quarter of an hour reviewing the case, the cost would be $6,000 in the first year and $90,000 over 10 years.

3.9.4.3 Amendments

Many providers and health plans currently allow patients to amend the information in their medical record, where appropriate. The principal economic effect of the Privacy Rule would be to expand the right to request *amendments* to those who are not currently covered by amendment requirements under state laws or codes of conduct. In addition, the rule may draw additional attention to the issue of inaccuracies in information and may stimulate patient demand for amendment of medical records.

Individuals who request an opportunity to amend their medical record have already obtained a copy of it. Therefore, the administrative cost of amending the patient's record is separate from inspection and copying costs.

DHHS assumes that one-quarter of the people who request to inspect their records will seek to amend them. Over ten years, the number of expected amendment requests is 2.7 million. The provider or health plan is not required to evaluate any amendment requests, only to append or otherwise link to the request in the record. Sometimes an assistant will only make the appropriate notation in the record, requiring only a few minutes; other times a provider or manager will review the request and make changes if appropriate, which may require as much as an hour. DHHS estimates half an hour for each amendment request at a cost of $47 per hour. The first-year cost for the amendment policy is estimated to be $5 million. The ten-year cost of this provision is $80 million.

3.9.4.4 Complaints

The Privacy Rule requires each covered entity to have an internal process to allow an individual to file a complaint concerning the covered entity's compliance with its privacy policies and procedures. The covered entity only is required to receive and document a complaint (no response is required), which will take, on average, ten minutes (the complaint can be oral or in writing). Since one in every thousand patients is expected to file a complaint, approximately *10 million complaints* will be received over ten years. Based on a weighted-average hourly wage of $47 and ten minutes per complaint, the cost of this policy is $7 million in the first year. Using wage growth and patient growth assumptions, the cost of this policy is $100 million over ten years.

3.9.4.5 Accounting of Disclosures

A certain percentage of patient records held by a particular entity type will have a disclosure that will have to be recorded in the individual's record.

Assumptions are provided for the rate of disclosures by provider entity type as follows:

- fifteen percent of all patient records held by a hospital,
- ten percent of ambulatory care patient records, and
- five percent of nursing home, home health, dental and pharmacy provider patient records.

These percentages represent about *60 million disclosures* that will have to be recorded in the first year, with each recording estimated to require two minutes. At the average nurse's salary of $30 per hour, the cost in the first year is $26 million. For health plans, disclosures of protected health information are more rare than for healthcare providers. At the average wage for the insurance industry of $34 per hour, the initial cost for health plans is $7 million. The ten-year cost for providers and health plans is $500 million.

Although hospitals generally track patient disclosures today, hospitals may seek to update software systems to assure full compliance. Each upgrade would cost $35,000 initially and $6,300 annually thereafter, for a total cost of $570 million over ten years.

The Privacy Rule requires covered entities to provide individuals with an *accounting of disclosures* upon request. One in a thousand patients will request such an accounting each year, which is approximately 850,000 requests. If a nurse takes an average of five minutes to copy any disclosures, then the cost for the first year is $2 million. The total ten-year cost is $34 million.

3.9.4.6 Authorizations

Authorizations are required in various circumstances, such as for disclosure of protected health information to an employer for an employment physical. Obtaining authorization under such circumstances is current practice, and thus entails no extra cost. To use or disclose psychotherapy notes for most purposes (including for treatment, payment, or healthcare operations), an entity must obtain specific authorization by the individual that is distinct from any authorization for use and disclosure of other protected health information. This is current practice, so there is also no new cost associated with these *authorizations*.

The requirement for obtaining authorizations for use or disclosure of protected health information for most *marketing* activity will make direct third-party marketing more difficult because covered entities may not want to obtain and track such authorizations, or they may obtain too few to make the effort economically worthwhile. However, the Privacy Rule permits an alternative arrangement: the covered entity can engage in health-related marketing on behalf of a third party, presumably for a fee. Moreover, the covered entity could retain another party, through a business associate relationship, to conduct the actual health-related marketing, such as mailings or telemarketing, under the covered entity's name. The effect is to change the arrangement of practices to enhance accountability of protected health information by the covered entity and its business associates; however, there is nothing inherently costly in these changes.

3.9.5 Exceptions

Protected health information can be disclosed without authorization under the approval of a business associate agreement or an Institutional Research Review Board. De-identification removes protected health information from the status of protected. Together these conditions of business associate, research, and de-identification could be called exceptions and have costs varying on the extent to which the covered entity engages the exception.

3.9.5.1 De-identification

The Privacy Rule allows covered entities to use de-identified health information. Entities that de-identify information will have to review data flows to assure compliance with the Rule. For example, an automated system may need to be re-programmed to remove additional identifiers. Health plans and hospitals would have an average of two existing agreements that would need to be reviewed and modified. These agreements would require an average of 150 hours by hospitals and 120 hours by health plans to review and revise to conform to the Privacy Rule. Using the weighted average wage of $47, the initial costs will be $120 million, and the total cost will be *$1.1 billion* over ten years.

The Privacy Rule and the increasing trend toward computerization of large record sets will result over time in de-identification being performed by relatively few firms or associations. Whether the covered entity is a small provider with relatively few files or a hospital or health plan with large record files, it will be more efficient to contract with specialists in these firms or associations (as 'business associates' of the covered entity) to de-identify files. The process will be different but the ultimate cost is likely to be the same or only slightly higher, if at all, than the costs for *de-identification* today.

3.9.5.2 Research

Researchers who seek individually identifiable health information and the Institutional Review Boards (IRBs) that review research projects will have additional responsibilities. A covered entity doing research will need to seek IRB approval, if it wants to avoid the requirement to obtain authorization for use or disclosure of protected health information for research. Thus costs will exist for research already using IRBs and for research not yet using IRBs as follows:

- Of the estimated 4,000 IRBs in existence, the median number of initial current research project reviews is 133 per IRB, of which only ten percent do not receive direct consent for the use of protected health information. (Obtaining consent nullifies the need for IRB privacy scrutiny.) Therefore, in the first year of implementation, there will be 77,000 initial reviews affected by the regulation, and the requirement to consider the privacy protections in the research protocols under review will add an average of 1 hour to each review. Each of the affected 77,000 studies will require an average of an additional 8 hours of time for protocol development and implementation. At the average medical scientist hourly wage of $47, the initial cost is $32 million; and the total ten-year cost of these requirements is $470 million over ten years.
- The total volume of non-IRB reviewed research is equal to 25 percent of all IRB-reviewed research, leading to 19,000 new IRB reviews in the first year of the regulation. The total one-year cost for new IRB and privacy board reviews is $8 million. The total ten-year cost for the new research requirements is *$100 million*.

3.9.5.3 Business Associates

The Privacy Rule requires a covered entity to have a written contract or other arrangement that documents satisfactory assurance that a business associate will appropriately safeguard protected health information. Business associate contracts should be fairly standard, except for language that will have to be tailored to the specific arrangement between the parties, such as the allowable uses and disclosures of information. The standard language initially will be developed by trade and professional *associations* for their members. The trade and professional associations' work plus any minor tailoring of it by a covered entity would amount to one hour per non-hospital provider and two hours for hospitals and health plans. The larger figure for hospitals and health plans reflects the fact that they are likely to have a more extensive array of relationships with business associates. Changes in business associate contracts will cost $100 million. This will be an initial year cost only because this contract language will become standard in future contracts.

Table "Nolan Training Costs"

Category of Organization	Hospitals	Physician Offices
# Employees	5,100,000	1,600,000
Assumed % industry staff to be trained	95%	90%
# of Employees to be trained	4,900,000	1,500,000
Hours of training	2	1.5
Cost per hour	$22	$40
Subtotal 1st Year	$215,000,000	$87,000,000
Number of Classes	250,000	70,000
Instructor Cost	$40,000,000	$8,000,000
Materials Cost	$20,000,000	$7,000,000
Total First Year	$280,000,000	$100,000,000
Segment Turnover Rate	5%	4%
New Hire Costs	$14,000,000	$4,000,000
Refresher Training	$55,000,000	$20,000,000
Total Subsequent Year Cost	$73,000,000	$26,000,000
Total 5 Year Cost	$570,000,000	$210,000,000

The regulation includes a requirement that the covered entity take steps, if the entity knows of violations by a business associate. This oversight requirement is consistent with standard *oversight* of a contract.

Covered entities will have to establish policies to ensure that only the *minimum necessary* protected health information is shared with business associates. To the extent that data are exchanged, covered entities will have to review the data and systems programs to assure compliance. For non-hospital providers, the first year will require an average of three hours to review existing agreements, and thereafter, they will require an additional hour to assure business associate compliance. Hospitals will require an additional 200 hours the first year and 20 hours in subsequent years; health plans will require an additional 110 hours the first year and 10 hours in subsequent years. The cost of the covered entities assuring business associates' complying with the 'minimum necessary' requirement is $200 million in the first year, and a total of $700 million over ten years. These estimates include both the cost for the covered entity and the business associates.

3.9.6 A Different Estimate

The preceding estimates are provided courtesy of the DHHS. However, some organizations disagree with the estimates. The *Blue Cross Blue Shield* Association asked the Robert E. Nolan Company to analyze federal privacy proposals to determine their

Industry	Year 1 Privacy Costs Per Establishment in $1,000s	Average Year 2-10 Privacy Costs per Establishment in $1,000s
Drug Stores & Proprietary Stores	6	4
Accident & Health Insurance & Medical Service Plans	62	28
Medical Equipment Rental & Leasing	4	2
Offices of Doctors of Medicine	4	2
Offices of Dentists	2	1
Offices of Doctors of Osteopathy	3	2
Offices of other Health Practitioners	2	1
Nursing & Personal Care Facilities	8	5
Hospitals	102	38
Medical & Dental Laboratories	3	2
Home Healthcare Services	6	3
Miscellaneous Health	4	2
Average for all Small Business	4	2

Table "Average Per Small Business Cost": Average Annual per Establishment Privacy Costs

impact on the U. S. healthcare economy. The Nolan report is as detailed as the DHHS report but has different results.

Nolan found that the implementation of commonly proposed privacy rules would add an additional $43 billion in costs over a 5 year period (Nolan, 1999). According to the Nolan report these costs would be administrative in nature and not add additional benefits. The $43 billion in costs includes the following:

- $1.94 billion for rules requiring new authorizations from current subscribers to use their data for treatment, payment of claims, or other operations;
- $9.1 billion for requirements that healthcare organizations track disclosures of protected health information and retain for 7 years;
- $4.0 billion for standards that allow patients and subscribers to inspect, copy and amend information; and
- $23.4 billion for infrastructure supporting implementation of above provisions (systems, training, and other compliance costs)

To understand in further detail these costs one item will be further examined. For training Nolan estimates that $1.4 billion over 5 years will be required. This contrasts to the DHHS estimate of $737 million dollars over 10 years. The variance in estimates for training costs is on a par with the overall variation in estimates between DHHS and Nolan. In other words, the Nolan estimates are several times greater than the DHHS estimates.

Nolan's training analysis is as detailed as DHHS's. Nolan looks at ten categories of organizations, including hospitals, physician offices, dentist offices, and insurance carriers. Within each category of organization, Nolan presents fifteen facets that include number of employees, percent of employees to be trained, hours of training required, and cost per hour of training. The full details for two of the organization categories are presented in the Table "Nolan Training Costs". From such an analysis Nolan concludes a *$1.4 billion 5-year training cost*.

3.9.7 Small Entities

The government estimates that small entities will bear very little cost to achieve HIPAA compliance. The *Small Business Administration* defines small businesses in the healthcare sector as those organizations with less than $5 million in annual revenues. These small businesses represent 80% of all healthcare establishments. While small businesses represent a significant portion of the total number of healthcare establishments, they represent a small portion of the revenue stream for all healthcare establishments. In 1997, the small healthcare businesses generated approximately $430 billion in annual receipts, or 30% of the total revenue generated by healthcare establishments.

Wherever possible, the Privacy Rule provides a covered entity with flexibility to create policies and procedures that are best suited to the entity's current practices in order to comply with the Rule. This allows the covered entity to assess its own needs in devising, implementing, and maintaining appropriate privacy policies, procedures, and documentation.

Provision	**Cost in Millions of $s**		
	First Year Cost (2003)	**Average Annual Cost (Years 2-10)**	**Ten Year Cost (2003-2012)**
Policy Development	600	0	600
Minimum Necessary	930	540	5,800
Privacy Officials	720	580	5,900
Disclosure Tracking/History	260	96	1,130
Business Associates	300	56	800
Notice	220	45	620
Copying	1	2	19
Amendment	5	8	77
Requirements on Research	40	60	580
Training	290	50	740
De-Identification of Information	120	120	1,200
Employers with Insured Group Health Plans	50	0	50
Internal Complaints	7	11	110
Total*	3,200	1,600	18,000
Net Present Value	3,200	900	12,000

Table “Costs of Privacy Compliance”: The Cost of Complying with the Proposed Privacy Regulation, in Dollars

This approach allows covered entities to strike a *balance* between protecting privacy of individually identifiable health information and the economic cost of doing so.

To determine the costs for small businesses, the costs were basically distributed proportionally among the businesses. On a per-establishment basis, the average cost for small business of complying with the proposed rule in the first year is $4,000 per-establishment (see Table “Average Per Small Business Cost”). The ongoing costs of privacy compliance are approximately $2,000 each year thereafter. These costs may be offset in many firms by the savings realized through requirements of the Transactions Rule.

3.9.8 Overall

The savings and costs generated by all administrative simplification standards should result in a net savings to the healthcare system. HIPAA states:

> any standard adopted under this part shall be consistent with the objective of reducing the administrative costs of providing and paying for healthcare.

This statement refers to the administrative simplification regulations in their totality, including the Privacy Rule. The Transactions Rule shows a net savings of *$29.9 billion* over ten years (2002-2011), or a net present value savings of $19 billion. This estimate does not include the growth in e-health and e-commerce that may be spurred by the adoption of standards.

The DHHS estimated cost of compliance with the Privacy Rule is $17.6 billion over the ten year period, 2003-2012. The net present value, applying a 11.2 percent discount rate, is $11.8 billion. The first year estimate is *$3.2 billion* (this includes expenditures that may be incurred before the effective date in 2003). This represents about 0.23 percent of projected national health expenditures for 2003. By 2008, seven years after the rule’s effective date, the rule is estimated to cost 0.07 percent of projected national health expenditures.

Over all entities large and small, the largest initial costs (see Table “Costs of Privacy Compliance”) result from

- the minimum necessary provisions pertaining to internal uses of individually identifiable health information, and
- the cost of a privacy official.

Covered entities will also have recurring costs for training, disclosure tracking, and notice requirements. A small number of large entities may have significant costs for de-identification of protected health information and additional requirements for research.

3.9.9 Review Questions

1. What method did DHHS use in estimating the costs of implementing privacy?
2. What are the biggest cost items in the DHHS cost estimate?
3. What are some of the roles involved in the implementation of privacy and what are the typical salaries for these roles in different entities?

4. What is the difference between the DHHS and Nolan Report estimates and how can the difference be explained?
5. The DHHS cost estimates sound reasonable. The Nolan Report cost estimates sound reasonable. What are some factors that could lead to different levels of cost. (Project Question)

3.10 Case Studies

Health care entities have implemented privacy compliance programs in different ways, but the similarities are marked. Two examples follow.

3.10.1 Air Force

The U.S. *Air Force* health system is massive and obligated to comply with HIPAA (Rada, 2002a). To make HIPAA compliance a workable solution, each of the Air Force *Medical Treatment Facilities* (MTFs) appointed a HIPAA Implementation Coordinator and Privacy Officer.

The Privacy Officer is of sufficient rank and experience to make an impact on the organization and be part of the executive committee -- someone like the Administrator, Risk Manager or another officer with sufficient relevant experience. He is responsible for implementing existing Air Force privacy policy, defining local policy to meet specific situations, ensuring the staff receives privacy training, and establishing procedures for dealing with privacy complaints. The *Privacy Officer* reports functionally to the executive committee to ensure that the MTF as a whole is compliant with the privacy rule.

The HIPAA *Implementation Coordinator* ensures that privacy and security requirements are meshed at the local level and is the go-to person for updates. He is also the chair for the HIPAA Compliance Implementation Team composed of the Privacy Officer, the *Medical Information Systems Readiness Team* (MISRT), and contracted support. This is not a permanent position, as it will be dissolved upon full implementation of HIPAA at the MTF. The MISRT has representatives from

- Information management,
- Medical clinics, and
- Patient administration.

The MISRT should have a direct reporting link to the executive committee and its charter should ensure that it has the ability to implement the requirements of HIPAA.

In order to best support the MTFs for HIPAA privacy compliance, Headquarters contracted for consulting services to assist with HIPAA Privacy implementation. Throughout 2002, training was provided on different aspects of HIPAA, starting with the *Risk Assessment* training that helped each facility understand its organizational privacy and security risks

The MISRT meets at least monthly. The agenda and tracking of action items are the responsibility of the chair. *Deliverables* include the following:

1. Gap analysis,
2. Development of local policy where gaps exist,
3. Recommend changes in business processes to comply with HIPAA rules,
4. Monitor implementation with HIPAA Compliance Program,
5. Oversee initial training of MTF staff on Privacy.

The chair publishes minutes and reports to the MTF Commander. The Team is dissolved upon full implementation of HIPAA at the facility.

3.10.2 Kindred

Kindred Healthcare, Inc. (www.kindredhealthcare.com) provides long-term healthcare services primarily through the operation of nursing centers and hospitals. Its Health Services Division operates 288 nursing centers, with 38,000 licensed beds in 32 states, and a rehabilitation therapy business. Its Hospital Division operates 64 hospitals, with 5,300 licensed beds in 24 states, and an institutional pharmacy business. Kindred employs about 53,000 people who care for more than 34,000 patients and residents each day.

Kindred's Privacy Program begins with the *Executive Board* of Kindred which appointed a HIPAA Advisory Committee chaired by the Corporate Compliance Officer (Pfeiffer, 2002). Feeding this Committee are people from Kindred's:

- Compliance Department
- Corporate Law Department
- Information Systems, and
- Human Resources.

This Committee in turn divides the compliance program into 3 top-level units called:

- hospitals,
- long-term care, and
- corporate.

The *Privacy Project* began in Jan. 2001 with the appointment of the HIPAA Advisory Committee. This Committee developed a proposal that was approved in May 2001. The schedule for 2001 proceeded as follows:

- In May an educational awareness program began that continues in perpetuity.
- In May through August the Committee developed policies and procedures that were approved in September.
- In May through August, the Committee developed a program plan which resulted in an approved budget for 2002 in September 2001.

The Privacy Project in 2002 included

- a state law privacy assessment,
- integration of the privacy policies and procedures into the organizational policies and procedures,
- inventory of contracts and the need for business associate agreements, and
- the development of training programs and piloting of those training programs.

For 2003 the compliance training rollout is completed by April 2003.

Kindred has developed a listing of types of service it offers and whether or not a *business associate* agreement is needed (see Table "Kindred Business Associate Conditions"). While the entries in this table could apply to many health care entities, they particularly reflect the activity of long-term care, such as wheelchair transportation and beautician.

Table "Kindred Business Associate Conditions": The left-most column is the type of service for which a business associate addendum or contract is considered. The comment column helps interpret why or why not a business associate agreement would be needed.

Type of Service	Business Associate Addendum Needed?	Comments
Activity Consultant	Yes	
Ambulance	No	Treatment
Ancillary Charge System	Yes	
Attending Physician	No	Treatment
Attorney External	Yes	
Audiology	No	Treatment
Beautician	No	Workforce
Behavior Health Therapist	No	Treatment
Nurse Instructor Consultant	Yes	
Chaplains	No	No protected health information disclosed
Chiropractor	No	Treatment
Students training	No	Workforce
Computer consultant	Yes	

Contracted Billing	Yes	
Copy Machine Vendor	Yes	
Dentist	No	Treatment
Dietician	No	Treatment
Home Health	No	Treatment
Hospice	No	Treatment
JCAHO	Yes	
Laboratory	No	
Massage Therapy	No	Treatment
Medical Director	Yes	
Medical Equipment	No	Treatment
Medical Records Consultant	Yes	
Optometry	No	Treatment
Pharmacy	No	Treatment
Researchers	Yes	
Social Services Agency	No	Treatment
Third Party Billing	Yes	
Transcription Service	Yes	
Wheelchair Transportation	No	Treatment

3.11 Opposition

Main Points

- Providers and payers lobby the government to modify the Privacy Rule so as to reduce the obligations on themselves.
- The proper regulation should respect the balance between the rights of individuals to privacy and the preservation of the common good which may entail some restrictions on privacy.
- Information warfare and privacy are intimately linked, and the implications for healthcare must be considered.

Opposition has come for some time from the providers and payers to the Proposed and Final Privacy Rules. The complex relations among government, the healthcare industry, and the public will determine the future of the Privacy Rule (Rada and Gue, 2001).

3.11.1 Views

The diversity of *political views* is reflected in excerpts from news reports in February 2001 (AHA, 2001 and Pear, 2001). In a February meeting of the U.S. Senate Committee on Health, Education, Labor and Pensions, Senators debated whether DHHS should reopen and thus delay the Privacy Rule. Some committee members questioned the cost and feasibility of the implementation schedule of the regulations. Others called for implementing, enforcing and expanding the privacy rules. Committee Chairman Jim Jeffords said he has asked the General Accounting Office to interview a variety of health care organizations and report the results in order to help the committee determine the need for additional *legislation* to change the regulations.

Senator Pat Roberts said he was stunned and terribly worried by the rules. He added that in parts of Kansas hospitals are short of doctors and nurses and are struggling to keep their doors open and they cannot cope with the new regulations. The healthcare industry is lobbying the government to delay, change, or kill the regulations.

On the side supporting the legislation came other voices:

- Senator Ted Kennedy said the burden of health care systems' compliance with the regulations is less than the burden of someone having to find a new job after being fired because of an employer's knowledge of the employee's health information.

- Senator Hillary Clinton said the regulations need to be stronger and expressed concern about the possible release of patient information for marketing purposes.

Janlori Goldman, director of the Health Privacy Project at Georgetown University, said the rules met a genuine need. She said that millions of Americans withhold information from doctors or provide inaccurate information in an effort to avoid the stigma or discrimination that might result from the disclosure of medical secrets.

Attorney John Houston testifying on behalf of the American Hospital Association said:

> Because nearly 50% of hospitals' patients are Medicare and Medicaid beneficiaries, we believe Congress should closely examine the high costs associated with implementing the privacy rule and supply the necessary funds to ensure that implementation does not put hospitals in financial jeopardy.

Hospitals, insurance companies, health maintenance organizations and medical researchers say the rules would impose costly burdens.

The American Medical Association (AMA) took a very strong stand against the Proposed Privacy Rule. The AMA made diverse points including:

- On the one hand, the AMA wanted stricter privacy rules that limited access and covered more entities (Anderson, 2000). The AMA said that under the HIPAA Privacy Rule patients' confidential information could be disclosed without their consent for a broad array of purposes unrelated to the patient's individual treatment or payment and extending far beyond the necessary disclosures and uses patients would expect when they seek healthcare. HIPAA did not give the government enough authority to enforce privacy with the business associates of physicians, but holding physicians accountable for how those business associates would use patient information was an unreasonable burden on physicians.
- On the other hand, the AMA opposed privacy regulations because they are expensive for doctors to implement. The AMA claimed that the administrative burden would have a disproportionate impact on small physician offices.

The AMA also said that the confidential relationship at stake is between the patient and his or her physician, and not between the patient and the healthcare system. The physician is the guardian standing between patients and the unrestricted use and access to patients' private medical records. The HIPAA Privacy Rule is founded on the principle that the patient shares information with the healthcare organization over which the patient has ultimate, continuing authority. The AMA suggested that the patient surrenders authority over the patient information by entering into a relationship with a doctor. The doctor then has authority over the information.

Ultimately, neither the providers nor insurance companies pay for healthcare, but patients, their employers, and government pay. If the problem is that healthcare providers cannot afford to implement the regulations, then perhaps their re-imbursement schemes should be modified so as to accommodate costs incurred for supporting privacy. The government analysis says that the savings from implementing the Transactions Rule will offset the costs of implementing the Privacy Rule. If this analysis is wrong, then the options are to either reduce *expenditures* elsewhere in the healthcare system or to pay covered entities more to implement privacy.

3.11.2 Balance

Some people say privacy is under siege. Although privacy is cherished, so are other goods. Should a person have a right to know whether those who care for his or her mother in a home for the elderly have a record of abusing the elderly? Evidence shows that such criminal records in nursing home staff are not rare (LaGrasse, 1998). Privacy must be balanced with the common good. When courts or common parlance cite the common good, the reference is often to either

- public safety or
- public health.

In important matters of public health and safety, privacy may need to be sacrificed.

The social philosophy of *communitarianism* holds that a good society crafts a careful balance between individual rights and the common good (Etzioni, 1998). In a society that strongly enforces social duties but neglects individual rights (as does Japan, for instance, when it comes to the rights of minorities), fostering individual rights might improve the balance. In the United States, individual rights are given high priority.

Privacy involves at least government, business, and the individual. American culture, policy, and law tend to protect the individual from *privacy invasion* from the government more so than from business. However, in the United States business may be guiltier than government of invading privacy.

According to Etzioni (1999):

> Although they [citizens] fear Big Brother most, they need to lean on him to protect privacy better from Big Bucks.

Citizens need to break the *privacy paradox* of distrusting the government that would help them. Citizens need protection from the government against business privacy invasion.

The challenge of balancing privacy and public good is particularly difficult in the context of specific historical and social conditions. Four criteria can be used to help determine whether an imbalance exists:

- First, a society should take steps to limit privacy only if it faces a well-documented and macroscopic threat to the common good. For instance, when many thousands of lives are lost, as with HIV, society faces a clear and major threat that may merit some infringement on privacy to manage.
- The second criterion is that the society tries first to use non-privacy threatening measures to remove the danger to the common good. For instance, when medical records are needed by researchers, the data should be collected as much as possible without identifying individuals.
- Third, to the extent that privacy-curbing measures are introduced, a communitarian society makes them as minimally intrusive as possible. For instance, the National Practitioner Data Bank allows a hospital that is considering whether to grant a physician the right to practice in the hospital to conduct limited background checks on the physician. The Data Bank discloses only high-level facts, such as that a physician's license to practice medicine was revoked, and does not give details of the violations. Because the hospital will know that a physician would not have had his license revoked for other than serious cause, the hospital does not need to know more detail.
- Fourth, measures that treat undesirable side effects of needed privacy diminishing measures are to be preferred over those that ignore these effects. Thus, if more widespread HIV testing is deemed necessary to protect public health, efforts must be made to enhance the confidentiality of the records of those tested.

Although the proceeding might include examples where invasion of privacy supports the public good, opposite examples exist. For instance, medical records are used at the expense of privacy where the balance for the common good could go to greater privacy.

The balances are complex and involve different types of entities and different types of good. To achieve harmony may require compromises. For instance, one kind of change that the government could help implement would be to reduce legal liability for errors in the record. A peaceful balancing of the power between individuals and organizations requires *mutual respect*. Organizations that share record keeping with individuals could be sheltered from legal battles each time an individual finds a discrepancy in the records. Rather the individual and the organization should work together to maintain good records.

To open an insurance company's underwriting files to inspection by applicants and policyholders, for example, gives the company a powerful motive to record only accurate, pertinent information. The purpose of privacy policies is not to encourage applicants and policyholders to look for information in underwriting files that could serve as basis for defamation actions and windfall recoveries. A record keeper that engages in fair privacy practices could have a *limited liability* for accidental errors in information content or practices.

3.11.3 Information Warfare

Given the many concerns about the privacy regulations, what *alternatives* exist? Privacy is not an issue that can be ignored. Legal or political action by entities such as the AMA that might alter the impact of the Privacy Rule might provoke diverse reactions. One particularly intriguing, though also frightening, reaction involves information warfare.

3.11.3.1 What is It?

Information Warfare is all operations conducted to exploit information to gain an advantage over an opponent, and to deny the opponent information which could be used to an advantage. The *taxonomy* of information warfare includes propaganda and espionage (Kopp, 2000):

- propaganda is the use of information to confuse, deceive, mislead, destabilize, and disrupt an opponent, while
- espionage divines secrets from an opponent and prevents the opponent from doing the same.

Other views of information warfare provide further classifications. Shwartau (1996) defines three classes of information warfare:

- Class 1 is personal and includes the study of all sources of information about an individual;
- Class 2 is corporate and concerns business or economic interests; and
- Class 3 is global and affects national interests.

Another taxonomy focuses on the intent of the perpetrator. The *hacker* is deemed to be curious but not intentionally destructive. The cracker intends to do harm. The 'power projectors' want to change the economic or political order.

Professional groups have been formed to wage information war. Typical *roles* in an information warfare group include:

- analyst of existing information,
- software engineer to develop new programs for attacking or protecting information,
- attacker who actually goes into the field and steals or destroys data, and
- camouflager that hides the activities of the information warfare unit.

Information warfare can be serious business.

3.11.3.2 Health Implications

What does information warfare have to do with healthcare? Various scenarios are next sketched of healthcare information warfare.

Under the HPAA privacy rule, covered entities would have to obtain the patient's authorization before the entity could use or disclose the patient's information for marketing purposes. Health insurers, benefits management administrators, and managed care organizations have the greatest ability and economic incentive to use protected health information to determine how to market services to patients. As regulations reduce the access to identified patient information, these organizations will need to look for ways to get de-identified data that supports marketing or will need other strategies for acquiring the information that they feel they need to compete in the marketplace. They will have incentive to acquire information that is hidden from them, and an information conflict situation exists. An organization's marketing and public relations departments often engage in *legitimate espionage* and can be expected to explore the options enabled by the Internet.

While some organizations want private information to support marketing, others might highlight their respect for private information as part of an advertising (or propaganda) campaign. Healthcare providers and payers might compete with one another for clients on the basis of how well they provide privacy and security. Thus a hospital x that had more patient-friendly privacy policies for patients than hospital y might expect on that basis to have more *satisfied customers* than y. Under normal market pressures, this should lead to benefits for x.

The laws or regulations about chains of trust among business associates also create a potential for dissatisfied parties to take action. If healthcare provider x buys medical equipment from supplier y and then x does not renew the contract with y, y might look carefully for evidence of information practices of x that would make x vulnerable to legal prosecution. More generally, one can imagine that an entity x that was in competition with an entity y might support the bringing of harmful evidence about y to the fore. Thus x might directly or indirectly support individuals who had rightful claims against y. Business x might attempt to nurture individual patients of a healthcare provider y to scrutinize y's privacy provisions or x could appeal to the employees of y. *Whistleblowers* are supported by many of the privacy rules. Thus an employee of business y who discovers some privacy violation has protection against reprisal from y.

The various situations under which information is withheld or shared reflect a range of information pressures in the *healthcare terrain*. The new highways and byways of the Internet redefine the healthcare terrain and introduce new pressures. Information traffic jams become increasingly common as the number of speeding travelers increases.

3.11.4 Review Questions

1. What is the AMA position on privacy?
2. How has the government position on the Privacy Rule evolved in 2001?
3. What are the implications of information warfare for health care?
4. The AMA, the AHA, and insurance companies seem to oppose the Privacy Rule. Information systems companies and litigation lawyers seem to favor the Rules. Might one argue that the divisions run along lines of who sees the greatest financial incentive? (Project Question)

3.12 Conclusion

The HIPAA Privacy Rule creates a national baseline for the privacy of healthcare information. The future direction will depend on how healthcare organizations implement the Rule and how patients assume responsibility for their health information.

3.12.1 Summary

The Privacy Rule describes how patient information must be handled in the healthcare system. The Rule both

- brings the patient closer to the process and
- requires healthcare organizations to clearly specify what roles are to manipulate what patient information.

Both of these changes should improve the healthcare process, but in distinct ways. A patient may want *control* of his medical records, and the healthcare organization or others may also want control. Computers raise the stakes because people can do more with information now than in the past.

3.12.1.1 Uses and Disclosures

The Privacy Rule is applicable to all healthcare providers and health plans that engage in electronic transactions. For such covered entities, all information, whether paper-based, electronic, or otherwise must be handled in accord with the Privacy Rule.

Covered entities must post notice about their privacy practices and make clear to patients the rights that patients have. These notices must be posted or distributed in such a way as to come to the attention of all concerned parties upon their initial counter with the provider whenever practical. Furthermore, the covered entity must either obtain from the patient some sort of acknowledgment of having read the Notice of Privacy Practices or must document the patient's refusal to provide such acknowledgment .

Treatment, payment, and healthcare operations are fundamental processes of the healthcare enterprise, and the use of information in those processes is often called 'routine use'. If individually identifiable health information is to be disclosed for other than routine use, then authorization from the patient is required. This authorization must contain the expiration date of the authorization, the signature of the patient, and certain caveats.

A use is internal to an entity, while a disclosure sends protected health information from one entity to another. While uses and disclosures are permitted with authorization, the Privacy Rule asks for non-treatment purposes that the 'minimum necessary' information is shared. While minimum necessary use restricts information flow, two other features of the Rule attempt to facilitate flow. Business associate relationships may be created to facilitate common information support functions between entities without requiring authorizations. Likewise, de-identification is a way for health information to be shared without authorization.

The Minimum Necessary Standard is implemented by developing policies for what *roles* should manipulate what information. Healthcare professionals must have relatively unencumbered access to the medical record for the purpose of delivering care. Other frequent demands on protected health information must be handled through policies in a systematic way. For atypical requests, the entity must review the requests one at a time and decide what use or disclosure of information is the minimum necessary.

Covered entities frequently share information with other entities for certain support purposes. For instance, a health plan may share data with a consulting company that will help the health plan detect patterns in the data. Rather than requiring that the covered entity get an authorization from each patient for such sharing, the Privacy Rule allows the covered entity to enter into a business associate contract with the support company and then share the information.

For certain marketing and research purposes de-identified information is perfectly adequate. If various information, such as the patient name and address, are removed from the record, then the record can be shared without authorization. The Privacy Rule provides an algorithm for the de-identification of health information.

3.12.1.2 Special Opportunities

Individuals may object to some processes and have those processes changed. On the other hand, for some processes the individual has no authority to intervene.

Facility directories have various uses, and healthcare entities by default may include patient information in the directory. However, patients must be given an opportunity to object to such inclusion in the directory, and then the entity must honor the objection.

The Privacy Rule treats information about any medical condition the same as information about any other medical condition with one exception, namely the psychiatric condition. *Psychotherapy notes* may not be routinely shared and require patient authorization for any disclosure.

About a dozen exceptions are given in the Rule when authorization is not required for disclosures. The tone of these exceptions is conveyed in two categories of exception. One category relates to a type of patient and the other category relates to a type of use. Military patients illustrate the exception for type of patient. Military patients lose much of their privacy. The reason is that the national defense requires able-bodied people to handle dangerous weapons, and the commanders of troops are expected to have access to medical records of their troops. The exception for type of use is illustrated with research. Research serves a public good. If researchers needed to get authorization for every patient record that the researcher might see, then research might be slowed. So the Rule allows researchers to propose to their institution permission to see records and to be granted this permission by their institution.

Marketing cannot be done with information unless the patient authorizes the use of information for that purpose. However, the Privacy Rule allows healthcare entities to take various marketing-like liberties with protected health information.

The Privacy Rule gives patients important new rights. The patient has the right to

- *access* the patient record. The entity cannot charge for the effort of processing the request for access or for finding the information but only for the copying of the information. The individual can request the format in which the information is to be delivered and where it is delivered.
- *amend* the record when the patient believes important information is missing from the record. If the entity chooses to deny the request, then the individual can request a review of the denial. If the review upholds the denial, the individual can request that the record permanently show the request for an amendment.
- see an *accounting* of what disclosures were made.

In all cases the Rule requires the entity to respond to the individual quickly.

3.12.1.3 Administration

For an entity to comply with the Privacy Rule requires in order:

- sharing the vision,
- developing the objectives and plans,
- implementing the plans, and
- continuously monitoring the progress towards the objectives.

The Privacy Rule does not seek to straightjacket entities but rather sketches broad objectives. Each entity can then refine those objectives to its situation.

Entities face several *administrative requirements*. They must designate a privacy officer, document their privacy policies, train their staff on privacy, safeguard information, be sensitive to complaints from staff and patients about privacy matters, and impose sanctions on violators of the privacy policy. DHHS provides details on each of these requirements. For instance,

- training must occur for each and every member of the entity's workforce no later than the compliance date and
- whenever the entity's privacy policy changes the members of the workforce whose functions are affected by the change must be retrained.

Safeguards must be imposed that will be further delineated in the Security Final Rule. For the diversity of requirements, the challenge on the entity is to meet them in a way that integrates smoothly with current practices and that improves the quality of the entity services.

HIPAA imposes fines on violators of the Privacy Rule. DHHS enforces the Privacy Rule by both actively reviewing entity behavior and by openly soliciting any and all complaints from patients or staff. Through business associate agreements DHHS stimulates enforcement of privacy by encouraging one entity to help monitor another.

3.12.1.4 Other Regulations

Various Federal privacy laws or regulations provide a context for HIPAA. The Privacy Act of 1974 applies only to federal agencies but is broad in its mandate. Unfortunately, it has been only loosely interpreted and enforced. HIPAA strengthens the Privacy Act. Medicaid privacy rules are stricter than HIPAA. All in all, the relationship between HIPAA and other federal activities as regards privacy suggests a simple harmony – either the existing activity is strengthened or the existing activity will continue as is because it is already stronger than HIPAA.

State privacy laws are another story. State health privacy statutes cover a broad range of entities and, not surprisingly, are both weak and strong. In terms of broad consumer protections, one can identify many gaps in state statutes, such as:

- a limited right for a patient to access his or her own medical record;
- little ability for patients to limit disclosure of their medical records; and
- little recourse when the laws are violated.

On the other hand, state laws enacted in response to a particular public concern or a public health threat are often strong, detailed, and aimed at the state's unique experiences with its citizens. Also when the states legislate by entity, they address the information needs of particular entities. An HMO, for example, may have different needs than a family planning clinic.

The approach of states to privacy has tended to be a *case-by-case* approach. For a certain kind of information in the hands of a certain kind of organization a certain law or rule has been created as the situation seemed to demand it. Generally the state laws have not taken a broad overview of privacy issues or a patient-centric view. HIPAA does just the opposite -- HIPAA takes a broad, patient-centric view.

One challenge to applying HIPAA is that state laws may preempt HIPAA whenever they are stronger than HIPAA. However, the definitions of 'law' and 'stronger' are not obvious:

- State laws may often be common law and thus only operationally defined in court cases. So knowing the law requires essentially practicing it.
- The notion of 'stronger' privacy is also subject to interpretation. What one person sees as stronger privacy, another might see as weaker privacy. The Privacy Rule says that stronger means that the patient has more control.

Societies for healthcare professionals will typically have some policy on privacy for the membership. However, these policies are typically much weaker than HIPAA and tend not to give patients control of patient information.

The Joint Commission on Accreditation of Healthcare Operations (JCAHO) has certification guidelines that incorporate privacy. JCAHO intends to continually update these guidelines to conform to the federal legislation and rules. Healthcare organizations needing to be certified by JCAHO will be obliged to follow the HIPAA Privacy Rule.

The European Union has a broader and more customer-centric approach to privacy than the United States. All European businesses sending information outside Europe must comply with strict privacy regulations. American organizations with European operations that want to send information to the US have a problem. This problem has been temporarily resolved by a Safe Harbor agreement between the European Union and the United States.

3.12.1.5 Impact

The market has failed to give patients adequate control over their own information. This *market failure* is attributable to the relatively weak position of any given patient relative to the healthcare organization. The patient has difficulty to know what the privacy policies are or how the organization is following the policy.

DHHS made an extensive analysis of the cost of implementing the Privacy Rule over a 10-year period. The total cost is estimated to be $18 billion. The two largest items are the employment of a 'Privacy Official' and the implementation of the 'Minimum Necessary Use' regulation with each costing about $6 billion over the first 10 years.

To perform its cost estimates DHHS determined the roles that would have to perform the work, how many hours they would take, and what the hourly wages were. The analysis is one starting point for *long-term planning* of resources and strategies for healthcare entities.

Different parties see the monetary costs of implementing the HIPAA Privacy Rule differently. The Nolan Company under a contract from a health plan estimates costs at *$43 billion* in the first 5 years. Still the costs relative to total healthcare costs are small.

Reaction to the Privacy Rule has been intense and extreme. The privacy framework has been attacked as

- too weak by some patient advocates and
- too strong by some providers and payers.

The American Medical Association (AMA) sees the Privacy Rule as imposing an excessive responsibility on physicians. The AMA also implies that the patient-physician relation involves the transfer of authority over patient information to the physician. Thus the AMA objects to HIPAA both for simple cost reasons but also for philosophical or political reasons.

The tension over the Privacy Rule could lead to *information warfare*. Information warfare is conducted to exploit information to gain an advantage over an opponent. Classic examples of information warfare are propaganda and espionage. While relationships among healthcare organizations and between them and patients are congenial, information warfare among these participants could occur. One party might attempt to discredit another by revealing flaws in the privacy practices of the other.

3.12.2 Directions

The Privacy Rule limits the circumstances in which an individual's health information can be used. The use of health information is made relatively easy for healthcare purposes and more difficult for purposes other than healthcare. The Privacy Rule is based on five principles:

- Boundaries - An individual's healthcare information should be used for health purposes and only those purposes, subject to a few carefully defined exceptions.
- Security - Organizations ought to protect health information against misuse.
- Accountability - Those who misuse personal health information should be punished, and those who are harmed by its misuse should have legal recourse.
- Public Responsibility - Federal law should identify those limited arenas in which public responsibilities warrant authorization of access to medical information, and should allow but constrain uses of information in those contexts.
- Consumer Control - Patients should be able to see what is in their records, get a copy, correct errors, and find out who else has seen them.

On the first four principles there is consensus in the large. Yes, boundaries should be secure. Yes, those who are responsible for boundaries and security should be held accountable. Yes, exceptions occur when the public good is at stake.

Much quibbling occurs over the specifics of those first four principles. However, the regulations are not trying to be precise about what has to be done. Small entities may have different mechanisms from large entities. What exactly is done is less important than that the organization demonstrate in its operations that it works to the principles. This is sound business practice anyhow – the essence of a *quality organization* is that it makes clear its principles and consistently works by them.

Saying that achieving the first four principles is a simple matter of working towards reasonable objectives belies the full story. In particular, there is controversy about policing of business associates. Most agree that business associates should respect the principles of privacy. But who will be responsible for seeing that business associates show this respect? HIPAA puts this burden on the covered entities, and the covered entities object. The regulations should apply directly to the business associates, but HIPAA does not give DHHS the authority to regulate the business associates directly.

The showstopper is the fifth principle of 'consumer control'. The principle of 'consumer control' is not part of the tradition of American healthcare. Also, giving the consumer more control will require expensive modifications to administrative processes in the healthcare entities. Thus some healthcare entities are fighting this sea change in the way information is controlled. However, the financial costs are only the tip of the iceberg. What bothers some is the shift in the power base.

The state privacy laws are so complex and inconsistent that the layperson can hardly be expected to understand them. Yet, without federal intervention, the consumer is largely reliant on state privacy laws. The consumer is the one most disadvantaged by the status quo. An individual patient in the need of healthcare is in a weak position to disagree with an information practice of a healthcare organization and to identify from the *maze of state regulations* what, if any, might be on the patient's side.

One might recall the famous lounge song "Something's Gotta Give" (Mercer, 2000):

> When an irresistible force such as you
> Meets an old immovable object like me,
> You can bet as sure as you live,
> Something's gotta give

Patients and the healthcare industry are face-to-face over privacy. Given that the patient and the doctor are in a symbiotic relationship, a win-win resolution to the privacy-power contest should be expected. However, both the patient and healthcare professional may find themselves moving through uncharted territory as they share the power of information.

4 Security

Learning Objectives

- Describe a model of security in terms of real-world policy, computer models, and technical mechanisms.
- Construct a life cycle of compliance in terms of awareness, gap analysis, risk analysis, implementation, training, and audit.
- Construct access policies and compare them to those developed by other organizations.
- Develop a role-based access control model that indicates several roles and their permissions for a healthcare entity.
- Distinguish authentication, authorization, and audit.
- Design a system for encrypting communications for a healthcare entity that includes a public key infrastructure.

The Notice of Proposed Rule Making (NPRM) for 'Security and Electronic Signatures' was published in August 1998. The NPRM details the system and administrative requirements that a covered entity must meet in order to assure that health information is safe from people without authorization for its access. By contrast, the Privacy Rule describes the requirements that govern the circumstances under which protected health information must be used or disclosed with and without patient involvement and when a patient may have access to his or her protected health information.

4.1 Introduction

Main Points

- Security of healthcare information systems is substandard.
- The solution to the problem is not the acquisition of a new technology but the improvement of an organization's workflow.
- A security framework shows that human policies come first and then drive a computer policy that in turn uses technical mechanisms.
- The computer policies emphasize confidentiality, integrity, and availability.
- The Security NPRM applies to all healthcare providers, plans, and clearinghouses that use information in electronic form and will demand compliance 2 years after having been published as a final rule.
- The cost of complying with these rules is hard to estimate but may involve major changes to an organization and thus could be very costly to implement, although they would hopefully lead to more effective and efficient organizations in the long run.

HIPAA mandates that healthcare organizations secure health information from the lowest layer of data transport through the administrative processes (CPRI, 1996). This chapter examines DHHS's proposed rule for security.

4.1.1 The Problem

Security is inadequate. How many hospital-based organizations have developed at least minimally adequate health information security structures to date? In the private sector such information is hard to reliably obtain. If a hospital knows that its information systems are easily breached by hackers, then will the hospital announce that information to the public? Probably not. Experts estimate that probably 10% or fewer of private healthcare organizations have adequate security – in other words, 90% or more have *inadequate security* (Hagland, 1998).

The federal government is sometimes more forthcoming with its own internal analyses than the private sector is. The Government Accounting Office under the direction of the U.S. Congress has performed various security audits of federal government agencies. In a report to the U.S. Congress from the *Government Accounting Office* the title tells the story (GAO, 2000): "Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies". An audit of the *Veterans Health Administration* (VHA) speaks more precisely to the problems with healthcare information. A September 2000 report about the VHA contains the following (GAO, 2000b):

> Access control and service continuity problems are placing financial and sensitive veteran medical information at risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, and/or destruction. …, we found additional access control and service continuity problems at these facilities and serious weaknesses at the VA Maryland Healthcare System. Similar security problems also persist throughout VHA and the department. One reason for the VA's continuing information system control problems is that it had not established an effective, integrated computer security management program throughout the department. …, it remains important for VA to develop detailed guidance to ensure that the key program elements we highlighted in our October 1999 report — periodically assessing risk, monitoring system and user access activity, and evaluating the effectiveness of information system controls—are fully addressed and implemented consistently across the department. Consequently, we are reaffirming our October 1999 recommendation for VA to develop detailed guidance in these areas. … Moreover, VA's ability to continue to develop and implement an effective computer security management program is in jeopardy because VHA had not yet ….

Computerized information is integral to the fabric of the healthcare enterprise. Yet healthcare computing systems are not secure enough for their crucial roles.

4.1.2 Workflow

Security is dependability. Security is something that secures, and secure means *dependable*. Everyone wants dependable healthcare information systems. The work required to achieve this security is intimately connected to many other operations of the organization. Maintaining a dependable information system requires that

- each person knows what information he is to see and what he is to change and
- the system not allow him to see or change anything else.

Security is running the organization. To satisfy these requirements an organization must manage its *workflow*. Yet, security is often viewed as a technical issue, such as of a firewall in the computer network or a token card used to gain access to a computer terminal. The truth of security is far from this technical solution and closer to the essential concerns of running the organization.

Policy is more important than technology. The following extracts from an interview illustrate the importance of *policy over technology*. The interviewees are Douglas Fieldhouse and Albert Shar of Technology Services, University of Pennsylvania Health System, Philadelphia. The interviewer Mark Hagland (1998) asked "what tools offer the most promise for the future?" Fieldhouse replied:

> There are lots of great tools out there. Unfortunately, most people don't know what they need yet. The firewall you decide you require really depends on your own security policy; it's an instrument of your policy. If you don't have a current, up-to-date security policy, you're not going to know what products you need. A lot of my peers are in similar situations. We had to get something, and the policies and procedures were not forthcoming, and so we just went out and got the best, most flexible products out there we could. Unfortunately, we're working reactively.

Shar added:

> Let me take an even more cynical view. The firewall technology is one more piece of technology that can really be exceptional if used properly. This should be used based on the policy that's determined. But what's happening is, just because we have a firewall, people end up believing that that's equivalent to a security policy, which it's not. Secondly, it's an abdication of responsibility, because the technologists -- and that's what we are -- essentially determine the policy de facto, and frankly without the input in terms of what the business needs are. I see that in some cases, some of the things we've done have actually had a negative impact on security. For example, because we had a firewall in our organization, and people couldn't get to electronic information that needed to be available, it was relatively easy for a doctor to get a modem and hook up to the medical record system and go around the system. And that was motivated by the desire to do better medicine. In other words, whenever we're not responsive to a business need in terms of the technology that we're implementing, it has sort of the opposite effect of what we're trying to achieve.

Data only for the right people. Computer security policies must reflect the real-world policies of the organization. One computer security policy begins with a decomposition of the data in the medical record and the staff that maintain the record (Pangalos, 1995):

- The data are divided into administrative information, non-medical historical information, social information, personal demographic information, non-personal demographic information, insurance information, billing information, diagnosis, examination request, examination result, treatment data, and use of special materials.
- The staff are divided into head doctor, responsible doctor, on-duty doctor, head nurse, nurse, paramedical staff, registration staff, and financial staff.

Using these categorizations of data and staff, the computer security policy proceeds through an elaborate mapping of staff to data for operations of selecting, inserting, updating, and deleting data. One can readily see that such computer security policies require an intricate model of how the healthcare organization itself functions. A workflow management system would support the scheduling of operations by people on data. Such a system would be the essential ingredient of a secure system in which viewing or modifying data is only done at the *right time by the right people*.

Security is not Y2K. Yet, many healthcare organizations are likening the security problem to the Y2K problem and asking the Y2k team to solve the security problem. The security problem is not like the Y2K problem. The *Y2K problem* was essentially a technical problem. The security problem is essentially a policy and management problem. A healthcare organization's security problems are more administrative than technical.

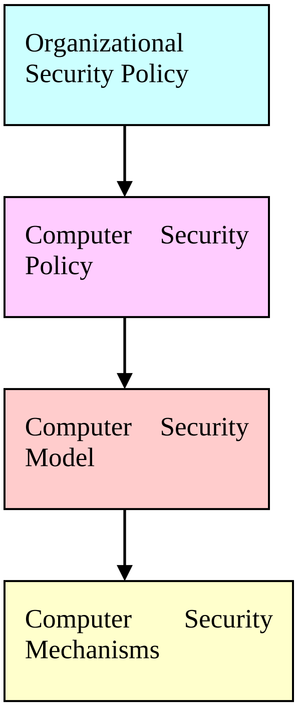


Figure “Security Policy”: The diagram shows the progression from an organizational policy, to a computer policy, to a computer model, to mechanisms.

4.1.3 Security Framework

Tasks must be authorized. The National Research Council defined security (1991) as:

> the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

To achieve information system security involves activity at multiple levels of which one breakdown gives (see Figure “Security Policy”):

- organizational policy,
- computer security policy,
- computer security model, and
- computer security mechanisms.

The goals of an organization combined with its environmental circumstance dictate the organization’s security policy. This *organizational policy* is a set of laws, rules, and practices that regulate how an organization manages, protects, and distributes resources to achieve its security objectives. If an organization has no explicit security policy, then policy assumptions guide its actions.

Computers support people. A computer security policy must faithfully represent the organizational security policy. It must also consider threats that are not identified per se in the organizational policy but are intrinsic to computer operations, such as the threat of a computer virus. A *computer security policy* is expressed in a natural language such as English. The organization should make the computer security policy as precise as possible. Since natural language in complex cases is often ambiguous, organizations may designate who is to interpret the policy.

A computer security model restates the computer security policy in a formal or mathematical way and thus reduces the ambiguity. Such a model guides the design of the security aspects of computing systems. The designers need an unambiguous statement of what the policy means, and the model provides this.

Mechanisms implement models. Computer *security mechanisms* provide the trusted computing base and extensively use cryptography. Cryptography allows encoding of messages so that people who see the message cannot understand it unless they have an appropriate key. Sharing these keys becomes a complex matter which itself can lead to organizational policy.

4.1.4 Computer Security Policies

Computer security policies are categorized in various ways of which one popular way uses the following three concepts (System, 1991):

- *confidentiality*: controlling who gets to read information,
- *integrity*: assuring that information is changed only in a specified and authorized manner, and
- *availability*: assuring that authorized users have continued access to information and resources.

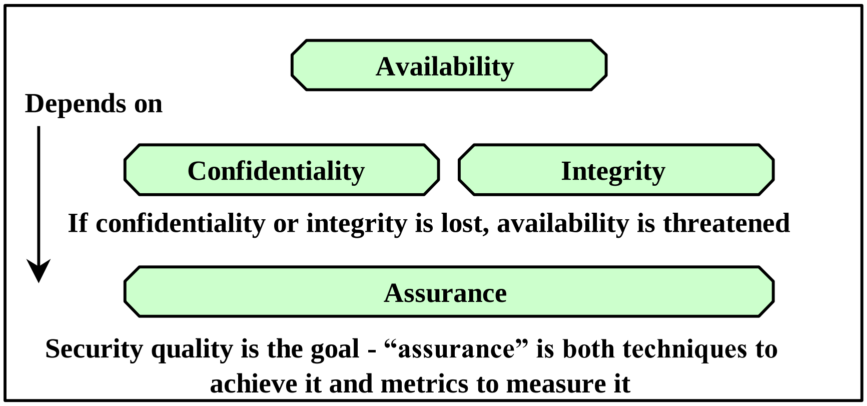

Availability
Depends on
Confidentiality
Integrity
If confidentiality or integrity is lost, availability is threatened
Assurance
Security quality is the goal - "assurance" is both techniques to achieve it and metrics to measure it

Figure "Security Relationships"**:** Availability depends on confidentiality and integrity and together these support the assurance of quality (Stoneburner, 2000).

Availability depends on confidentiality and integrity (see Figure "Security Relationships").

Confidentiality receives much attention. The most fully developed policies are those that have been developed to ensure confidentiality. The Department of Defense computer security policy is based on confidentiality levels. Every piece of information has a security level. A person is cleared to a particular security level and can see information only at that, or a lower, level.

Integrity deserves more attention. Integrity policies have not been studied as carefully as confidentiality policies. Separation of duties in the changing of computer information is an example of an integrity policy. If one person can enter an order for a certain radiation to be administered to a patient, then a different person may be required to approve the order.

Availability is little understood. What causes a system to become unavailable and how can this be prevented? People do not understand these disasters, but can address recovering from a disaster. A contingency policy is the extent to which most organizations currently have an availability policy. These contingency policies typically specify backup procedures and schedules so that an information system can be restored after a catastrophic loss. The main HIPAA security requirement as regards availability is indeed a data backup or contingency policy.

Computer security concepts are wide-ranging. The description of confidentiality, integrity, and availability is far from an exhaustive accounting of the major concepts of computer security policy. Different people for different purposes view computer security policy differently. For example, two important concepts that are orthogonal to the three just described are:

- *resource control*: controlling who has access to computing resources exclusive of information and
- *accountability*: knowing who has had access to information resources.

Resource control includes the physical access to the components of the information system. Accountability is supported by audit trails, and, in turn, supports confidentiality, integrity, and availability.

4.1.5 Applicability and Schedule

The regulation covers providers, plans, and clearinghouses. Collectively, these entities are called '*covered entities*'. Within covered entities, HIPAA's security provisions apply to all individually identifiable health information that is electronically maintained or used in an electronic transmission.

Even the one physician office, insulated from HIPAA's transaction requirements by paper forms and stamps and envelopes, is subject to HIPAA's security requirements, if

- bills are printed from a practice management system,
- charts are transcribed and stored in a word processor, or
- lab results are sent by modem to a printer at the back of the office.

No distinction is made between internal entity communication and communication external to the entity.

Any medium counts. Electronic information on any medium, including magnetic tape, disk, or compact disc, is covered by the regulations. Transmissions are covered for any network, whether Internet, leased lines, dial-up lines, private networks, or any other kind.

Electronic signatures are welcome. However, the DHHS regulation does not mandate the use of electronic signatures with any specific transaction. Instead, the regulation proposes that whenever an *electronic signature* is required for an electronic transaction by law, regulation, or contract, the signature must meet the standard. Use of this standard would satisfy any Federal or State requirement for a signature, either electronic or on paper.

DHHS consulted many organizations. In the development of the security standard, DHHS was required to consult with certain organizations but went well beyond the required list. Those consulted included, but were not limited to, the:

- National Committee on Vital and Health Statistics,
- Accredited Standards Committee X12,
- American Society for Testing and Materials,
- Association for Electronic Healthcare Transactions, and
- Health Level Seven.

Simultaneously the government welcomed input from any and all individuals and organizations. This extensive *consensus building process* proved time consuming but hopefully leads to widely accepted conclusions.

Organizations have two years to comply. Covered entities are generally required to comply with the requirements no later than *two years* after publication of the final rule. The exception is that each small health plan would have three years after the date of publication of the final rule.

4.1.6 Impact

Penalties apply. HIPAA does not per se specify penalties for security violations. However, penalties for violations of *privacy* are severe and include a 10-year prison term and a $500,000 fine for exploitation of confidential information. Security and privacy are intimately linked, as respecting privacy is best done when security policies are top notch.

Costs are not known. Providers, health plans, and clearinghouses that transmit or store data electronically may have already implemented security measures. However, little information is available regarding the extent to which providers', plans', and clearinghouses' current security practices are deficient. Moreover, some security solutions are almost cost-free to implement (e.g., reminding employees not to post passwords on their monitors), while others are not. Healthcare providers that currently submit healthcare information on paper but archive records electronically should have very little extra cost to ensure that their existing electronic systems conform to security requirements for maintaining health information. Large organizations with extensive computer operations may face high costs in becoming adequately secure. DHSS offers *no estimate of the costs* of complying with HIPAA security regulations.

Implementation strategies vary. Covered entities will have many choices regarding how they will implement security. Some may choose to assess security using in-house staff, while others will utilize consultants. Practice management software vendors may also provide security consultation services to their customers. Entities may also choose to implement security measures that require hardware or software purchases at the time they do routine equipment upgrades.

4.1.7 Preview

No recognized, existing single standard integrates all the components of security that must be in place as defined in HIPAA, and thus a new standard is needed. Therefore, DHHS has proposed a new security standard (DHHS, 1998e). The security standard specifies the requirements of a healthcare entity to safeguard the integrity, confidentiality, and availability of its electronic data. The standard also describes the implementation features that satisfy each requirement.

Rules are grouped. The Proposed Security Rule specifies several dozen specific rules that must be met. The rules are grouped into 4 categories of which 3 are:

- *Administrative procedures* are documented, formal practices to manage the selection and execution of security measures to protect data and the conduct of personnel in relation to the protection of data.
- *Technical security services* control and monitor information access.
- *Technical security mechanisms* prevent unauthorized access to data that is transmitted over a communications network.

The categories could be labeled real-world security policy, computer security policy, and computer security mechanisms in a one-to-one mapping to administration, technical services, and technical mechanisms, respectively (Summers, 1997).

Physical safeguards are a 4th category. Physical safeguards protect physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Physical safeguards also cover the use of locks, keys, and administrative measures used to control physical access to computer systems and facilities. This book focuses on what DHHS calls administrative procedures, technical security services, and technical security mechanisms and pays less attention to *physical safeguards*.

In the next sections, the life cycle of security compliance is presented, and then the proposed regulations are rendered in three major sections called:

- *real-world policy*,
- *computer models*, and
- technical mechanisms.

The regulations are described with rich background, principles, and examples.

4.1.8 Review Questions

1. What did the Government Accounting Office audit on security reveal?
2. Why is workflow more important than technology for security?
3. Put a security framework along the spectrum from technical mechanisms to computer models to human policies.
4. What is the difference between confidentiality, integrity, and availability in a computer security policy?
5. To what information and activities does HIPAA's security regulation apply?
6. Why are the costs for implementing security not clear?

4.2 Life Cycle

Main Points

- A gap analysis determines where an organization needs what kinds of changes to become compliant.
- Risk analysis considers the various threats to security and then suggests the remedies that are most cost-effective.
- An example of risk analysis shows the straightforward but exhaustive effort required to delineate and assess the factors.
- An information security officer should be appointed to administer the security program.
- Other staff throughout the organization also should contribute to the security effort.
- Training will cover some core concepts for all people and then be specialized depending on the role of the person.
- Quality control is about performing consistently with objectives and is what the security regulations ask organizations to do.
- Compliance to security regulations requires working consistently to security objectives.

Are people aware? Do they know where they stand and where they need to go? An awareness campaign and a gap analysis start the security policy development.

4.2.1 Awareness

Who starts the HIPAA ball rolling in any given organization? Every organization must have role(s) that care for security. In a small organization the role might be played by the office manager. A large organization might have dozens of specialist *roles* focused on security. In any case, the person or persons filling the role(s) most related to security might naturally be the first to help the organization come to grip with the security requirements of HIPAA.

Awareness is needed. The people in security roles should be on the alert about important legislation that impacts their performance and thus acquire a basic *awareness* of HIPAA as part of their routine. The government has publications on the topic, vendors offer various kinds of training, and workshops or conferences are offered on the subject. The security staff should be acquiring the information that allows them to act in an aware way.

The harder part of the awareness task addresses senior management – those not primarily responsible for security but in control of the resources that are needed to respond adequately to the HIPAA requirements. Has the organization committed nearly as much resource (both people and money) to security as it ought to commit? The requirements of HIPAA and evidence for inadequate security are ammunition to stimulate awareness in the *senior management*. A written report followed by a presentation may help provide awareness. Awareness and then action are part of an iterative process. As the effort broadens and deepens, more people need to get involved and each time people need various kinds of awareness.

4.2.2 Gap Analysis

An early challenge is to know the current status of the security protection within the organization – the baseline. Then this *baseline* must be compared to the HIPAA requirements to determine the gap. If the gap is large, then the new resources needed are large.

4.2.2.1 Baseline

How is the baseline assessed? The baseline assessment *inventories* an organization's current security environment with respect to policies, processes, and technology. The scope will drive how this should be done. If the assessment is narrowly tailored to HIPAA, the baseline assessment design can be driven by the regulatory framework. If however, an organization wants this to be integrated in its business processes, an organization might be better served to design the baseline to capture information in keeping with its lines of business. Capturing the baseline information along lines of business, as well as for differing information technology environments, will support the appropriate level of detail that an organization will need for it's gap analysis.

What needs to be reviewed? Defining which security components can be reviewed once because they are standardized throughout an organization will help *avoid duplicate analysis*. For example, the Wide Area Network does not need to be assessed in each part of the organization, since it should be the same across parts. However, capturing varying practices distinct from system capabilities is important. For example, standard password assignment procedures do not mean that adherence is consistent in different parts of the organization.

DHHS wants an inventory. DHHS requires a Security Configuration Management Inventory that includes documentation of hardware and software assets. This requirement can be satisfied during the *baseline assessmen*t. An organization will need to understand this inventory in order to know its potential vulnerabilities and determine what existing security capabilities reside in the assets. Using a Y2K asset inventory as a starting point might save time and resources. Organizations then need to expand the inventory to incorporate HIPAA subject applications and information systems that may not have been included in the Y2K effort.

4.2.2.2 Implementation

The organization should qualitatively rate its readiness. Qualitative criteria should be developed to evaluate the current environment for each of the security standards (Kooney, et al, 2000). The measurement criteria suggested as part of the gap analysis could include rankings of current readiness weighed against HIPAA requirements. A simple *five-point scale* could be used that identifies the organization's status relative to each requirement as follows:

1. No identified process or control,
2. Informal or partial process or control,
3. Process or controls implemented for many required HIPAA elements,
4. Process or controls fully implemented for all required HIPAA elements, or
5. Process or controls exceed required HIPAA elements.

Every part of the organization may be included in the gap analysis, even if current security processes and controls vary widely or do not exist at all in some parts of the organization. Example parts include:

- remote sites such as clinics, physician offices, home health agencies,
- smaller lines of business or regional headquarters locations, and
- home-based workers, such as medical transcriptionists.

Gap details need to be captured. For instance, saying an organization has only partial or informal controls is not *sufficient detail* to help determine how the gap would ultimately be filled. Instead, a detailed statement is necessary, like "the mainframe environment has the necessary control, but the following remote sites are inadequate because of certain reasons".

The gap analysis needs to involve the entire organization. Participants in the gap analysis should represent the entire organization and will need to include representatives from all lines of business and all support offices. Key support offices include legal, internal audit, information technology, training, human resources, facilities management, and risk management. Typically, many of these participants will already be part of the *cross-functional security team*.

4.2.2.3 GAO Manual

GAO provides an audit manual. The U.S. Government Accounting Office (GAO) published a Federal Information System Controls Audit Manual in 1999 that is 275 pages long. The document details how to do an information systems audit. Such an *audit* is similar to a *gap analysis* where the audit manual sets the standards of the performance to be expected and directs the auditor in testing the system to find how far it is from the standard. The GAO Manual could apply to any organization, including healthcare organizations. The manual begins with these two sentences (GAO, 1999):

> Federal agencies … and the public rely on computer-based information systems to carry out agency programs …. The methodology outlined in this manual provides guidance to auditors in evaluating internal controls over the integrity, confidentiality, and availability of data maintained in these systems.

Auditors are asked to engage in a 3-step process of: *planning*, *testing*, and *reporting*:

- During the planning phase, the auditor gains an understanding of the entity's computer-related operations and controls and related risks. In view of these risks, the auditor tentatively concludes which controls are likely to be effective. The auditor then plans to confirm that the seemingly correct controls are indeed working. Where controls seem to be missing, the auditor must plan further explorations as to the vulnerabilities and possible solutions.
- During the testing phase, the auditor first tests general controls through observation, inquiry, inspection, and other tests. If there are serious problems with the general controls, then the audit of application-specific controls only continues when many employees may be using an application and may be likely to abuse its controls.
- The report is vital to corrective action. The report should discuss each *weakness* in terms of the related criteria, the condition identified, the cause of the weakness, and the actual or potential impact on the entity and on those who rely on the entity's data. The auditors should prepare one *report for management* that avoids technical details but emphasizes managerial issues. Another *report for technical staff* should provide precise causes of the weaknesses.

The GAO Manual provides criteria that the auditor must address . The major criteria fall into 6 categories:

- entity-wide security program planning and management,
- access control,
- application software development,
- system software,
- segregation of duties, and
- service continuity.

Within each category are several critical elements The 5 critical elements for the category 'entity-wide security program planning and management' are provided here by way of example:

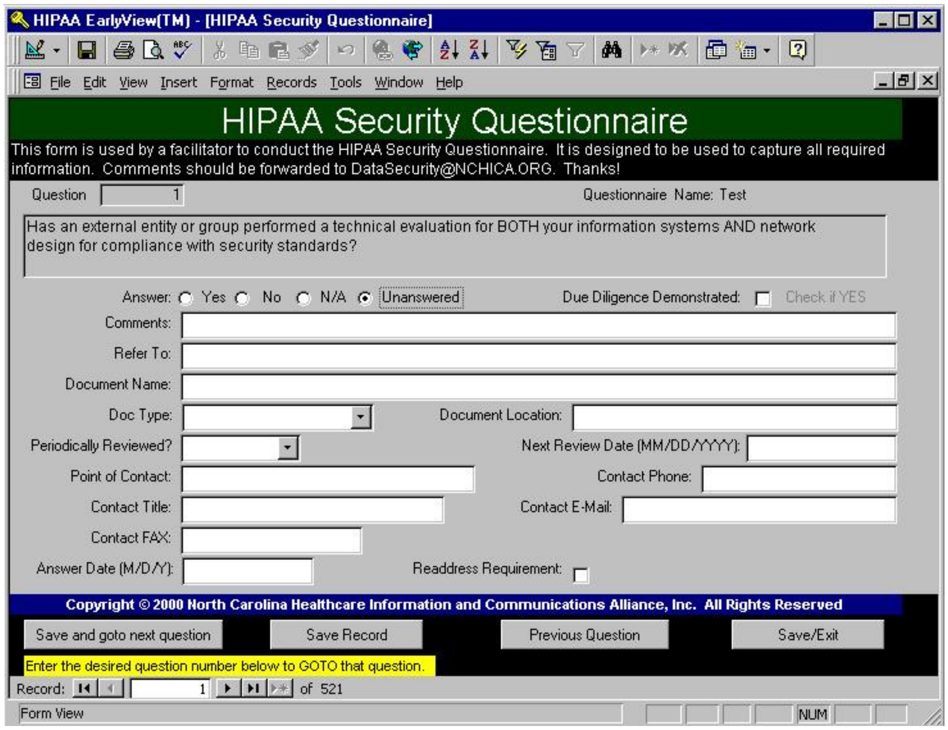
- periodically assess risks,
- document an entity-wide security program,
- establish a security management structure and clearly assign security responsibilities,
- implement effective security-related personnel policies, and
- monitor the security program's effectiveness and make changes as needed.

Step-by-step instructions are given. For every 'critical element' several 'control activities' are given and for each control activity, precise steps or 'control techniques' are given. As an arbitrary example, one 'control activity' is 'control personnel activities through formal operating procedures and supervision and review'. The GAO Manual lists several 'control activities' of that critical element of which one is 'active supervision and review are provided'. Four *control techniques* are given:

- Personnel are provided adequate supervision and review, including each shift for computer operations.
- All operator activities on the computer system are recorded on an automated history log.
- Supervisors routinely review the history log and investigate any abnormalities.
- System setup is monitored and performed by authorized personnel. Parameters are set during the personnel program load in accordance with established procedures.

Audit procedures are then indicated for these 'control techniques' as follows:

- Interview supervisors and personnel.
- Observe processing activities.



HIPAA EarlyView(TM) - [HIPAA Security Questionnaire]

HIPAA Security Questionnaire

This form is used by a facilitator to conduct the HIPAA Security Questionnaire. It is designed to be used to capture all required information. Comments should be forwarded to DataSecurity@NCHICA.ORG. Thanks!

Question 1 Questionnaire Name: Test

Has an external entity or group performed a technical evaluation for BOTH your information systems AND network design for compliance with security standards?

Answer: ○ Yes ○ No ○ N/A ● Unanswered Due Diligence Demonstrated: □ Check if YES

Comments:

Refer To:

Document Name:

Doc Type: Document Location:

Periodically Reviewed? Next Review Date (MM/DD/YYYY):

Point of Contact: Contact Phone:

Contact Title: Contact E-Mail:

Contact FAX:

Answer Date (M/D/Y): Readdress Requirement: □

Copyright © 2000 North Carolina Healthcare Information and Communications Alliance, Inc. All Rights Reserved

Enter the desired question number below to GOTO that question.

Record: 1 of 521

Figure "HIPAA EarlyView". This screen image shows one of the 500 forms in the risk assessment. This particular form is based on the question "Has an external entity performed a technical evaluation for both the information systems and network design for compliance with security standards?". The form asks for documentation of the answer, a point of contact, a next date for evaluation, and other such information useful for risk containment. The image comes http://www.nchica.org/activities/EarlyView/large_screen_shot.htm.

- Review history log reports for signatures indicating supervisory review.
- Determine who is authorized to perform the initial program load for the system, what steps are followed, and what controls are in place to monitor console activity during the process. Determine whether operators override the IPL parameters.

From such detailed instructions, auditors can consistently perform *reliable audits* across different entities.

The GAO Manual provides a greater emphasis on the *underlying software* of the entity than does the HIPAA security regulation but otherwise the general approaches are the same. HIPAA security addresses chain of trust agreements that are not addressed in the GAO Manual. While the details of the GAO Manual are not specific to healthcare organizations and not identical to the concerns of DHHS, the GAO Manual is a starting point for an organization that wants to develop its own audit manuals for HIPAA security.

4.2.2.4 EarlyView Tool

HIPAA EarlyView is for HIPAA gap analysis. The *North Carolina Healthcare Information and Communications Alliance* (NCHICA) produced a tool called 'HIPAA EarlyView Self-Evaluation Tool' for gap analysis. *NCHICA* is a non-profit, volunteer organization whose members are healthcare providers, payers, state government, information technology vendors, law firms, and others in North Carolina who want to advance the cause of information technology in healthcare in North Carolina. The members decided to develop a gap analysis tool for HIPAA Security and began by studying the Security NPRM. Teams of volunteers were assigned to develop questions according to each of five sections of the proposed rule. Each team produced about 100 questions. A total of 521 questions were produced for Version 1.0 of *HIPAA EarlyView* (NCHICA, 2000).

The first 5 questions are about *Certification* and follow:

1. Has an external entity or group performed a technical evaluation for both your information system and network design for compliance with security standards?
2. Does your organization have an internal audit group that performs technical evaluations for both information systems and network design for compliance with security standards?
3. Does your organization maintain a technical evaluation history for both information systems and networks?
4. Does your organization require that both information systems and networks are reviewed after any additions or significant modifications to design?
5. Does your organization document all steps taken to ensure and maintain security compliance?

The next 4 questions are about *Chain of Trust* and follow:

6. Does your organization require that a chain of trust agreement be signed with all third parties that process protected health information?
7. Does your organization explicitly state requirements for ensuring confidentiality and integrity of data in any chain of trust agreements?
8. Does your organization explicitly state requirements for availability of data in all chain of trust agreements?
9. Does your organization maintain the right to audit the security measures of third parties who process protected health information?

The questions follow relatively directly from the implementation requirements of the *Security NPRM*. The strength of NCHICA's questions is that a substantial number of organizations agreed to the 521 questions.

Questions are augmented with forms. For each question, there is an associated form that the person completing the form is asked to complete. The *form* asks the same information for each of the 521 questions and is basically asking for pointers to documentation that supports the answer to the question. The questions on the form include one multiple-choice question and about a dozen fill-in-the-blank questions. Some of the questions follow:

- Document type?
- Document location?
- Point of contact?
- Contact phone?
- Periodically reviewed? If yes, when is the next review?

With the answers to these questions, the organization knows where to go for more information related to the question.

The survey connects to a database. The 'HIPAA EarlyView' tool includes a piece of software that connects to Microsoft Access. For $150 a person can buy this piece of software and then enter answers to the 521 questions into a local *Microsoft Access database*. The tool provides several reports on the answers so that an organization can review its status. An example of a data entry screen from 'HIPAA EarlyView' shows the dozen questions in a structured interface for one of the 521 questions (see Figure "HIPAA EarlyView").

EarlyView is being refined. The tool is intended for health plans, providers, and clearinghouses and has been purchased by a substantial number of such organizations. However, many variants of the questions and tool could be developed. In fact, NCHICA has licensed the tool to IBM and Raytheon both of who have developed variants of the tool to market to their own clients. In the IBM case, the number of questions has been reduced from 521 to about 100 and branching questions that relate to the specific characteristics of the organization are included. NCHICA would like to see a *standardized questionnaire* used nationally so that data could be collected and readily analyzed about the national trends in healthcare information security.

4.2.3 Risk Analysis

Risk analysis follows gap analysis. Risk containment is critical to compliance.

4.2.3.1 Principles

No matter how well a system is designed, vulnerabilities remain. Users, whether normal or hostile, may trigger or exploit these vulnerabilities (see Figure "Risks"). Such vulnerabilities become risks, and organization must determine how much effort to invest in preventing what *risks*.

Risk is organization specific. Determining organizational risk depends on an organization's definition of risk adversity and the criticality of its data. Both of these are organization-specific and require examining an organization's mission and business strategy. The process of determining organizational risk involves (Hellerstein, 1999):

- looking at the type of data an organization has,
- determining who the likely candidates are for intercepting that data, and

- determining the level of capital resources to target the problem.

Engaging in such a *risk assessment* means bringing together representatives from all business units to identify just what data needs to be secured.

The main goal of risk analysis is to help with selecting cost-effective safeguards. Risk analysis involves estimating the potential losses from threats, and how much the safeguards could reduce them. Risk analysis often measures risk in terms of an annual loss expectancy. This is the loss in money units that can be expected in a year. Safeguards can affect the annual loss expectancy by affecting the likelihood of the threat, or its impact, or both. A risk analysis involves the following steps (Summers, 1996):

1. Identify the assets and assign monetary values to *assets*.
2. Identify the *threats* and the vulnerabilities. Estimate the likelihood of each threat. For each asset vulnerable to the threat, estimate the impact of the threat.
3. Calculate the *exposure* of each asset to each threat, in the absence of any additional safeguards.

Table “Loss Ratings for Data Integrity”

Expected Loss Rating	Meaning
Low	data is old or non-vital, change is likely to be detected through normal procedures
Medium	data is important to patient care, change may be detected through normal procedures or cross-checking
High	data is critical to patient care, change is permanent or unlikely to be detected

4. Identify potential safeguards and estimate how much they reduce the exposures. Estimate the costs of the safeguards and determine *cost-effective safeguards*.

Even considering only cost-effective safeguards, their total cost may well exceed the available funds. The organization must decide how to allocate its resources among the potential safeguards.

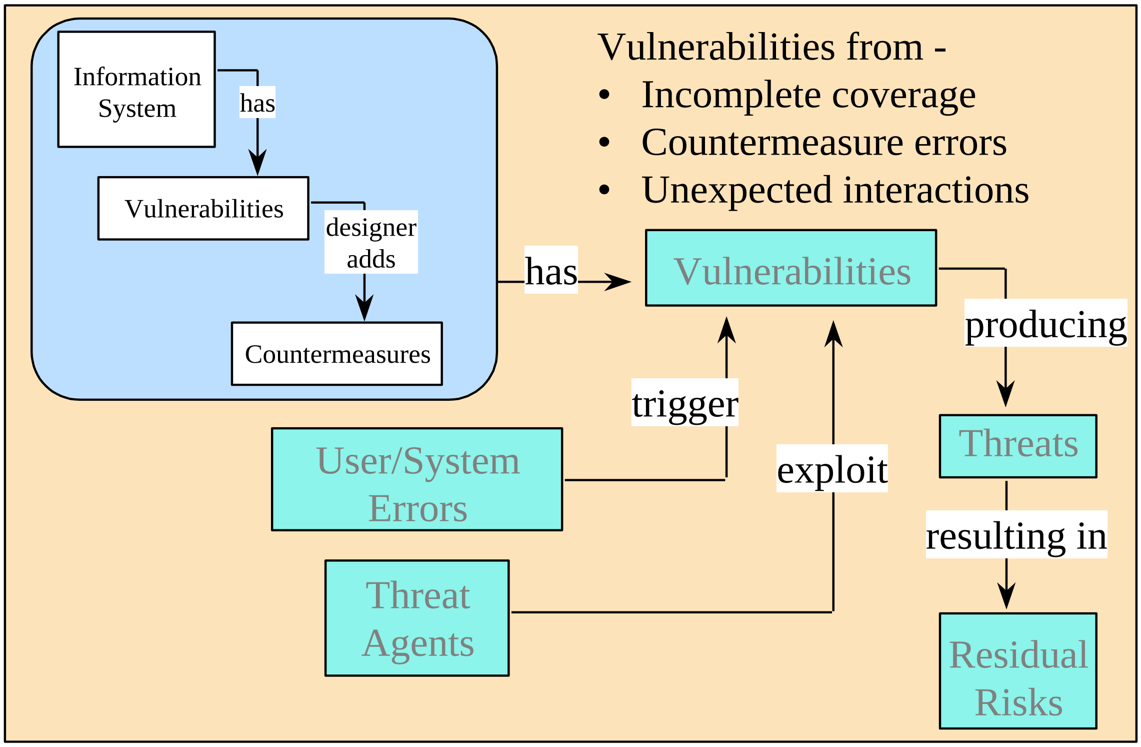


Figure "Risks": The design of the system is shown in the upper left. This inevitably leaves vulnerabilities or gaps which are triggered or exploited by agents and result in risks.

Table "Loss Ratings for Confidentiality"

Expected Loss Rating	Meaning
Low	disclosed information is not sensitive, person receiving confidential information has no intention of using it
Medium	disclosed information is somewhat sensitive, person receiving information does not intend to use it for malicious purposes
High	disclosed information is sensitive, person receiving confidential information intends to use it to harm the patient's care or reputation or for financial gain

CRAMM is one of many generic tools for risk analysis. Most risk analysis uses structured methodologies and software tools that gather and store data, compute risk measures, evaluate cost-effectiveness, and present the results. CRAMM is a British government standard (CRAMM, 2000). A CRAMM analysis begins with identifying the assets, assigning values to them, and determining potential impacts. Using a built-in list of threats, CRAMM software generates *questionnaires* that elicit the vulnerability of each asset group to each threat. The software then calculates a risk number for each impact. Finally, existing countermeasures and others from CRAMM's database are considered. A countermeasure can reduce risk in various ways.

Security breaches cost how much? The costs of security breaches are *difficult to estimate*, as is their likelihood. If the clinic's primary server is violated and its data copied, how does one estimate the cost of this loss to the clinic? If the public becomes aware that the clinic's server has such susceptibility, what is the cost to the clinic of this blow to its reputation? Despite the various objections that can be made to risk analysis, it remains a vital step in assessing an organization's security situation and helping decide what security safeguards to implement.

4.2.3.2 Example

An example of risk analysis is presented for *Georgetown University Medical Center's kidney dialysis unit* and related sites. The site has dialysis machines in one facility with three remote facilities connected to the dialysis machines via an Internet link. This risk analysis assesses the current level of information security and proposes cost-effective measures to improve security (Kim et al, 1997).

Threats are categorized according to their impact on data integrity and confidentiality. Frequency of threat and expected loss are estimated:

- For each threat, a *frequency of occurrence* of Low, Medium or High is given.
- *Expected loss* is also rated Low, Medium, or High. This value refers to the potential for damage should each threat occur.

For data integrity, the expected loss from an occurring threat is rated High, if the changed data is critical to the patient's care, or if the change is permanent or unlikely to be detected (see Table "Loss Ratings for Data Integrity"). For confidentiality, the rating of expected loss depends mostly on the intentions of the person who gains access to confidential information illegitimately. Breach of patient confidentiality by someone who has no intention of using the information would incur a Low expected loss (see Table "Loss Ratings for Confidentiality").

Data integrity can suffer from three events: I1 Alteration, I2 Incorrect Input, or I3 Uncontrolled Software. For the case of the renal dialysis facilities, a description and the threat frequency and expected loss of each event are presented:

I1: A staff member, visitor or outsider might be able to modify or delete patient information stored electronically in the telemedicine system or any of the computers. This could be due to unfamiliarity with the system or to malicious intent. Frequency: Low; Expected Loss: Medium

I2: When patient information is entered into the telemedicine database manually, there is always the possibility of data entry errors. The frequency of such an occurrence is low because most data will not be typed in but transferred electronically. Frequency: Low; Expected Loss: Medium

I3: Software brought by staff members from outside the dialysis unit could malfunction. Frequency: Low; Expected Loss: High

Seven types of breach of patient confidentiality are identified. For each breach the threat frequency and expected loss are given:

C1: System is susceptible to interception during transmission. Frequency: Low; Expected Loss: Medium

C2: Data is intercepted in transit between data cartridge and long-term archive. Frequency: Low; Expected Loss: High

C3: Inadequate password management process. Frequency: High; Expected Loss: Medium

C4: Poor user password protection practices. Frequency: High; Expected Loss: Medium

C5: Off-site archive susceptible to unauthorized building access. Frequency: Low; Expected Loss: Medium

C6: Loss of confidentiality due to inadequate audit trail log. Frequency: Low; Expected Loss: Medium

C7: Violation of patient confidentiality due to inadequate system access control procedures. Frequency: Low Expected Loss: Medium

Countermeasure costs are estimated. Controls can be used at the electronic dialysis unit to counteract the threats to security. The cost to implement each *countermeasure* refers to not only direct financial costs but also the additional time and effort required to implement the countermeasures. Costs are ranked on a scale of 1 to 7 where 1 is the least expensive and 7 is the most expensive. For example, a cost of 1 would indicate little or no inconvenience and a negligible dollar amount. The recommendations follow in the form of a description of the countermeasure, its estimated cost, and the breakdown of components of the cost:

R1. Increase security awareness training for all staff. Cost: 3 (time for staff, time for trainer, educational materials)

R2. Use of encryption during transfer between telemedicine units. Cost: 2 (encryption algorithm, minor inconvenience)

R3. Use of encryption between data cartridge and archive over network. Cost: 2 (encryption algorithm, minor inconvenience)

R4. Control access to telemedicine application. Cost : 2 (access control mechanism)

R5. Require the use of audit logs: Cost: 3 (install audit mechanism, minor inconvenience)

R6. Enforce password management practices. Cost: 1 (minor inconvenience to personnel)

Threat	**Severity**	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**	**R8**	**R9**
I1	2	50%			90%	30%	20%			
I2	2	20%				10%				
I3	2	70%			90%	30%		70%		
C1	2		100%							100%
C2	3			100%						
C3	6	70%					70%			70%
C4	6	70%				20%	70%			
C5	2								90%	
C6	2					100%				100%
C7	2				100%					100%
total severity reduction		11.20	2.00	3.00	5.60	4.60	8.80	1.40	1.80	10.20
cost of		3	2	2	2	3	1	1	1	6

R7. Install virus protection software. Cost: 1 ($100: cost of the software)

R8. Better access control for off-site archive. Cost: 1 (cost of lock, minor inconvenience to users)

R9. Upgrade to Windows NT version of CareLink. Cost: 6 (cost of upgrading to Windows NT, upgrading to new CareLink version, installing and testing the system)

The above countermeasures are evaluated by considering their cost, which threats they diminish, and by how much. To do this, the threats themselves are assigned a severity according to their frequency of occurrence and expected loss (see Table "Severity of Threats").

Computations assign a cost/benefit value to each countermeasure. The Table "Analysis of Countermeasures" analyzes the countermeasures based on the severity of threats, and reduction of a threat's severity achieved by the corresponding countermeasure. The cost of each countermeasure is also listed. For each countermeasure, the cost/benefit ratio is the cost of the countermeasure divided by the total severity reduction. A ratio of less than 0.8 is considered favorable and provides a reasonable *cut-off point* between intuitively effective and non-effective countermeasures.

Values percolate through the countermeasure analysis. The Table "Analysis of Countermeasures" lists the threats in the leftmost column, followed by their severity. Countermeasures are listed in the top row. At each intersection between a threat and a countermeasure, a percentage indicates the amount of reduction in the threat's severity achieved by the corresponding countermeasure. At the bottom of the table, each countermeasure is evaluated. The total severity reduction is a sum of the reductions in severity for all the threats that the countermeasure can mitigate. For example, countermeasure 'R1 Training' mitigates threats I1, I2, I3, C3, and C4 by 50%, 20%, 70%, 70% and 70%, respectively. Threat I1's severity is reduced by 50% from 2 to 1.0, I2's severity is reduced by 20% from 2 to 0.4, and so on. A *total severity reduction* by countermeasure R1 is given by the sum of severities times the percent reductions of each corresponding threat. The sum, 11.20, is entered in the row showing total severity reduction. The greater the total reduction in severity, the greater is the perceived benefit from the countermeasure.

Table "Severity of Threats"

			Frequency
Expected Loss	Low	Medium	High
Low	1	2	3
Medium	2	4	6
High	3	6	9

Training and password management are recommended. Enforcing password management has the best cost/benefit ratio and should be done. The results of this risk analysis also show that it is necessary to increase *security awareness training* for all staff. Although most staff members are healthcare professionals, the need for protecting patient confidentiality raises new issues which may be unfamiliar to the staff. An increase in the security awareness of staff members, especially in regard to electronic patient records, will mitigate many of the risks related to unintended threats to the system.

4.2.4 Information Security Staff

What information security staff are needed? While successful security processes must be implemented across the organization, one role should have prime responsibility for security and that role is called the 'information security officer'. The officer's duties are described in the next section. If the organization is large, then the officer will direct an information security staff.

4.2.4.1 Information Security Officer

The information security officer coordinates the security policy and procedures of the organization. Security initiatives require organization-wide involvement, championed by both the CEO and CIO. The 'owner', however, can be a corporate information security officer. The information security officer identifies the impact on the *information security program* of changes in the patient, business, and computer systems environments in the healthcare industry and specifically within the organization. Based on an awareness of the industry and organizational needs, the information security officer should direct the information security program. The scope of this responsibility encompasses the organization's information in its entirety.

The information security officer has authority and responsibility for:

- Implementing and maintaining a process for defining the organization's goals and objectives for information security.
- Determining the methodology and procedures for accomplishing the goals of the information security functions.
- Proposing information security policies to senior management and establishing standards and programs to implement the policies.

- Determining which security incidents and findings will be communicated to senior management.
- Determining the adequacy of risk assessment and the appropriateness of risk acceptance.
- Determining information ownership responsibilities or when ownership decisions must be escalated.
- Making personnel and administrative decisions in the supervision of the information security and computer access control administration staff, including hiring, termination, and training.
- Controlling the use and expenditure of budgeted funds.
- Preparing a quarterly status report for the chief executive officer.

The information security officer requires these skills and abilities:

- Ability to organize and direct educational programs for all levels of staff on information security topics.
- Knowledgeable about the organization structure, methodologies, and culture.
- Ability to direct projects and participate in teams.
- Knowledge of current technical and procedural techniques in information security.
- Knowledgeable about state and federal regulations, accrediting organizations and healthcare industry standards, and litigation avoidance issues relative to information security matters.
- Ability to establish liaisons with internal and external constituencies with respect to information security matters.

The information security officer has a mix of responsibilities that requires both *technical and managerial abilities*.

4.2.4.2 Other Staffing

Other staff support the information security officer. There does not appear to be a specific relationship between the size of the organization and the *number of information security staff* required. The complexity of the organization, the status of the information security program, and the rate of change in the organization structure, systems and networks are significant factors in determining the information security staff required. The information security function may be a part-time assignment for one person or a full-time assignment to a large staff. The information security unit is typically assigned to the chief information officer but may be assigned to any senior manager in the organization, if that manager will provide the most effective reporting arrangement. Regardless of the size of the information security unit, the information security function must be an organization-wide function and not limited to a specific department or person. Many of the security administration functions will be distributed throughout the organization.

Tenet staffing is illustrative. Tenet HealthCare Corporation (www.tenethealth.com) is a nationwide provider of healthcare services and owns or operates over 100 acute care hospitals and employs over 100,000 people nationwide. While the Y2K problem is different from the HIPAA-compliance security problem, Tenet built on its Y2K experience and staff. Alan Cranford, a Tenet vice-president who headed the company's Y2K committee, said that the Y2K effort worked so well that the Tenet Board of Directors decided to use the *Y2K group* as a model for a similar group under his direction to implement HIPAA security (Carpenter, 2000). Cranford says:

> It's a different mix of people and a different process. Whereas Y2K involved more technology, HIPAA is more in security compliance, information systems, field operations, and legal and audit services. But we feel the same approach will work well, using in some cases the same people.

Tenet first put together a steering group and a work plan before deciding who would join the HIPAA group. Auditors who worked on the Y2K effort are among those who return to track HIPAA compliance.

4.2.5 Training

Training is essential. An important element in a security program is the process of keeping security on everybody's mind through an ongoing training program. The security rules require training for all staff regarding the vulnerabilities of the health information in an entity’s possession and procedures that must be followed to ensure the protection of that information. Employees need to understand their security responsibilities and make security a part of their day-to-day activities.

4.2.5.1 Content

The training program involves the whole organization. The information security training program is intended for all individuals and organizations involved with handling health data information—at all *organizational levels*, including management, clinicians, patients, vendors, and the general public (CPRI, 1996b). Commitment to security must be made at the highest level of an organization and then emphasized throughout all levels. Education programs should be tailored to meet the needs of individuals and situations and may range from classroom lectures and workshops to written material to online guides and tutorials. A special training component should address managers' and supervisors' responsibilities related to managing information security. The education program should be developed as a collaborative program with input from the education and training staff, system security staff, management, patients, and other involved individuals.

Some content is for all individuals and includes the following:

- *Personal responsibility* of trainees for information security management, and the extent to which scope and accountability vary within positions.
- *Sensitivity of health data* and the type and degree of protection needed in relation to the context of the data and the role of the user.
- *Consequences and sanctions* of security breaches to the involved individual, the organization, patients, and the healthcare goals.
- *Workflow management* and its relation to access control and audit.
- *Encryption* and its support for secure transmission.
- Methods of continuous review and assessment for *quality improvement*.
- *Virus protection*.
- *Password management*.

Some content is just for managers and includes the following:

- Management's responsibilities to establish information security training programs for all involved individuals as well as the general public.
- Strategies for assessing, implementing, monitoring, and evaluating information security policies and practices
- Management's responsibility to be knowledgeable about emerging technologies and regulations.
- Legal requirements for information security and the criminal or civil penalties that may result from inappropriate disclosure.
- Appropriate and consistent responses following security violations.
- User education in importance of monitoring login success and how to report discrepancies.

Suggested content for patients and clients, and the general public includes basic system security practices used by organizations to protect information and responsibilities to make informed decisions.

4.2.5.2 Methods of Implementation

Training methods vary. The best ways to implement an information security education program depend on the size of the organization, the status of existing policies and security programs, available resources, and the level of management commitment. In a solo practitioner's office, the training could consist of a brief statement regarding the needs and current proposed level of security in the office, a question and answer period, and signed statements of understanding and nondisclosure. On the other hand, in a large, multi-center organization, the implementation of an effective information security education program might require hiring additional training staff or a contractor. Regardless of the size of the organization, the strategies for training should include:

1. Develop long-range training and education *strategic plan*.
2. Conduct *learning needs assessment*.
3. Assign training and education *responsibilities*.
4. Conduct *resource inventory*.
5. Develop management consensus on *content* to be taught.
6. *Plan* new employee and continuing training and other education processes.
7. *Provide training* and education stratified by job description, department, level of access, and type of user.
8. Identify in the information security guidelines the *frequency of training* and specific training material.
9. Conduct *continuing evaluation* of training.
10. Use results of evaluation and audits to *revise training*.
11. Return to step 3.

First-time training is special. It should occur at the institutional level and the specific-to-job level and should:

- Document trainee attendance,
- Grant access only after training is completed and agreements are signed, and
- Focus on concrete examples.

The first-time training is followed by continuing awareness campaigns to provide organizational reinforcement. Information security training should be a precondition for any credentialing processes.

4.2.6 Quality Control

Security control is quality control. The gap analysis and risk analysis are steps in an organization confirming its *objectives* and assessing its compliance with its objectives. The DHHS security rules tell an organization to specify its objectives and to continually document its efforts to achieve these objectives. The approach is remarkably similar to that for quality control as prescribed by the world's largest standards organization (the International Organization for Standardization, also known as ISO).

4.2.6.1 ISO 9000

The standard for quality management is ISO 9000. *ISO 9000* was issued in 1987 and is the most widely known, most widely adopted, and best selling standard of any that ISO has published (Rada, 1996).

ISO 9000 is broad. ISO 9000 can be applied to quality systems of any organization, commercial or non-commercial. The language and apparent assumptions of ISO 9000 are targeted to the *manufacturer*, but these manufacturing elements can in all cases be adapted to even the most *service-based businesses* (Voehl et al, 1994). The term 'ISO 9000' is usually used to refer to a set of intimately related standards. One standard is a roadmap for the others. One standard covers quality design, quality management, and quality assurance for different kinds of companies. Another standard covers risks, costs and benefits, management responsibility, quality system principles, and other building blocks that help users customize quality standards to conform to real-life situations. The term ISO 9000 is used to refer to this *set of quality-related standards*.

An entity should operate to quality. ISO 9000 addresses the organization's operating process, its quality records, and its quality control. The operating process creates the final service (see Figure "Quality Control"). The *quality records* are maintained relative to this process, and the control system corrects for divergences from quality. Quality control is supported by a procedure manual that provides guidance for the implementation of the quality system on a day-to-day basis. The control system must include a means for identifying, collecting, indexing, storing, retrieving, and maintaining quality records.

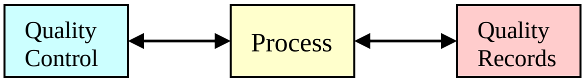


Figure "Quality Control": The rectangle in the middle shows the basic process of the organization. The quality records that are indicated in the right must reflect each step of the basic process. The quality control is indicated on the left and applies to the quality records relative to the ongoing process.

A quality system helps people work to quality. This requires both that the documentation is relevant to the standard and that the behavior of people is relevant to the standard (Huyink and Westover, 1994). Before *certifying* that an organization satisfies the ISO 9000 requirements, one wants to know that the documentation follows the quality standard and people follow the documentation (see Figure "Documents to Behavior").

Mapping Documents and Behavior

		documents relative to standard	
		good	**bad**
behavior relative to documents	**good**	documents conform to standard and people follow documents	documents do not follow standards but people follow documents
	bad	documents conform to standard but people do not	documents do not follow the standard or are missing and people do not follow them

Figure "Documents to Behavior**":** This 4x4 table has columns which indicate the quality of the documents and rows which indicate the behavior of people relative to the documents.

HIPAA's security regulations ask an organization to make a plan and stick to it. The details of the plan are left very open, but the high-level *objectives* are indicated. An organization must begin by assessing its position relative to security, plan how to achieve its objectives, and then work to the plan.

4.2.6.2 Compliance

Compliance is complex. Organizations want to know whether or not their security status makes them compliant with HIPAA. Yet, organizational policy is dictated in only general terms by the regulations from DHHS. Judging whether or not an organization's policies are compliant with the regulations will involve a fair amount of *subjectivity*.

Part of the judgment furthermore must be not so much whether the policy is as it should be but whether the organization actually works according to its policy. Such an assessment requires a careful organizational scrutiny, and the organization should verify that it engages in such scrutiny.

Security regulations require documentation. DHHS asks an organization to:

- certify its systems,
- specify how it processes records,
- audit itself, and
- monitor security breaches.

The documented results of activities could be provided as evidence of compliance to an external accreditation organization. In further detail, each organization is required to

- *evaluate its computer* systems or network designs to certify that the appropriate security has been implemented. This evaluation could be performed internally or by an external accrediting agency.
- formally *specify its processes*. This would include documented policies and procedures for the routine and non-routine receipt, manipulation, storage, dissemination, transmission, and disposal of health information. This is important to limit the inadvertent loss or disclosure of secure information because of process issues.
- continually internally *audit its processes*. This is the in-house review of the records of system activity (for example, logins, file accesses, security incidents). This is important to enable the organization to identify potential security violations.
- implement accurate and current *security incident procedures*. These are documented instructions for reporting and responding to security breaches.

Technology supports precise measurements. The parts of security that involve a technology mechanism may be more amenable to tests of compliance than parts which involve people. For instance, if an encryption algorithm should use 128 bits instead of 64 bits, then the determination of whether or not a given encryption program of the computing system is compliant with the 128-bit requirement would be straightforward to assess. For the rule that requires an organization to have an adequate access authorization policy the test of compliance is less straightforward.

Who will certify? DHHS does not propose to be the agency that certifies organizations as being compliant, although it takes some responsibility for investigating and punishing cases where a lack of compliance is expected. An opportunity exists for other organizations to provide such *certification*. Several accreditation organizations, such as the Electronic Healthcare Network Accreditation Commission, the Joint Commission on Accreditation of Healthcare Organizations, and the National Committee for Quality Assurance, indicate that their accreditation will require compliance with the HIPAA security rules.

4.2.7 Review Questions

1. What is the role of an awareness program in an organization's HIPAA efforts?
2. Why is a baseline assessment done in a gap analysis and what else must be done?
3. What are the features of the HIPAA EarlyView gap analysis tool?
4. What are the principles of risk analysis?
5. What are the responsibilities of the information security officer?
6. What are the features of a training program?
7. In what ways is ISO 9000 compliance similar to compliance with HIPAA security regulations.

4.3 Real-world Policy

Main Points

- Access control supports confidentiality and can be seen from the perspective of business policies.
- Policies limiting physical access to machines are also required.
- An extensive example of real-world security policy at two large organizations suggests a template for similar organizations.

People make security. Regardless of how much technology is used to lock or secure information, the way the people work with one another and with information ultimately has the greatest impact on security. The security policy has to come before the technical decisions are made. If the technology is in place before a security policy is, then the organization has the added difficulty of *retrofitting its technology* to suit its policy.

4.3.1 Access

Confidentiality means controlling who gets access to information. DHHS requires that patient information remains confidential. An organization is required to establish and maintain formal, documented policies and procedures for granting different levels of access to healthcare information. This involves policies for establishing access, authorizing access, and modifying access.

4.3.1.1 Personnel and Partner

Authorizations are controlled. All personnel with access to health information must be authorized to do so. Organizations should:

- assure supervision of personnel performing systems maintenance,
- maintain access authorization records, and
- employ personnel clearance procedures.

Termination procedures help prevent unauthorized access to secure data by those who are no longer authorized to access the data. Termination procedures would include the following mandatory implementation features:

- changing combination locks,
- removal from access lists,
- removal of user accounts, and
- return keys, tokens, or cards that allow access.

The failure to terminate an account of a former employee can have disastrous consequences.

Chains of Trust are agreed. If data were processed through a third party, the parties would be required to enter into a *Chain of Trust Partner Agreement*. This is a contract in which the parties agree to electronically exchange data and to protect the transmitted data. The sender and receiver are required and depend upon each other to maintain the integrity and confidentiality of the transmitted information. Multiple two-party contracts may be involved in moving information from the originating party to the ultimate receiving party. For example, a provider may contract with a clearinghouse to transmit claims to the clearinghouse; the clearinghouse, in turn, may contract with another clearinghouse or with a payer for the further transmittal of those claims. These agreements are important so that the same level of security will be maintained at all links in the chain when information moves from one organization to another.

4.3.1.2 Access Examples

What access policies are in use? Policies do not need to be computer-based, and in the next example the policy is based on who is in a renal dialysis unit. A more elaborate policy for Partners HealthCare System is then presented.

A clinic's policy focuses on physical presence. The security policy in the Georgetown University Medical Center renal care clinic provides all necessary patient information when needed to appropriate people. For instance, patients have the right to review their own information at any time but not the information of other patients. Because patient records are freely available to all persons circulating in the dialysis unit, only *authorized personnel* may enter the dialysis unit. Authorized personnel are the dialysis patients, all dialysis unit staff, and attending and consulting physicians. Family members or guardians of dialysis patients may enter to assist in preparing patients for beginning or ending dialysis but are otherwise not permitted to remain in the dialysis unit. The unit Head Nurse may grant temporary access to the dialysis unit to other persons as needed. A member of the regular unit staff must accompany all persons with temporary access during their entire stay. The Head Nurse will require all persons with temporary access to sign-in and sign-out of a visitors' logbook.

An integrated delivery network has complex access policies. Partners HealthCare System, Incorporated (Partners) was established in 1994 as the corporation overseeing the affiliation of Brigham and Women's Hospital, Massachusetts General Hospital, and North Shore Medical Center. In *Partners' real-world policy*, the right to access and to contribute to a patient's medical information is granted to staff, if they are, have been, or will be involved in that patient's care. In this context, 'staff' includes all clinicians or appropriate support staff that participate actively in a patient's care, e.g. physicians, psychologists, social workers, nurses, physician assistants, medical assistants, physical therapists, occupational therapists, medical students, and case managers. In further detail:

- Staff may be unexpectedly involved in the emergency care of a patient. Thus, provisions must be made to allow such staff to access a patient's medical information. At the same time, such *emergency access* must be closely monitored, to be certain that it has been appropriate.
- Clinicians should be able to access information about patients for whom they have responsibility wherever these patients receive care within Partners. *Primary care clinicians* should have access to the medical information of patients for whom they are the primary caregiver or for whom they are covering for the caregiver. Subspecialists should have access to the medical information of patients for whom they serve as primary care physician, and to the medical information of patients they have seen in the past, or are scheduled to see in the future, as consultants or as specialty care providers.
- Staff in ancillary departments, e.g., laboratories, radiology, and volunteer services, should have access to patient's medical information that is required by their responsibilities. Laboratory technicians, for example, would typically need the results of laboratory tests. Volunteers would not typically access clinician information, although access to non-clinical information, e.g., bed location, might be appropriate.

Information is classified. Some information is given special security. Partners says that access to information about certain patient problems requires special security measures and restrictions because of the sensitive nature of the clinical problem. Clinically sensitive problems include conditions and treatments for which state or federal law impose special restriction. Examples of such protected information include records of psychological or sociological therapy, HIV test results, records pertaining to sexually-transmitted disease, and drug abuse records.

4.3.2 Machine Policy

Physical resources need to be controlled. While the real-world policy is predominantly about the activities of people with healthcare information, the policy also addresses the management of the *physical resources* of the organization. For hardware and software, DHHS requires configuration management and contingency planning. Physical access to computers also needs to be carefully controlled.

Configuration management and contingency plans are needed. System configuration management ensures that routine changes to system hardware or software do not contribute to security weaknesses. This *configuration management* entails:

- documentation of all system modifications,
- procedures that test for security features whenever hardware or software are changed, and
- virus checking.

A *contingency plan* must be in effect for responding to system emergencies. The organization must perform periodic backups of data, have available facilities for continuing operations in the event of an emergency, and have disaster recovery procedures in place.

Physical media must be properly disposed. DHHS specifically calls for controlled access to and disposal of any device with digital information. In particular, the policies must be precise about digital storage media, such as diskettes and data tapes, and about computers themselves. Thus, for instance, when disposing of a tape or a computer, the organization must make certain that no individually identifiable health information remains on the tape or in the computer memory. Also, of course, paper waste should be *destroyed*.

Physical safeguards must minimize unauthorized access. While the latest concerns about security often revolve around illegal access to information via the Internet, a sound security policy must also address the traditional matters of *locked doors*. This would be especially important in public buildings, provider locations, and in areas of heavy pedestrian traffic. Sign-in procedures should be implemented for visitors, and escorts should be provided where appropriate.

4.3.3 Kaiser Example

Kaiser has a sophisticated security policy. Kaiser Permanente (www.kaiserpermanente.org) is a nonprofit, group-practice health maintenance organization with headquarters in Oakland, California. There are 8 million enrolled members, of whom 6 million live in California. With its unique integration of health plan, hospitals, and the closely affiliated Permanente Medical Groups, the *Kaiser* system has a special opportunity to make a success of its *security initiative*, and particular motivation to ensure that its member records are not compromised.

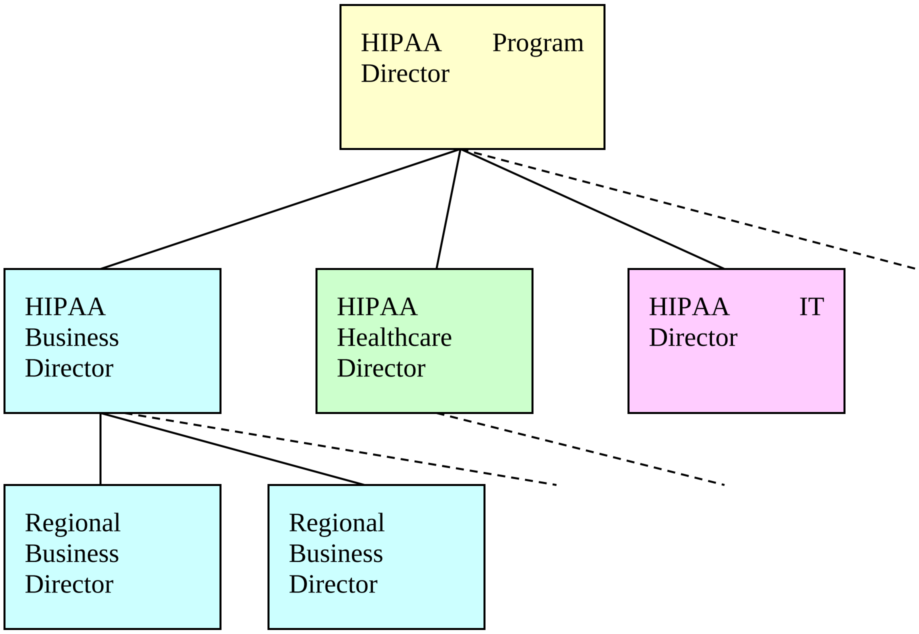

HIPAA Program Director
HIPAA Business Director
HIPAA Healthcare Director
HIPAA IT Director
Regional Business Director
Regional Business Director

Figure "Kaiser HIPAA Organization": The dashed lines indicate further connections first to the other directors, such as of HIPAA Finance, and then to other regional directors that have partial responsibility to the HIPAA directors.

Kaiser's history is rich. Kaiser has been a leader in information systems use for decades. Kaiser made major extensions to its clinical data repository in 1994 and was then stimulated to also extend its security policy. The CEO asked that a security group be formed to develop policy. Physicians, nurses, and staff from medical records, clinical information systems, occupational health, legal, human resources, and internal audit were consulted. A 15-person *security group* was drawn from these constituencies and began meeting in 1995. Soon afterwards, the group contracted outside consultants; went through a self-education process; and then moved into the development of an over-arching set of policies to guide the organization's security implementation. From 1996 through 1997, the group developed its policies one-by-one and released them one-by-one throughout Kaiser via electronic mail (Hagland, 1997). The group also created a *training toolkit* to train people on these topics, and secured the cooperation of the local data processing staff to give everybody training. Portions of Kaiser's policies on roles of staff, local area networks, and email and fax are presented next.

4.3.3.1 Roles of Staff

Kaiser has User, Manager, and Trustee roles. Kaiser has defined the security responsibilities of these roles(CPRI, 1999b):

A User is any person who accesses any corporate data in any form. Each *User* is responsible for:

- maintaining the confidentiality of information;
- complying with regional policies, standards, and procedures including those in this document;
- maintaining a secure work area;
- safeguarding output (such as printed reports, screen prints, copies, diskettes); and
- reporting an observed or suspected breach of information security to management.

Managers oversee and are accountable for specific operational units within Kaiser. *Managers* are responsible for:

- reviewing job responsibilities of a new or transferred employee, consultant, or other user and determining access privileges;
- requesting access by the fewest users necessary to ensure completion of work;
- contacting the Security Officer when a new user requires system access;
- annually reminding users of Kaiser's confidentiality policies; and
- informing users under their supervision of changes in policies, standards, or procedures.

The Trustee is responsible for leading, managing, and administering activities related to an application from a user perspective. For information security, the *Trustee* is accountable for:

- determining how a business application and its data are used and developing and communicating application-specific policies that are consistent with Kaiser policies;
- identifying and monitoring for appropriateness the set of authorized users of the application and its data stores;
- auditing use of and access to the application and data; and
- working with local or departmental management to take corrective action in the event of inappropriate or unauthorized use.

Through these precise definitions of responsibility Kaiser addresses the workflow of the organization.

4.3.3.2 Data Classification

Kaiser classifies data. All corporate data, regardless of medium, is classified according to its value and level of sensitivity. This in turn implies an access policy based on *data confidentiality*. Trustees are responsible for classifying data, and for ensuring that access audits are monitored.

Classification principles emphasize costs and damages. Classification is based upon the data's real monetary *cost* or cost to replace, and the degree to which disclosure or misuse could damage a patient, customer, business partner, or Kaiser. The classification determines the access controls to be placed upon the data. Within general categories of data (e.g., patient medical record), some data may be considered more sensitive or critical than others. Some information in the patient medical record (such as mental health or therapeutic abortion) could be especially *damaging to the patient*, if accidentally or intentionally disclosed. Therefore, this data shall have a higher level of classification.

Data is classified as public, internal, confidential, or registered confidential. Attributes of each classification include: ‘example’, ‘classification criteria’, ‘access’, ‘encryption’, and ‘auditing’. The classification of data is as follows:

Public

- Example: press releases
- Classification Criteria: none
- Access: available to the general public
- Encryption: not required
- Auditing: none.

Internal

- Example: internal phone directories
- Classification Criteria: disclosure may cause some harm to Kaiser or its customers
- Access: generally available to all staff on a need-to-know basis
- Encryption: required if transmitted via Internet
- Auditing: none.

Confidential

- Example: patient treatment data
- Classification Criteria: disclosure may cause some harm to Kaiser or its customers
- Access: limited to as few persons as possible, on a need-to-know basis
- Encryption: required if transmitted via Internet
- Auditing: accesses should be audited as determined by Trustee.

Registered Confidential

- Example: mental health treatment data
- Classification Criteria: disclosure may cause severe harm to Kaiser or its customers
- Access: limited to as few persons as possible, on a need-to-know basis
- Encryption: required if transmitted via Internet
- Auditing: all accesses should be audited.

This data classification also loosely defines who should be assigned what security clearance and the encryption and auditing implications. Unfortunately, the rules for determining the ‘need-to-know’ category of staff are difficult to make precise.

4.3.3.3 Local Area Network

Local area network policies are defined. The definition of roles is one necessary approach to security, but a complementary approach is to define how physical resources will be used. An example of a resource-based security policy is that for Local Area Networks (LANs). Kaiser takes precautions to safeguard the hardware, software, data, and mainframe entry points used by LANs. LAN servers must be located in *physically secure areas*. Entry to server areas is limited to the LAN system administrator or other designated persons.

Configuration authority is limited. Server and workstation configuration is only performed by an authorized member of the LAN system administration team. Servers and workstations must be configured to *prevent users* from:

- booting the system from diskettes,
- installing unauthorized software,
- modifying system configuration files, or
- modifying access control lists for system files or files belonging to other users.

LAN security administrators apply appropriate access *control lists* to ensure that locally stored data may be accessed only by those persons who need the data to perform their job functions. Users are trained to apply access controls to their personal business files.

IDs and passwords are policed. To support user authentication each user must sign-on to the LAN with a *unique user ID*. User IDs may not be shared. Passwords must expire no more than every 35 days and must be at least 6 characters long. The LAN security application *disallows re-use* of the 5 most recently used passwords.

Auditing is done. LAN security administrators reserve the right to conduct periodic spot audits of workstations and to remove any applications or data which have been placed there inappropriately. The department manager will determine which LAN activities or data access must be monitored. The LAN system administrator configures the system to *log these accesses*.

4.3.3.4 Fax and Email

Faxing must be done carefully. All staff are told to take precautions when using fax machines to transmit documents. Fax machines should not be located in areas accessible to the general public. Staff shall *verify the fax number* of the recipient before transmitting. A recipient of a Registered Confidential document must be notified by phone before the document is transmitted. If at all possible, this type of document should not be faxed.

Email must be done carefully. Kaiser encourages caregivers to communicate with their patients via email and requires caregivers to comply with certain rules regarding email. First, both caregiver and patient must agree to communicate via email. Furthermore:

1. The patient must be informed of rules and *guidelines for email communication*.
2. Email is *not for urgent communications*. Patients must be informed that if their messages are not answered in what they consider to be a reasonable period of time, the addressee may not be at work. Another method of communication should then be used.
3. All communications must begin with the *patient's full name* and medical record number.
4. Patients must understand that messages might *not be confidential*. Messages can be misdirected to or intercepted by unintended parties.
5. Clinically relevant messages and responses will be *documented* in the medical record.

Failure to comply with this policy will result in disciplinary action up to and including termination and possible criminal prosecution. A sample email policy follows.

> Ownership and User Privacy of E-Mail
>
> Use of electronic mail is a part of <ENTITY> business processes. All e-mail originating within or received into <ENTITY> is the property of <ENTITY>.
>
> Confidentiality of Electronic Mail
>
> When e-mail is used for communication of individually identifiable health information, a notation referring to the confidential nature of the information should be made in the subject line, and the information should be distributed only to those with a legitimate need to know.
>
> Retention of Electronic Mail
>
> Often, e-mail messages are non-vital and may be discarded routinely. However, some e-mail may be considered a formal record and should be retained. For instance, all clinically relevant e-mail messages, including the full text of a patient's query, as well as the reply, should be stored in the patient's medical record.
>
> Provider/Patient Use of E-mail
>
> The patient should acknowledge these conditions for email use:
>
> E-mail communication is a convenience and not appropriate for emergencies or time-sensitive issues.
>
> No one can guarantee the privacy of e-mail messages. Employers generally have the right to access any e-mail received or sent by a person at work.

The fax and email policies highlight the importance of communicating in ways that are mutually agreeable and safeguard the confidentiality of the information communicated. Kaiser has a handful of other security policy documents, such as one on data retention and another on security training. Together these policy documents constitute an extensive and sophisticated approach to *security in a large healthcare organization*. Kaiser has been anticipating legislation such as HIPAA for many years and is thus well prepared for it.

4.3.3.5 HIPAA Specifics

Kaiser has instituted a formal HIPAA Program. The Program is divided into functional areas with these focuses: project management, business, healthcare, information technology, finances, security, communications, and change management. As Kaiser is a national company divided into geographic regions, the approach to HIPAA requires the fostering of regional implementations while developing national solutions where practical. A national *HIPAA Program Director* is supported by a program office and advised by an Advisory Board (Henderson, 2000). Reporting to the Program Director are Directors for each of the functional areas, including business, healthcare, and information technology. These functional directors coordinate the work of regional directors as regards HIPAA (see Figure "Kaiser HIPAA Organization").

Roll-out has begun. The Kaiser HIPAA Program specified assessment in 2000, design in 2001, and implementation in 2002. The assessment included an awareness campaign and the appointment of people in the key roles. A Kaiser clearinghouse was designed to support the interactions between Kaiser and external entities. Budgets and implementation plans within the regions were also designed.

4.3.4 Mayo Example

Mayo has a strong security policy. The Mayo Foundation (www.mayo.edu) is a charitable, not-for-profit organization based in Rochester, Minnesota. It has 40,000 staff and 500,000 patients. Mayo has a mission as regards security that is stated as follows (CPRI, 1999):

> Data is one of the most valuable assets of Mayo Foundation. It is Mayo's policy to protect this asset from accidental or intentional unauthorized modification, disclosure or destruction. Mayo's data security program must be a well-organized and cost-effective plan which formulates the safeguards to protect patient and Foundation interests.

Mayo's administrative structure to achieve this mission is similar to the structure of Kaiser. Indeed the basic issues to be addressed and legitimate approaches are common across large organizations. Mayo has four key roles to achieve the security mission: data security officer, steward, custodian, and user.

The Data Security Officer directs the data security program. The data security officer is responsible for recommending, developing, implementing and monitoring a consistent data security program. The *data security officer*:

- Coordinates the development and maintenance of data security policy and standards;
- Coordinates data security activities with Mayo Security, Internal Audit Services, Information Services and Treasury Services;
- Monitors security activities to ensure implementation and operational integrity of data security standards;
- Assists the data stewards in assessing their data for classification and advises them of available controls;
- Develops, implements, and maintains a data security awareness program; and
- Provides consulting services for data security throughout Mayo.

Stewards are responsible for a particular set of data. The steward is the person responsible for a particular set of data, for example, a division chair or principal research investigator. Stewards are responsible for implementing data security policy and will ensure custodianship. The *steward* will:

- Assume responsibility for data;
- Recommend appropriate business controls and practices;
- Communicate control and protection requirements to custodians and users;
- Authorize data access and assign responsibility for custody of the data;
- Monitor compliance and periodically review control decisions; and
- Review security violations and report to management.

Stewards will assess their data and the corresponding threats.

Data is classified by stewards. They classify their data as public information, Mayo internal, Mayo restricted or Mayo confidential; and ensure appropriate controls. The meaning of the *data classification* follows:

- *Public* information requires no security controls.
- *Mayo internal* information should be kept within the institution, but requires no special handling in-house. An example is non-medical patient demographic data.
- *Mayo restricted* information should be handled on a need-to-know basis within the institution and not released externally. Examples include purchasing information, accounts payable, and most research data.
- *Mayo confidential* information is very sensitive and should be closely controlled from creation to

destruction. Examples include patient medical information and personnel salary.

The custodian implements the data security policy. The custodian is the person responsible for supplying data processing services and taking care of the system. An example custodian is a system manager. The *custodian*:

- administers steward-specified business and data protection controls,
- administers access control,
- provides backup and recovery of data, and
- detects and responds to violations and weaknesses

Users use Mayo data processing services. They must be aware of the data's sensitivity and take appropriate measures to prevent unauthorized disclosure of it. Users are responsible for protecting institutional information to which they have access and for reporting security violations. *Users* must comply with the data security policy and standards, and they are accountable for their actions.

Monitoring is pervasive. Compliance with the data security standards is monitored. *Monitoring compliance* is the responsibility of the system or area management, the data security officer, and Internal Audit. All users, custodians, and stewards should report instances of noncompliance. All exceptions to these standards are to be requested in writing by the steward of the data and approved by the Information Security Subcommittee.

Employees monitor one another. Employees who have a reasonable basis to believe that a breach of confidentiality has occurred should *report the incident* as soon as possible to any of the following:

- Immediate Supervisor,
- Administrator,
- Human Resources, or
- Data Security Officer.

Employees who have a reasonable basis to believe that a breach of confidentiality has occurred but do not report it are subject to corrective action.

Internal investigations are done. An investigation will be conducted by administration responsible for monitoring the performance of an individual suspected of breaching confidentiality. All information gathered from the investigation will be reviewed with the appropriate members of management, the Data Security Officer, the Human Resources Service Partner, and Legal Counsel, if warranted. These individuals will document the investigation and determine what corrective action is to be taken, which may include, but is not limited to, suspension or *termination of employment*. Under no circumstances will retaliation or intimidation of a complainant be tolerated.

The policies of the Mayo Clinic are repeated in various forms in other healthcare organizations. The *Hawaii Health Information Corporation* has an elaborate policy for information stewardship that defines the roles of the custodians, stewards, and users. That policy is copied in the Appendix of this book.

4.3.5 Culture

Is expensive technology needed? Installing new encryption software and new firewalls may be expensive for a healthcare organization. The first question should be what is needed in a particular organization? What is usually most needed is *changing the culture*.

4.3.5.1 Expensive Equipment?

Vendors encourage purchases. Vendors argue that a lack of broad-based consumer understanding of security options results in relatively low levels of demand for security systems. From the consumer's perspective buying something inexpensive is easier than buying something expensive, but getting a more secure technical system tends to *cost* more. Does risk assessment justify the greater cost?

Abuses may not be technically preventable. The experience of most organizations is with relatively unsophisticated abuses by individuals authorized to access a given system. These abuses are often perpetrated by insiders and happen to have involved computers but need not have. The *bread-and-butter work* of the information security officer is mostly devoted to worrying about such incidents as the following:

- a member of management extracts valuable proprietary data from his employer's computer and sells the data to a competitor,
- an employee copies a backup tape containing confidential personnel information, which he then reveals to his friends,
- an employee uses his employer's computer facilities to arrange illegal narcotic transactions.

These three incidents are typical in a particular sense (NRC, 1991). In none of them did any single computer action of the perpetrator, as a computer action, extend beyond the person's authority to manipulate the computer. There was no problem of password integrity or unauthorized access to data. Rather it was the pattern of actions, their *intent*, and their cumulative effect that constituted the *abuse*.

These kinds of incidents consume much of the security officer's time. What the security officer is likely to want, beyond what he typically has, are better tools for monitoring and auditing the effects of collections of actions, and the easy ability to select and summarize from these in various ways.

Extending computer networks extends the risk. The new pervasiveness of computer networking has increased opportunities for unscrupulous people to exploit the network. However, the experience with exploitation of these networks is also relatively new. Professional and criminal investigation of computer network crime has yet to make clear what the patterns are. Most people consider computer security to be abstract and concerned more with *hypothetical* than likely events. Few individuals not professionally concerned with security have been directly involved in a computer security incident. Yet, people know that installing computer security safeguards has negative aspects such as added cost, slower response times, and the awkwardness of monitoring.

4.3.5.2 Culture Challenge

Although secure technology is an imperative component of a secure enterprise network, technology must defer to culture, if a security program is to succeed. Indeed, as sophisticated as network-security hardware and software is today, technology is the 'easy' part compared to the task of instilling a culture of security in an organization (CISCO, 2000). Security ranks as a *cultural issue* because it cuts across all facets of an organization's business operations. It necessarily integrates the business-unit owners of information and requires continuous feedback on all management levels.

Experts agree that culture is first. The following extracts from an interview illustrate the importance of culture. The interviewees are Douglas Fieldhouse, Network Analyst, University of Pennsylvania Health System; Jane Lawson, Information Security Manager, Hartford Hospital, and Cindy Zak, Director of Health Information Management, Hartford Hospital. The interviewer is Mark Hagland (1998):

> *Fieldhouse*: While the technological solutions aren't necessarily easy, they're a lot easier than the cultural issues, easier than getting buy-in. When it comes to developing a set of policies and procedures at the departmental level, it gets to be extremely hard, tedious, time-consuming work, and most people, quite frankly, don't want to do it.
>
> *Lawson*: Getting top management and physician buy-in remains one of the greatest challenges facing us all. Yes, that involves changing the corporate culture, but doing that is a shared responsibility of all the staff throughout an entire organization. … What I've found is that healthcare professionals hold to a very general philosophy, that yes, patient information is confidential, but when you go to specifics, they don't really know what that means. … There's so much more to information security than just protecting information from people who wander into the hospital. What I've found is that we need to sit down and talk to people very specifically about what security means, right down at a granular level, because that's where the impact is. ….It comes down to telling people things like, 'No, you don't have the right to go into the system and look up your friend's birth date.' And explaining why it's important not to share passwords.
>
> Zak: Over and over, we provide manager training, and on the surface, managers say that security is 'motherhood and apple pie.' But when it shows up in their own world they don't equate the security to their world. …. For example, managers will attend security training and hear about physical security, and then place a workstation with clinical information in an open hallway.

Risk analysis, gap analysis, confidentiality policies, machine security policies, staffing of a security office, and training contribute to the development of a culture that is attentive to information security.

Cultural case studies are available. Culture development at *Salinas Valley Memorial Healthcare System* (SVMHS) illustrates one way to positively support security culture. SVMHS employs 3,000 people of whom 40 work in the information technology (IT) department. Tom Duncan is the Director of the IT department and has been working toward HIPAA compliance since 1996 (Simers and Hamilton, 1999). HIPAA has served as a road map to SVMHS to follow in the course of developing its IT system. Duncan first studied the intent of HIPAA for a year. Then in 1997 SVMHS began educating hospital administrators, physicians, and line employees throughout the organization. Education is still considered by Duncan and his team as the critical link to moving their program forward.

An early start helps. The SVMHS IT Department has a *Computer Systems Security Analyst* who works for Duncan. That Analyst and Duncan spend about a day a week on HIPPA-related projects. Starting on the project early has allowed SVMHS to coordinate purchases to be compatible in their security features. Disparate systems add to the cost and frustration when trying to implement HIPAA regulations. Centralizing certain IT functions prevents the need to start from scratch each time a department adds a new piece of technology. Duncan says:

> We're ahead of the game. Although sometimes we're not on the leading edge, but the bleeding edge. There have been times when we've had to step back a bit from our efforts. But overall, not only will SVMHS be able to meet DHHS's implementation date, but the entire employee-base and medical staff will have a thorough understanding on how to access and use the technology appropriately. … There are technological issues, but it always boils down to people.

Duncan says that while certain people will be the custodian of information within the system, cultural change is required to achieve HIPAA compliance.

4.3.6 Review Questions

1. What are some policies for people to support confidentiality in terms of access control?
2. What roles has Kaiser emphasized in security?
3. What are the Kaiser policies on fax and email?
4. What are the classifications of information confidentiality at the Mayo Clinic?
5. Why is culture important in security?

4.4 Computer Models

Main Points

- Two prominent computer confidentiality models are the information flow model and the access control model.
- Role-based access control gives people access based on their role and can exploit hierarchies of information so as to reduce the complexity of developing and managing access policy.
- Three important services for security are authentication, authorization, and audit.
- An example of role-based access control shows one role giving access to another role.
- DHHS has provided a detailed computer security policy for a small healthcare provider.
- Security may be viewed as workflow management.

Real-world policies are translated into computer models. The policy principles of the real world continue to hold for the computing world, but the scope of computer policy changes. First, the real-world security policy must be automated faithfully. This means that it must be specified *unambiguously* -- an ambiguous policy may work for people but will not for computers. Second, policy choices must be made about the computing situation itself, such as how users identify themselves to the computing system.

4.4.1 Label and Access

Computer security modeling began in the 1960s. The earliest computer security modeling work was stimulated by the development of time-sharing systems in the 1960s. The early systems were developed and used at universities and so reflected the rather permissive policies of universities. The 1970s and 1980s saw a shift toward work reflecting military needs. In the late 1980s, another shift occurred toward business needs.

Two salient model types appeared from 1960 to now. One model is the *label model* or *information flow model* in which information is labeled and access depends on the label on the information. The other is the *discretionary access control model* in which a rule is developed for each combination of person, object, and operation to specify what operation that person can perform on that object.

Labels are ordered in the label model. A typical example is public, secret, and top secret with the obvious ordering. *Labels* are assigned to information and also to people. Thus, a document might be public, secret, or top secret. A person's label is often cited as the person's level of clearance. When a person identifies himself to a computer system, the computer ensures that he never sees information at a higher level than his clearance.

The label model is easily illustrated. The label model has long been used in Department of Defense computer security policies. For instance, a document labeled 'secret' might only be read by people with the rank of Lieutenant or higher. A document labeled 'top secret' might only be read by people with the rank of Colonel or higher. In the medical arena, the security level of a patient test report for a certain disease might be defined according to the possible social impact of an unauthorized disclosure about a patient with that disease. Thus test results for AIDS might be marked 'top secret', while test results for 'sore throat' might be marked 'secret'.

A medical data warehouse uses label-based access control. *Tufts Health Plan* in Massachusetts has 236 million rows of detail data about claims, membership, provider, pharmacy, and employer. Two hundred of Tufts two thousand employees use the warehouse for various purposes, such as claims analysis and retrieval of member information for specific transactional purposes (Haagland, 1997). Data in the warehouse is carefully segregated at the row level for access by staff and business partners, and audited regularly using audit trails. With extremely sensitive patient record information, involving plan members with HIV or who have had psychiatric care, for example, Tufts has developed a *data vault*. There are only two people in the organization who have access to that data vault. This method of controlling access is a combination of identifying data by security-risk level, and severely restricting the people who have access to certain types of data. If the number of people needing to access the data is reasonably small and static and the data relatively easily labeled, then this labeling approach is practical.

Permission to write entails refinements to the label model. The same medical data often has to be treated differently by different users. For instance, a nurse should be able to read the doctor's prescription but not to change it, whereas the doctor can also change the prescription. The label model has generally assumed that whenever a user could read an object that the user could also modify the object. To distinguish reading from writing privileges requires introducing refinements to the flow model. A more complicated version of the flow model has *subjects* that can initiate operations and *objects* that simply contain data, such as a piece of paper. Flow from object to subject is a read operation, and flow from subject to object is a write operation. A subject can only read from an object at an equal or lower level. A subject can only write to an object at an equal or higher level. Thus a subject can contribute potentially highly secure information to an object but only to an object at least as secure as any the subject can read. Notice that a subject in being entitled to write to a higher-level object is not entitled to read any part of that object (other than ostensibly the part that the subject is writing).

The label model can be further enhanced. A label on data can describe the security level of the data and other *categorizations*. For instance, for a label on a medical record, another category might reflect that

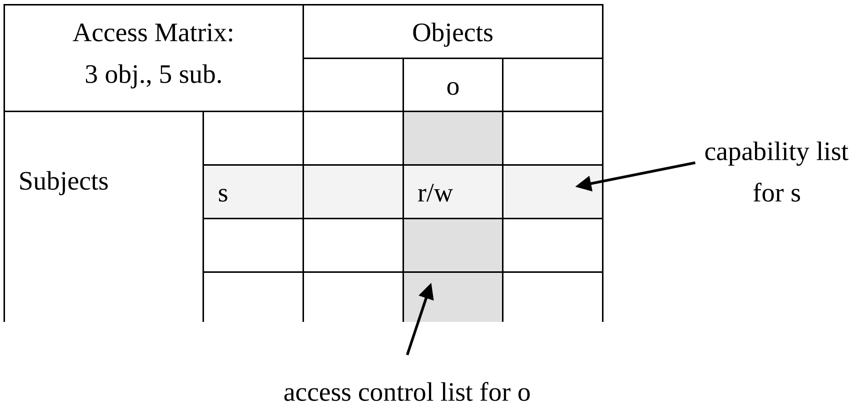


Figure "Access Matrix": Three objects and five subjects are depicted in this matrix.

the medical record is associated with a certain ward in the hospital. Only the responsible doctor in the appropriate ward is granted access to that data.

A label model provides mandatory access control. Although not logically required, the label model policy has generally been viewed as *mandatory* in that neither users nor programs in the system can break the flow rule or change levels. No real system can strictly follow this rule, since, for instance, procedures are needed for declassifying data.

Discretionary access control adds flexibility. The discretionary access control model is based on the idea of stationing a guard in front of a valuable resource to control who has access to it. This model organizes the system into objects, subjects, and operations. *Operations* specify the ways that subjects can interact with objects. The objects are the resources being protected. A set of rules specifies for each object and each subject what operations that subject can perform on that object. There are many ways to express the access rules of which the most popular is the access matrix. The access matrix has a row for each subject and a column for each object. In the access matrix, the cell corresponding to subject s and object o specifies the rights that subject s has to object o. A right represents a type of access to the object, such as read or write. A row of the access matrix corresponds to a *capability list* -- the list of all the rights of a subject. A column of the access matrix corresponds to an *access control list* -- the list of all the rights held by subjects to some object (see Figure “Access Matrix”).

4.4.2 Role-based Access Control

Models to increase efficiency may introduce hierarchies and exploit inheritance properties. For instance, a role might be defined and several people might be assigned to the role. The operations for that role are *inherited* by the people in the role without requiring explicit assignment of an operation to each person. This is the basis for role-based access control.

4.4.2.1 Users and Roles

With role-based access control (RBAC), access decisions are based on the roles that individual users have as part of an organization (NIST, 1995). Access rights are grouped by role name, and the use of resources is restricted to individuals authorized to assume the associated role. For example, within a hospital the role of doctor may have access to all information, and the role of researcher can be limited to gathering anonymous clinical information for studies. The use of roles to control access can be an effective means for developing and enforcing enterprise-specific security policies, and for streamlining the security management process (Ferraiolo, et al, 1995).

Role	Access
Patient	all information for the patient
Doctor	all information
Voluntary caring agency	name, address, clinical data
Researcher	age, sex, clinical data
Organization staff	name and ID

Table “Example Role and Access”

Roles and access permissions for healthcare organizations vary with the organization, but helpful generalizations exist. For instance, one model (see Table “Example Role and Access”) calls for a patient, doctor, researcher, organization staff, and voluntary caring agency staff roles to have certain accesses such that the doctor sees everything and staff see only name and ID (Barkley, 1998).

Roles can be updated without updating the privileges for every user on an individual basis. Users are granted membership into roles based on their competencies and responsibilities in the organization. The operations that a user is permitted to perform are based on the user's role. User membership into roles can be revoked and new memberships established as *job assignments* dictate. Role associations can be established when new operations are instituted, and old operations can be deleted as organizational functions evolve. This simplifies the administration and management of privileges.

RBAC is provably efficient. For each role, let U be the *number of individuals* in role and P be the *number of permissions* required for the role. Whenever (U plus P) is less than (U times P), RBAC requires fewer specifications than the laborious one-at-a-time specification of user access privileges. In fact, whenever U or P is greater than 2, then RBAC has the advantage. In any healthcare organization beyond a 1-person private office, RBAC may have some advantages as a security approach.

When a user is associated with a role, the user is given no more privilege than is necessary to perform the job. This concept of *least privilege* requires identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a role with those privileges and nothing more. In less precisely controlled systems, this is often difficult or costly to achieve.

4.4.2.2 Role Hierarchies

Roles may be put in a hierarchy because they have overlapping responsibilities and privileges. Users belonging to different roles may need to perform common operations. Some general operations may be performed by all employees. In this situation, it would be inefficient and administratively cumbersome to specify repeatedly these general operations for each role that gets created. Role hierarchies can be established to provide for the natural structure of an enterprise. A role hierarchy defines roles that have unique attributes and that may contain other roles; that is, one role may implicitly include the operations that are associated with another role (Ferraiolo, 2000). In the healthcare situation, a role called *Specialist* could contain the roles of *Surgeon* and *Pediatrician*. This means that members of the role 'Surgeon' and 'Pediatrician' are implicitly associated with the operations associated with the role of 'Specialist' without the administrator having to explicitly list the 'Surgeon' and 'Pediatrician' operations (Griew and Currell, 1995).

Operations may be further specialized. An *operation* can be used to capture complex security-relevant details or constraints that cannot be determined by a simple mode of access. For example, there are differences between the access needs of a teller and an accounting supervisor in a bank. An enterprise defines a teller role as being able to perform a savings deposit operation. This requires read and write access to specific fields within a savings file. An enterprise may also define an accounting supervisor role that is allowed to perform correction operations. These operations require read and write access to the same fields of a savings file as the teller. However, the accounting supervisor may not be allowed to initiate deposits or withdrawals but only perform corrections after the fact. Likewise, the teller is not allowed to perform any corrections once the transaction has been completed. The difference between these two roles is the operations that are executed by the different roles and the values that are written to the transaction log file. For example, a physician may prescribe medication. A pharmacist can be provided with operations to dispense, but not to prescribe, medication.

The number of users in a role can be limited. For instance, some roles can only be occupied by a certain number of employees at any given period of time. The role of Chief Radiologist, for example, might be granted to only one employee at a time. A user can become a new member of a role as long as the *number of members* allowed for the role is not exceeded.

A properly administered RBAC system enables system administrators to control access at a level of abstraction that is natural to the way that enterprises typically conduct business. This is achieved by statically and dynamically regulating users' actions through the establishment and definition of roles, role hierarchies, special operations, and other constraints. Thus, once an RBAC framework is established for an organization, the principal administrative actions are the *granting* and *revoking* of users into and out of roles. This is in contrast to the more conventional and less intuitive process of attempting to administer lower-level access control mechanisms directly (e.g., access control lists, capabilities, or type enforcement entities) on an object-by-object basis.

For distributed systems, RBAC administrator responsibilities can be divided among central and local sites. For example, within a distributed healthcare system, operations that are associated with healthcare providers may be *centrally specified* and pertain to all hospitals and clinics. The granting and revoking of memberships into specific roles may be specified by administrators at local sites.

Access policies may need to be modified. The software interface should help appropriate roles easily *modify* the access privileges associated with subordinate roles. Additionally, the granularity of access to documents may need to be fine in order to allow access to some parts of a document but not others.

RBAC deals well with confidentiality but less well with integrity. Integrity requires being clear about who can make what changes to which information and when. Getting the integrity specifications clear requires essentially scheduling the work of all staff on all information. This is an extension of role-based access control into *workflow management*.

4.4.3 Authentication to Audit

Access control is supported by authentication, authorization, and audit services. In brief:

- *Authentication* determines who is responsible for a given request,
- *Authorization* determines who is trusted for a given purpose, and
- *Auditing* records each operation that is invoked along with the identity of the subject and object.

Whenever an operation is invoked, the computer uses authentication to determine whether the requester is trusted for that operation (ASTM, 1996). If so, the computer allows the operation to proceed; otherwise it cancels the operation. In either case, it uses auditing to record the event.

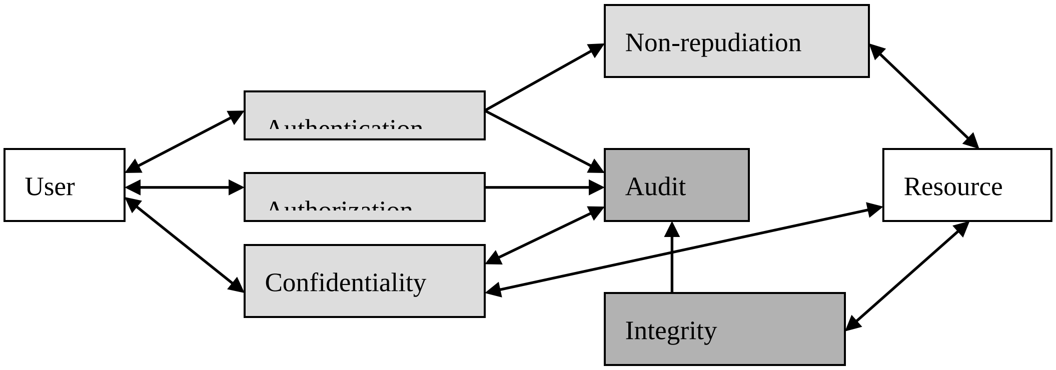


Figure "Security Services": Authentication and authorization are audited (Stoneburner, 2000). Integrity relates to the wholeness of the resource. The darker rectangles relate to recovery services, while the less dark rectangles relate to prevention services.

4.4.3.1 Authentication

HIPAA requires data authentication and entity authentication. *Data authentication* means that an organization can corroborate that data in its possession has not been altered or destroyed in an unauthorized manner. Examples of how data corroboration may be assured include the use of a check sum, double keying, a message authentication code, or digital signature. *Entity authentication* requires corroboration that an entity is who it claims to be. The following entity authentication implementation features might be used:

- A biometric identification system.
- A password system.
- A personal identification number (PIN).
- Telephone callback.

A token system uses a physical device for user identification.

The prevalent means of entity or user authentication in healthcare systems is the entry of passwords. Passwords are commonly implemented as a set of user identification codes and passwords. A *user identification code* is used to identify a user to the system and to other users. The user identification code provides the relationship between the user and what information the user may access. A password is a string of characters that in conjunction with other information, such as the user identification code, uniquely confirms the user's identity to the system. A password may be chosen by the user or assigned by the system. If passwords are stored on the system, then they should be encrypted. All passwords should be scheduled to expire at routine intervals.

Once a user has been authenticated, ensuring that the current user is still the authenticated user must be addressed. Minimizing the opportunity for an unauthenticated user to utilize another's access can be supported through the use of automatic logoff after a stated period of inactivity or when the authenticated user accesses the system from another terminal. The logon and logoff processes should be quick and efficient to help ensure that users comply with the requirement that they *logoff* following completion of their terminal activity.

4.4.3.2 Authorization

Authorization is the granting of rights. Authorization provides that an authenticated user has access to the functions, information, and privileges that the user is requesting the system to provide. Authorization to access a system includes both authorization to gain physical (or connectivity) access and authorization to gain access to resources contained within the system. Authorization is accomplished through access controls, *confidentiality* services, and *non-repudiation* (or attribution) services.

Confidentiality services protect against disclosure of information to entities not authorized to have that information. Locally, access controls placed on data files can protect them from being read by unauthorized users. Such access controls can protect the data, and the attributes associated with data files (existence, size, and variations). Confidentiality services can also provide for removal of data from storage media so they may not be read after memory or files have been (appropriately) 'deleted'. Confidentiality services must also be instituted within a network environment. The most common form of confidentiality service over a network is *encryption*.

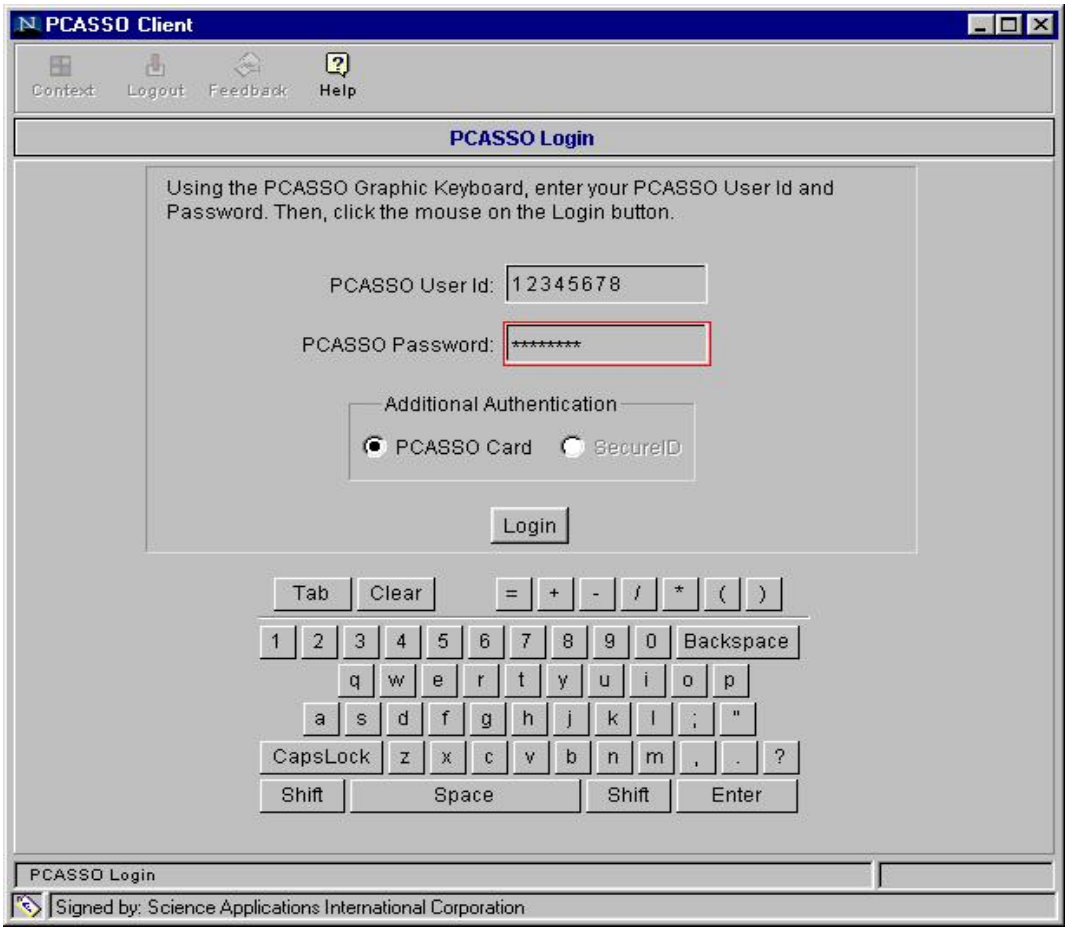
Non-repudiation prevents repudiation. Repudiation is a threat in which an individual falsely denies having taken an action. Non-repudiation services assure that information that purports to be from and actions that purport to have been performed by a user or system are as claimed. In other words, non-repudiation services provide evidence to prevent a person from unilaterally modifying or terminating obligations arising out of a transaction effected by computer-based means. A *non-repudiation service* does not eliminate repudiation, but ensures the availability of evidence to support resolution of any disagreement. The most commonly used non-repudiation mechanisms are digital signatures and audit trails.

4.4.3.3 Audit

The Security NPRM requires audit trails. An audit trail is a chronological record of activities occurring in the system, created immediately concurrent with user actions. Audit trails can be examined to detect and investigate breaches in security, determine compliance with established policy and operational procedures, and enable the reconstruction of a sequence of events affecting the information. *Audit trail records* contain

- identification of the user,
- data source,
- person about whom the health information is recorded,
- provider facility,
- time and location of the activity, and
- nature of the activity (i.e., function performed and information accessed).

Audit trails track access to view content, to create content (including that to update, modify, append, or import from other systems), and to copy to external



Using the PCASSO Graphic Keyboard, enter your PCASSO User Id and Password. Then, click the mouse on the Login button.

PCASSO User Id: 12345678

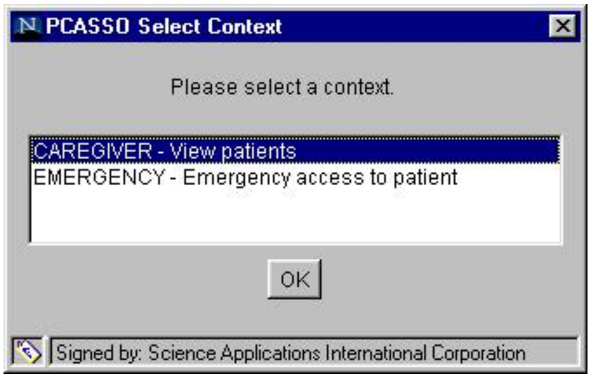
PCASSO Password: *********

● PCASSO Card ○ SecureID

PCASSO Login

Signed by: Science Applications International Corporation

Figure "Keyboard Widget"**:** After the user enters his User ID and password, the user clicks on the Login button.



PCASSO Select Context

Please select a context.

CAREGIVER - View patients
EMERGENCY - Emergency access to patient

Signed by: Science Applications International Corporation

Figure "Select a Role"

media or export to other systems. Audit trails also track the progress of each operation from the point of initiation through event steps to a terminal state (e.g., resolved or canceled). The authentication and authorization services are, in a sense, part of what is audited and thus feed into the audit (see Figure "Security Services").

4.4.3.4 Example

An example follows of how the Mayo Clinic implements some of the authentication, authorization, and audit features. All computer terminal access is controlled through a password or through physical security measures. Each user's identity is authenticated through a verification process. For example, access may be granted to a device, a unique token such as a card with a magnetic strip, or an individual password. Users select and change their own passwords, and should do so at least every ninety days.

The custodian implements data processing services. (The data to be handled has been classified into four categories of increasing sensitivity called public, internal, restricted, and confidential). The custodian must:

- periodically review user access privileges and *remove identification codes* from systems when users no longer require access.
- implement *inactivity time-outs* for terminals and workstations which access restricted and confidential information. Custodians must implement inactivity time-outs for all terminals and workstations at non-Mayo locations that have remote access to Mayo systems and information.
- *audit* all unauthorized accesses and attempts to access restricted and confidential information. Audit records shall be kept at least six months, and custodians must periodically review the audit records for evidence of violations or system misuse.

Custodians must be aware of access-control vulnerabilities for data while it is in transmission within the Mayo network. Proper engineering solutions may require leased lines or encryption.

4.4.4 Role-Based Example

PCASSO is a role-based access control system. *Patient Centered Access to Secure Systems Online* (PCASSO) allows users to search and display health information, including demographics, lab tests, and visit notes. The project is designed to give both staff and patients easier access to, and more control over, medical information over the Internet. PCASSO uses familiar Web technologies such as Web servers, web browsers, and Java applets. The server software and information is stored on a remote computer. PCASSO uses encryption to protect sensitive information being sent over the Internet. Science Applications International Corporation has partnered with the University of California at San Diego School of Medicine in the development and use of PCASSO.

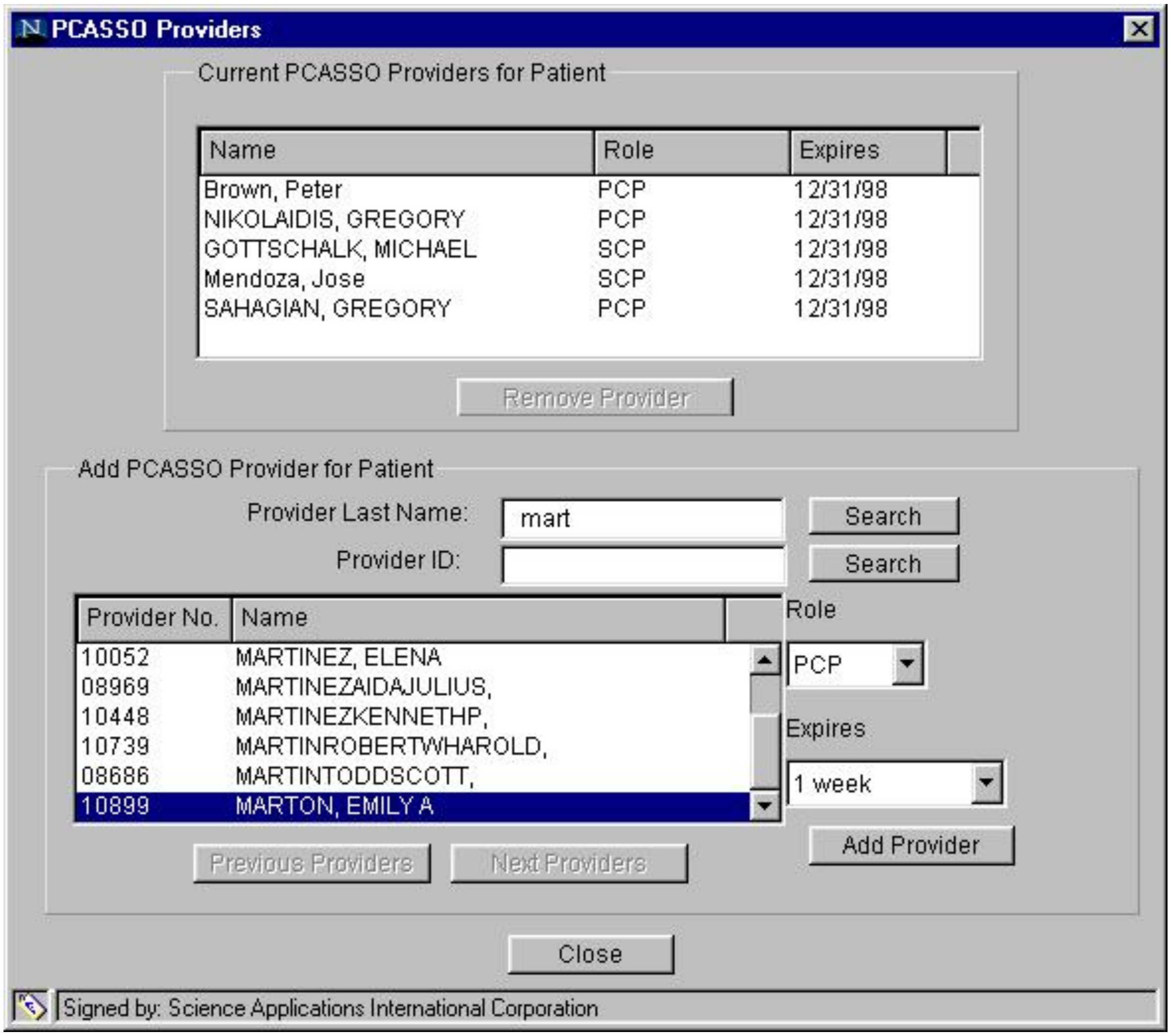
Login and Authentication use a web page 'keyboard widget' (see Figure "Keyboard Widget") and run by mouse point-and-click on the key representations to enter User ID and password. The keyboard widget makes it more difficult for a hacker to capture information the user enters than if the user entered the information using the keyboard. After the PCASSO client has the necessary access privileges, a dialog box will appear asking the user to insert his PCASSO *diskette*. This diskette contains security keys critical to PCASSO protection. Keeping this information on a diskette rather than on a hard disk makes it more difficult for a hacker to capture it.

A role is selected. If a user has multiple roles, the 'Select Context' dialog will appear. A 'context' is simply the user view and is associated with a role; such as 'caregiver'. Emergency situations may exist in which a doctor may need to review information relating to a patient, but the PCASSO system does not recognize a provider-patient relationship between the doctor and that patient. For such occasions, PCASSO provides an *Emergency role*, which enables the doctor to self-declare a provider-patient relationship (see Figure "Select a Role"). Use of the Emergency role is considered a privileged action, and as such, the access is effective for only a 72-hour period, and it is closely audited and monitored for potential misuse. To avoid creating suspicious audit logs and usage patterns, users should not use this role as a default role.

Referrals to specialists may be made. If a doctor is a Primary Care Provider referring his patient to a *specialist*, and he would like the specialist to have access to the patient's record, he will need to add that specialist's name to the list of providers in the PCASSO system (see Figure “Add Provider”). PCASSO will also automatically allow access to specialists based on scheduling information coming from the University of California at San Diego central scheduling system.

The PCASSO Security Policy Model uses Object-Attribute-Operation formalisms. The entities are:

- A *system* that represents the information-system itself.
- *Individuals* that represent the people using the system.
- *Roles* that represent the capabilities of people that are working in a particular relationship to



PCASSO Providers

Current PCASSO Providers for Patient

Name	Role	Expires
Brown, Peter	PCP	12/31/98
NIKOLAIDIS, GREGORY	PCP	12/31/98
GOTTSCHALK, MICHAEL	SCP	12/31/98
Mendoza, Jose	SCP	12/31/98
SAHAGIAN, GREGORY	PCP	12/31/98

Add PCASSO Provider for Patient

Provider Last Name: mart

Provider ID:

Provider No.	Name
10052	MARTINEZ, ELENA
08969	MARTINEZAIDAJULIUS,
10448	MARTINEZKENNETHP,
10739	MARTINROBERTWHAROLD,
08686	MARTINTODDSCOTT,
10899	MARTON, EMILY A

Role: PCP

Expires: 1 week

Signed by: Science Applications International Corporation

Figure “Add Provider”: Primary care providers are designated with the letters ‘PCP’ under Role, and secondary care providers are designated by ‘SCP’ under Role. To add a provider to his patient's list of providers, the doctor uses the ‘Add PCASSO Provider for Patient’ lower part of the window. He types in the new provider's name and click on the ‘Search’ button. When the provider appears in the list below, he selects the provider's name and specifies a role from the pull-down menu, i.e. PCP or SCP. Then he specifies the time period for allowed access by selecting from the ‘Expires’ pull down menu (e.g. 1 week, 6 months, 1 year) and clicks on the ‘Add Provider’ button. This new provider will be added to the ‘Current PCASSO Providers for Patient’ list.

the system or to a particular patient.

- *Patient-Information* that represents the patient-information managed by the system.
- *Contexts* that represent the patient or the system and provide a means of modeling requirements for simplifying the transitions between one patient-role and another.

The *high-level rules* are:

- The system shall provide a closed environment that ensures information confidentiality, integrity, accountability, and availability.
- The system shall audit all actions to the granularity of a single individual.
- System information and functions will be accessible only to authenticated individuals functioning in authorized roles.
- An individual may be authorized to adopt only one role for a given patient.
- Multiple individuals may be authorized for a single role.
- A given individual may be acting in only one role at any given time.
- Multiple individuals may be acting in the same role at any given time.
- Only a patient's primary care provider may alter the security attributes of the patient's record information.
- A patient's primary care provider can grant or revoke the ability of individuals to assume roles with respect to that patient.
- The primary care physician can authorize and grant rights to secondary care physicians.
- In emergency situations, care-providers with appropriate need should have unrestricted access to a patient-record.

Other rules exist, but one sees here how precision can be achieved through such rules. One thus avoids some of the ambiguity of traditional natural language constructs.

User evaluation of PCASSO is mixed. Generally patients welcome this additional access to information. On the other hand, physicians are unhappy with the system on two counts. First, the time taken to login into the system is greater than the physicians want. Second, the physicians work in flexible teams where one person will attend to a patient's need at one time and another physician at another time. The need to explicitly assign access permissions interferes at times with this flexibility. Physicians frequently invoke the 'emergency' access role. This frequent use of the 'emergency' over-ride option works against the intention of the designers of the role-based access system. Accordingly, the developers of the PCASSO system are *revising features* of PCASSO. One solution to the time of login would be to have a faster biometric authentication method. One solution to the overuse of the emergency role is to expand the notion of teams and to have physicians assigned liberally to teams with wide-ranging patient responsibilities. The belief remains that role-based access control is a superior method for controlling access to patient records.

4.4.5 Small Provider

Small providers can implement simple security models. The size and organizational structure of the entities that are required to implement the security standard vary tremendously, and the appropriate approaches vary accordingly. The following example describes the manner in which a small or rural provider might choose to implement the requirements of the standard. This example comes directly from the proposed regulations of the DHSS and is intended to help persuade small providers that the *costs* of operating in a secure fashion are not excessive.

For purposes of this example, a small provider is a one to four physician office, with two to five additional employees. The office uses a *PC-based* practice management system, which is used to communicate intermittently with a clearinghouse for submission of electronic claims. The number of providers is of less importance for this example than the relatively simple technology in use and the fact that there is insufficient volume or revenue to justify employment of a computer system administrator.

The office first assesses risks to its information assets. Then, to establish appropriate security, the office would develop policies and procedures to mitigate and manage those *risks*. These would include an overall framework outlining information security activities and responsibilities, and repercussions for failure to meet those responsibilities.

Next, this office might develop contingency plans to reduce or negate the damage resulting from processing anomalies. This office might establish a routine process for maintaining back-up media at a second location, obtain a PC maintenance contract, and arrange for use of a back-up PC should the need arise. The office would need to periodically review its plan to determine whether it still met the office's needs.

One person on staff might assume the role of 'security officer' along with other roles. The office would need to create and document a personnel security policy and procedures to be followed. The *security officer* should be charged with the responsibility for assuring the Personnel Security requirement is met. This responsibility would include seeing that the access authorization levels granted are documented and kept current. For example, records might be kept of everyone who is permitted to use the PC and what files they may access. Training in security must be provided to all personnel.

For this small provider, the Security Configuration Management requirement would be relatively easy to satisfy. The necessary features could be part of a purchased *hardware/software package* or be included as part of the support supplied with the purchase of equipment and software. For example, a new PC might be equipped with virus checking software. Termination procedures would incorporate specific security actions to be taken as a result of an employee's termination, such as obtaining all keys and changing combinations or passwords. The small or rural provider office would also need to ensure that it activated the internal auditing capability of the software used to manage health data files so that it tracks who has accessed the data.

Documentation is important. A small or rural provider may document compliance with many of the foregoing administrative security requirements by including them in an 'office procedures' document that should be required reading by new employees and always available for reference. This *office procedures* document should include:

- contingency plans,
- formal records processing procedures,
- information access controls (rules for granting access, actual establishment of access, and procedures for modifying such access),
- security incident procedures (for example, who is to be notified if it appears that medical information has been accessed by an unauthorized party), and
- training.

Periodic security reminders could include visual aids, such as posters and screen savers, and oral reminders in recurring meetings.

Physical access controls would be straightforward for this small or rural office, using locked rooms or closets to secure equipment and media from unauthorized access. The office procedures manual should include directions for authorizing access and keeping records of authorized accesses. *Media Controls* and *Workstation Use* policy instructions would be developed by the office and would include additional instructions on such items as where to store backed-up data, how to dispose of data no longer needed, or logging off when leaving terminals unattended. Safeguards for the security of workstation locations would depend upon the physical surroundings in the small or rural office. The small or rural provider may meet the requirements by locating equipment in areas that are generally populated by office staff and have some degree of physical separation from the public.

A simple access model is enough. The technical security services requirements for access control, entity authentication, and authorization control may be achieved simply by implementing a *user-based data access model*, i.e., assigning a user-name and password combination to each authorized employee. Other access models could be employed if desired, but would prove unwieldy for the small office. By assigning full access rights to a minimum of two key individuals in the office, implementation of the emergency access feature could be satisfied. Audit control mechanisms, by necessity, would be provided by software featuring that capability. By establishing and using a message authentication code, data authentication would be achieved. Use of the password system mentioned above could also satisfy the 'unique user identification' requirement.

Internet use is special. If this provider chooses to use the Internet to transmit or receive individually identifiable health information, some form of encryption must be used. For example, the provider could procure and use commercial software to provide protection against unauthorized access to the data transmitted or received. This decision must take into account what encryption system the message recipient uses. On the other hand, health information when transmitted via other means such as private wires or dial-up connections may not require such absolute protection as is provided by encryption. This small or rural provider would likely not be part of a network configuration, therefore, only integrity controls and message authentication would be required and could be provided by currently available software products, most likely provided as part of a contract with the provider's clearinghouse.

Small providers may need guidance regarding the content of the documents required by this rule (for example, specifics of a 'chain of trust' partner agreement). Models of the documentation discussed in this example should be developed by industry associations and vendors. If this model documentation is not developed, DHHS would work with the industry to develop them. The small or rural provider office would normally evaluate and s*elf-certify* that the appropriate security is in place for its computer system and office procedures. This evaluation could be done by a knowledgeable person on the staff, or more likely, by a consultant or by the vendor of the practice management system as a service to its customers.

4.4.6 Workflow Systems

Integrity concerns workflow. The combination of role-based and label-based access control can provide robust confidentiality but not integrity. *Integrity* can be gained by adding scheduling of modifications. The addition of scheduling to access control leads to a workflow management systems. A workflow management system (Hollingsworth, 1995):

- routes information from one human or computer system to another and
- determines the sequence in which activities are executed.

People, software systems, or a combination of these can execute activities.

The architecture for workflow management systems should emphasize the interoperability of components (www.wfmc.org). The key components are the *workflow engine* that in turn communicates with a monitoring module, a client module, a process definition module, and an application module (Michailidis and Rada, 1998). A complete workflow management system might provide all the information necessary for roles to do their assigned work and record all the manifestations of the performed work.

Workflow management is also knowledge management. Macintosh et al (1999) say, "Knowledge management involves the identification and analysis of available and required knowledge assets and knowledge asset-related processes, and the subsequent planning and control of actions to develop both the assets and the processes so as to fulfill organizational objectives." This definition of *knowledge management* is remarkably similar to the definition of workflow management.

Workflow management enables electronic commerce (Muth et al, 1998). An electronic commerce system includes not only transactions that center on buying and selling goods and services to directly generate revenue, but also those transactions that support revenue generation, such as generating demand, offering sales support and customer service, or facilitating communications between business partners. This customer support requires workflow management. Ultimately, to build adequate computer security policies one needs an *electronic organization* to mirror the real-world organization. Such electronic or e-organizations (like e-health, e-finance, or e-manufacturing) transcend space, time, and organizational boundaries to improve organizational performance (Mowshowitz, 1997).

Rather than considering the proposed HIPAA security requirements as a burden, healthcare organizations should view the requirements as a stimulus to acquire e-health characteristics -- in other words to acquire e-commerce and workflow characteristics. Patients and employees are increasingly demanding opportunities to share information online. If the confidentiality, integrity, and availability facets of security are seen from the *positive side* of leading the right people to the right information (rather than the negative side of blocking the wrong people from the wrong information), then security is an investment with positive cash returns.

4.4.7 Review Questions

1. What are the similarities and differences between the information flow and the access control models?
2. How does role-based access control bring efficiency and flexibility to access control?
3. Describe the functions of authentication, authorization, and audit relative to one another.
4. What are the key features of PCASSO?
5. Summarize how a small provider might implement security.
6. How is workflow an extension of security?
7. Suggest how a computer security model that combines label-based and role-based access control might be specifically suited to a hospital context. (Project Question)
8. How might the flexible team needs of the healthcare professionals be met by a modification to the PCASSO design. (Project Question)

4.5 Computer Mechanisms

Main Points

- Mechanisms for security should create a trusted computing base.
- With public-key encryption a person has a private and a public key and never needs to give anyone else his private key.
- A public-key infrastructure supports public-key encryption.
- Virtual private networks tunnel through the Internet with encrypted messages.
- Electronic signatures authenticate messages.
- An example of a large-scale PKI system shows how the technologies are being deployed.
- A detailed Internet security policy from HCFA is in use.
- Medical records are available in secure fashion across the Internet by relying on encryption and other techniques.

Computer security mechanisms support computer security policies. A trusted computing base is explained in the next subsection. Then the focus shifts to cryptography and follows onto the various more complex mechanisms that rely on cryptography, namely, public-key infrastructure, virtual private networks, and electronic signatures. The DHHS security regulations give healthcare organizations a range of computer mechanisms from which to choose in implementing adequate security. What are these *mechanisms* and what do they mean for healthcare?

4.5.1 Trusted Computing Base

The set of trusted hardware, software, and network components is the Trusted Computing Base (TCB). A component must be trusted, if it has to work for the system to meet its security specification. If a component is in the TCB, so is every component on which it depends because otherwise it is not guaranteed to work either. The *TCB* should:

- be simple, so that it can be practically analyzed, tested, and maintained,
- mediate all accesses that it protects so that the TCB cannot be bypassed, and
- be protected against any direct tampering.

The TCB is kept small by including in the TCB only *essential functions*. For example, a large and complicated word processor may be used to prepare purchasing orders, but the TCB can be limited to a small program that displays the completed order and asks the user to confirm it.

Since software consists of instructions that must be executed by hardware, the hardware is part of the TCB. Special hardware can be developed to support security, particularly for time-consuming encryption

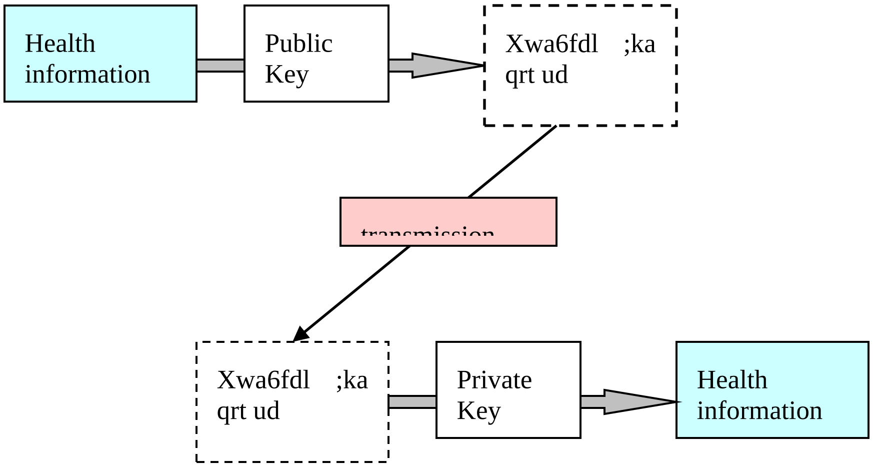


Figure "Public-key encryption": The plaintext 'health information' goes through the public key encryption and becomes the ciphertext 'Xwa6fdl ;ka qrt ud'. The ciphertext is transmitted and is then decrypted with the private key.

computations. Hardware also has physical interactions with the environment. For instance, someone can open a computer cabinet and remove a disk. *Physical protections* are vital.

The operating system is the brain of the computer network as it coordinates all the resources of the network and determines what users get access to what devices. The operating system thus includes authentication mechanisms, access controls, and audit trails. The *authentication mechanisms* include passwords, tokens, and biometric authentication. UNIX access control is coarser than Windows NT access control.

Application software is to be avoided as part of the TCB. In most systems, any application program running on behalf of a user has full access to all that the user can access. A program that appears to do something useful but has hidden within it the ability to cause serious damage is called a Trojan horse. A *Trojan horse* can be hidden in many places, such as a macro in a word processor. The danger is greater if the Trojan horse can make copies of itself. Such a program is called a *virus*. The Security NPRM calls for virus checking.

Communications networks among computers are part of the TCB. The Security NPRM requires that each organization protects communications containing health information that are transmitted electronically so that they cannot be easily intercepted and interpreted by parties other than the intended recipient. Organizations must also protect their information systems from intruders trying to access systems through external communication points. When using open networks, such as the Internet, some form of *encryption* should be employed. The utilization of a private-wire arrangement provides sufficient access control to make encryption unnecessary.

4.5.2 Cryptography

Cryptography encrypts and decrypts messages in secret code or cipher. Encryption converts data into a secret code for transmission over a network using an algorithm that allows only the intended receiver to decode it at the other end. The two main cryptographic methods are secret key and public key. In *secret key*, both sender and receiver must secretly share the information about how the message is encoded and decoded. *Public key* encryption involves both a private and a public key. The sender can use the receiver's public key to encrypt a message; the receiver uses his or her private key to decrypt it. Whereas the first method, secret key, requires first getting the key to the message recipient, in the second method, owners never have to send private keys.

Encryption techniques mathematically transform a message into a *ciphertext*. Mathematical operations called *one-way functions* are particularly suited to this task. A one-way function is comparatively easy to do in one direction but much harder to do in reverse. For example, with a little concentration, many people can probably multiply 24 by 24 without using a pencil and paper. One the other hand, calculating the square root of the number 576 is much harder, even with a pencil and paper.

'Pig Latin' is a cryptographic technique that is good for children but not for serious work. The *pig Latin one-way function* is to take the first consonant of a word and move it to the end of the word and append 'ay'. If the word begins with a vowel, simply append 'ay'. Thus the sentence

> 'This is a cipher for simple messages'

becomes in pig Latin

> 'hisTay isay aay iphercay orfay implesay essagesmay'.

To decrypt the encoded message one removes the 'ay's at the end of words and moves forward the last consonant. As soon as someone has the ciphertext and knows pig Latin, the person can decipher the message.

The RSA Algorithm is a one-way function and supports the possibility of public and private keys (Flinn and Jordan, 1997). The RSA Algorithm has three steps:

1. *key generation*: Two prime numbers 'p' and 'q' are chosen and multiplied together to form 'n'. An encryption exponent 'e' is chosen, and the decryption exponent 'd' is calculated using 'e', 'p', and 'q'.
2. *encryption*: The message M is raised to the power 'e', and then reduced modulo 'n' to form the ciphertext C.
3. *decryption*: The ciphertext C is raised to the power 'd', and then reduced modulo 'n' to re-recreate message M.

When the RSA Algorithm is used in a public key system, the modulus 'n' and the exponent 'e' are published as the public key. The other exponent 'd' is kept secret, as the private key. Each user holds his or her own private keys, and knows the public keys of the other user or users (see Figure "Public-key Encryption"). Detailed, complete examples of the use of public key encryption are available (Graaf, 2000). It bears note that 'p' and 'q', the factors of 'n', are not needed for encryption or decryption; they are only used in the key generation step. The difficulty of determining ‘p’ and ‘q’ from ‘n’ and ‘e’ is what protects the holder of ‘d’ from someone computing ‘d’ based on ‘n’ and ‘e’.

An illustration of the public key method follows:

- Rosa knows her own public key (e_{rosa} and n_{rosa}), her own private key (d_{rosa}), and Ray's public key (e_{ray} and n_{ray}).
- Ray knows the converse: his public key (e_{ray} and n_{ray}), his private key (d_{ray}) and Rosa's public key (e_{rosa} and n_{rosa}).
- For Rosa to send Ray a private message M that only Ray can read, she performs the following operation on the message M: $C_{M \text{ for ray}}$= (M raised to the power e_{ray}) modulo n_{ray}
- Ray, who is the only one to possess his private key (d_{ray}), performs the following to recover the message M: M = ($C_{M \text{ for ray}}$ raised to the power d_{ray}) modulo n_{ray}
- To sign a message S, Rosa encrypts with her own private key: $C_{\text{rosa signs S}}$= (S raised to the power d_{rosa}) modulo n_{rosa}
- Because only Rosa possesses d_{rosa}, only she can create this ciphertext $C_{\text{rosa signs S}}$. Anyone in possession of her public key (e_{rosa} and n_{rosa}) can verify the signature and obtain the deciphered message S by computing: S = ($C_{\text{rosa signs S}}$ raised to the e_{rosa}) modulo n_{rosa}

Thus to send a message to Rosa, Ray encodes it with Rosa’s public key. Broadcasting a message to 20 people each with individual private keys would require 20 different encryptions.

Pretty Good Privacy (PGP) is a computer program that uses RSA. For example, PGP can encrypt ‘Rosa’ so that it reads ‘457mRT%$354’. The computer can decrypt this message into ‘Rosa’ with PGP. *PGP* generates two keys that belong uniquely to the user. One PGP key is Secret and stays with the user. The other key is Public and is given by the user to his or her secret correspondents. Here is a sample Public Key:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 5.0
mQCNAi44C30AAAEEAL1r6ByIvuSAvOKIk9
ze9yCK+ZPPbRZrpXIRFBbe+U8dGPMb
9XdJS4L/cy1fXr9R9j4EfFsK/rgHV6i2rE83LjOr
msDPRPSaizz+EQTIZi4AN99iBomfLL
ZyUzmHMoUoE4shrYgOnkc0u101ikhieAFje77j
/F3596pT6nCx/9/AAURtCRBbmRyZSBCYWN
hcmQgPGFiYWNhcmRAd2VsbC5zZi5jYS51cz
6JAFUCBRAuOA6O
7zYZz1mqos8BAXr9AgCxCu8CwGZRdpfSs65r
6mb4MccXvvfxO4TmPi1DKQj2FYHY
jwYONk8vzA7XnE5aJmk5J/dChdvfIU7NvVif
=GQv9
-----END PGP PUBLIC KEY BLOCK-----
```

Suppose the Public Key listed above belongs to Rosa and that Rosa e-mails it to Ray. Ray can store Rosa’s Public Key in his PGP program and use Rosa’s Public Key to encrypt a message that only Rosa can read. One beauty of PGP is that Rosa can advertise Rosa’s Public Key the same way that Rosa can give out Rosa’s telephone number. If Ray has Rosa’s telephone number, Ray can call Rosa’s telephone; however, Ray cannot answer Rosa’s telephone. Similarly, if Rosa has Ray’s Public Key, Rosa can send Ray encrypted mail; however, Rosa cannot read Ray’s encrypted mail.

PGP is easy to use. Windows versions allow users to encrypt and decrypt files and send or receive email messages with a *mouse click*. Versions are available for many operating systems. PGP is available to download from the Internet, and many PGP versions are *freeware* (meaning that they are free).

4.5.3 Public-key Infrastructure

Acquiring and using keys requires an infrastructure. Public key cryptography, on its own, is not enough to re-create the conditions for traditional paper-based commerce in an electronic world. Users also need an infrastructure of:

- security policies to define the rules under which the cryptographic systems should operate,
- products to generate, store, and manage the keys, and
- procedures to dictate how the keys should be generated, distributed, and used.

This infrastructure is called, naturally enough, a *Public Key Infrastructure* (PKI). This section explains next the certificates used by PKI, then the management vital to using certification, and finally specific concerns in the healthcare sector.

4.5.3.1 Certificates

PKI uses 'digital certificates' which act like 'electronic passports' and bind the user to his or her public key. Dealing with these certificates involves a:

1. Security Policy,
2. Certificate Practice Statement,
3. Certificate Authority (CA),
4. Registration Authority (RA),
5. Certificate Distribution System, and
6. PKI-enabled Application.

Details of these PKI attributes follow:

1. The security policy defines an organization's top-level direction on information security, as well as the processes and principles for the use of cryptography. Typically, it will include statements on how the organization will handle keys and valuable information, and will set the level of control required to match the levels of risk.
2. A Certificate Practice Statement gives the operational procedures on how the security policy will be enforced and supported in practice. It typically includes definitions on how the CAs are constructed and operated, how certificates are issued, accepted and revoked, and how keys are generated, registered and certified, where they will be stored, and how they will be made available to users.
3. CAs are the digital world's equivalent of passport offices. They issue digital certificates and validate the holder's identity and authority. Digital certificates are most trustworthy when they are vouched for by a trusted CA (Verisign, 2000). CAs embed an individual's or an organization's public key along with other identifying information into each digital certificate and then cryptographically ‘sign’ it as a tamper-proof seal, verifying the integrity of the data within it and validating its use.
4. A RA interfaces between the user and the CA. It captures and authenticates the identity of the users and submits the certificate request to the CA. The quality of this authentication process determines the level of trust that can be placed in the certificates.
5. The Certificate Distribution System distributes certificates in a number of ways depending on the structure of the PKI. For example, the users may distribute certificates themselves, or certificates may be distributed through a *directory service*. A directory service may already exist within an organization or one may be supplied as part of the PKI solution.
6. PKI-enabled applications are applications that support PKI as a secondary service. PKI-enabled applications exist for communications between web servers and browsers, email, Electronic Data Interchange, and credit card transactions over the Internet. A PKI is a means to an end, providing the security framework by which PKI-enabled applications can be confidently deployed to achieve the end benefits.

Enterprises may create their own closed, private certificate infrastructure for internal use. However, public CAs, like those of VeriSign, are also available. All components of a PKI must interoperate, as it is unlikely that they will all be sourced from a single supplier. For example, the CA may have to interface with existing systems, such as directory servers already installed in the organization.

4.5.3.2 Management

Although the principles upon which a PKI system works can be complicated, the management should be simple. The PKI must enable non-technical personnel, such as business administrators, to operate it with confidence. Flexibility and ease of use will seriously impact the return on investment in a PKI system as they affect issues such as training, maintenance, system configuration, integration and of course future growth in user numbers. These issues can make the *cost of ownership* of a PKI far higher than the initial implementation cost and therefore need to be considered in the evaluation phase.

The CA should implement the organization's security policy. The certificate management policy must be accurately reflected in the roles of the CA and RA Operators and certificate users. For example, the CA Operator may decide to delegate the end-user certificate revocation to the RA Operators, while retaining revocation rights over RA Operator certificates.

The security of the CA and RA systems is critical for if compromised, the whole PKI solution will be jeopardized. The PKI must ensure that the CA's private key is held in a tamper-resistant security module and provision made for disaster recovery purposes. Access to the CA and RA should be tightly controlled, e.g. using smart cards to ensure strong user authentication. It should also be possible to configure the certificate management process such that more than one operator is required to authorize certification requests.

4.5.3.3 Healthcare Enterprise Needs

Healthcare providers are a *mobile community* and are typically affiliated with multiple institutions. In the absence of an extensible infrastructure, the care provider could be faced with numerous identities, accounts, and technologies across these multiple environments making a complex environment for the end-user, and potentially impacting the time-sensitive nature of access efficiency. One of the primary goals of the security infrastructure, therefore, is to enable a single professional certificate to be used across all healthcare applications, institutions, and across multiple security technologies.

Several commercial entities exist today that provide CA Services. However, these services are insufficient in the healthcare domain, as they do not certify the professional credentials of an individual. Healthcare applications must be able to ascertain not only the identity of an individual, but the individual's role, specialty, and the status of *professional credentials*. Furthermore, the certificate policies of the Healthcare Domain CAs must be consistent with the extensive validation processes that are currently conducted to establish trust and permissions that allow a clinician to practice medicine. Such policies must be consistent throughout the chain-of-trust relationships.

Many healthcare facilities are considering operating their own CA. While this option is sufficient for a self-contained operation, it is not scaleable for the level of *interoperability* required by healthcare. Healthcare transactions regularly involve unaffiliated entities. Under such a scenario, each organization must negotiate trust for the unaffiliated certificates. This negotiated trust must then be configured into each software product relying upon the certificates along with the appropriate access control. Most Certificate-aware software does not currently support multiple 'certificate mappings' and requires complex integration efforts for each CA recognized. Participating in a common CA model simplifies these relationships and configuration efforts. However, where a common CA does not exist, the use of automatic or semi-automatic certificate mappings is useful when the volume of traffic is high.

4.5.4 Virtual Private Networks

To provide healthcare professionals with the ability to connect to a healthcare organization's computing resources regardless of their location, a hospital might deploy a reliable and scalable *remote access* solution. Typically, the healthcare organization might either

- have an internal information systems department buy, install, and maintain corporate modem pools and a private network infrastructure or
- pay another company to maintain modem pools and a telecommunications infrastructure.

Neither of these solutions is best in terms of cost, reliability, flexible administration and management, and demand for connections. Therefore, it makes sense to find a middle ground where the organization either supplements or replaces their current investments in modem pools and their private network infrastructure with a less expensive solution based on Internet technology. By exploiting the Internet, healthcare organizations can increase accessibility economically (Microsoft, 1998).

A Virtual Private Network (VPN) connects one network over another network. VPNs accomplish this by allowing the user to tunnel through the

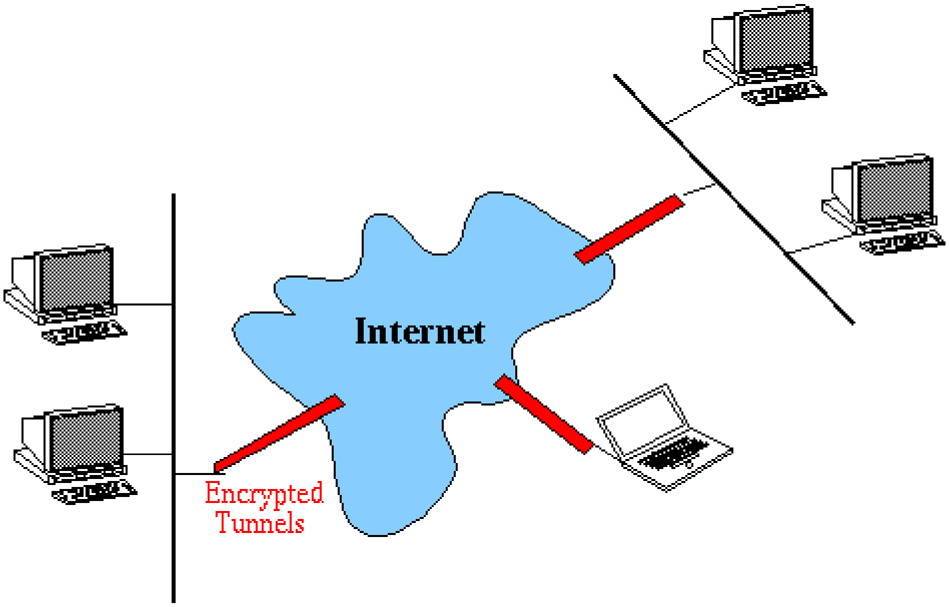


Figure "VPN": In this schematic of Virtual Private Network workstations and a laptop are in a virtual network that use encrypted tunnels through the Internet.

Internet or another public network in a manner that lets the tunnel participants enjoy the same security and features formerly available only in private networks (see Figure "VPN"). At a minimum, a VPN should provide:

- *User Authentication***.** The solution must verify a user's identity and restrict VPN access to authorized users. In addition, the solution must provide audit and accounting records to show who accessed what information and when.
- *Address Management*. The solution must assign a client's address on the private net, and must ensure that private addresses are kept private.
- *Data Encryption*. Data carried on the public network must be rendered unreadable to unauthorized clients on the network.
- *Key Management*. The solution must manage encryption keys for the client and server.

An Internet VPN solution takes advantage of the broad availability of the worldwide Internet.

Tunneling is a technique for transferring data from one network X over another network Y. The data to be transferred can be the packets of protocol X. Instead of sending a packet simply as it is produced by the originating node, the tunneling protocol encapsulates the packet in an additional Y header. The Y header provides routing information so that the encapsulated data can traverse the intermediate Y network. The logical path through which the encapsulated packets travel through the intermediate network is called a *tunnel*. Once the encapsulated packets reach their destination on the intermediate network, the packet is unencapsulated and forwarded to its final destination. Tunneling includes this entire process (encapsulation, transmission, and unencapsulation of packets).

Because the Internet facilitates the creation of VPNs from anywhere, networks need strong security features to prevent unwelcome access to private networks and to protect private data as it traverses the public network. User Authentication and Data Encryption are already supported. In the future VPNs will support Public-Key Infrastructures and Registration Authorities.

VPNs need to store per-user information in a directory service, so that administrators and applications can add to, modify, or query this information. Each access or tunnel server could maintain its own internal database of per-user properties, such as names, passwords, and dial-in permission attributes. However, because it is administratively unsupportable to maintain multiple user accounts on multiple servers and keep them simultaneously current, most administrators use a master, centralized account database.

4.5.5 Electronic Signatures

Signatures have long been a part of the process of documenting healthcare. They serve a practical purpose of identification. In the patient record, signatures are used to identify the person who made an entry, to indicate that a review of an entry has been made, and to designate approval of an entry (CPRI, 1996c). HIPAA calls for DHHS to adopt standards for electronic signatures with respect to transactions between providers and payers. However, transactions between providers and payers are not traditionally signed per se. Nevertheless, electronic signatures are important in many other healthcare transactions.

4.5.5.1 Purpose

There are four basic purposes of a signature:

- It serves as evidence of the *identity* of the signer.
- There is a *ceremonial benefit* - calling attention to the legal significance of the act of signing.
- A signature expresses approval or *authorization* - that the substance of the writing has a legal effect.
- Finally, a signature provides a sense of clarity and *finality* to the writing.

For example, the signature of a medical student on a report of a history and physical examination may denote that the student has obtained all the information possible at that time. The signature of the attending physician on that same document may denote approval afforded by review of its content and the finding that it is complete and accurate. These purposes of *signature* are the foundation for electronic signature policies. The meaning behind the signature serves to justify the importance of adherence to a signature policy.

As the means of documenting entries in patient records and creating signatures are fundamentally being changed by computerization, formal requirements in law need to be updated accordingly. To achieve the basic purposes of signatures in a computer-based environment, the system must provide for the following effects:

- the system must provide good evidence of who participated in the transaction (*user authentication*),
- the system must provide good evidence of the substance of the transaction and make it impractical to falsify or alter (*data origin authentication*),

- the system must provide for an affirmative act to serve the *ceremonial* and approval functions of a signature, and
- the system should provide the greatest possible assurance of authenticity and validity (*nonalterability*) with the least possible expenditure of resources.

Electronic signature technology may surpass traditional handwritten signatures in yielding some of the desired effects of signatures.

4.5.5.2 Laws

From a legal perspective, handwriting one's name on paper has been the principal means of signature for centuries. In addition, the legal concept of signature recognizes, in many cases, not only a handwritten name but also any mark made with the intention of authenticating the marked document. There are legal requirements for signatures. State licensure statutes may be the most restrictive, with some states still having 'quill pen' laws on the books requiring handwritten signatures. An increasing number of states, however, are promulgating requirements for healthcare providers for electronic signature of patient record entries. For instance, the Illinois Hospital Licensing Requirements permit use of electronic signatures or computer-generated signature codes for the purpose of authenticating medical records, if the hospital employing them complies with specific procedural requirements, including adoption by the hospital's board and medical staff of policy permitting such authentication and including adequate safeguards to ensure confidentiality with specified procedures to limit access to authorized users and ensure that user identifiers are not shared or misused. Separate authentication of each report generated is required.

In determining what constitutes an appropriate electronic signature for an organization, the environment in which the signature will be applied and all applicable accrediting, licensure, and other legal (federal and state) requirements that apply to the organization must be considered. The signature policy must comply with the Joint Commission on Accreditation of Healthcare Organizations *(JCAHO*) standard for hospitals which requires that

> the hospital has a system in place to assure that only authorized individuals make entries into medical records; identify the date and author of every entry in the medical record; and enable the author to authenticate an entry to verify it is complete, accurate, and final …. [Hospitals should] establish policies and mechanisms to assure that only an author can authenticate his or her own entry. Indications of authentication can include written signatures or initials, rubber-stamps, or computer 'signatures' (or key sequences).

The 'Medicare Conditions of Participation' require that there be a 'system of author identification' that 'ensures the integrity of the authentication and protects the security of all record entries'. Entries must be dated, and the authors of each entry must be identified and must authenticate their entries. Authentication may include "signatures, written initials, or computer entry."

In June 2000, the "Electronic Signatures in Global and National Commerce Act" became law. The law applies to any agreement affecting interstate commerce (NAMIC, 2000). The law does allow states to have different rules but only so long as they are consistent with the federal law. This Act should support the enactment of electronic signatures for healthcare as dictated by HIPAA. The Act defines the term *electronic record* as a writing, document, or other record created, stored, generated, received, or communicated by electronic means. The term *electronic signature* means a signature in electronic form, attached to or logically associated with an electronic record, that

- is intended by the parties to signify agreement to a contract or agreement;
- is capable of verifying the identity of the person using the signature; and
- is linked to the electronic record in a manner that prevents alteration of the record after signature.

Relating to the specifics of technology, the Act has chosen the open market approach: free markets and self-regulation, rather than government standard setting or rules, will govern the development and use of electronic records and electronic signatures.

4.5.5.3 Authentication

Electronic signatures include digital signatures and other notations of signatures such as those based on biometrics, those which use a token of some kind, or those which have been generated in a system secured minimally with a user identification and a password for access. This may extend to inclusion of addressing notations such as digitized images of paper signatures, typed notations such as s/John Doe, or even 'from' headers in electronic mail (ABA, 1996).

The integrity of the electronic signature depends on its representing the authentication of one individual and only that individual. This is done by limiting access to the computer software program that assigns or creates the signature mechanism. The software must be designed to insure the signature is unique to an individual and cannot be assigned to another individual. To accomplish this, electronic signature software programs most commonly rely on a user *password*.

A digital signature relies on cryptography. Digital signature verification is the process of checking the digital signature by reference to the original message and a public key, and thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key. To sign an entry, the signer identifies what is to be signed, the signer's software computes a code unique to the message, and the signer's software transforms the code into a digital signature by reference to the signer's private key. The resulting digital signature is unique to both the message and private key used to create it. To verify a digital signature, the verifier uses the public key to check whether the digital signature was created using the corresponding *private key*. This verification process indicates that the digital signature was created using the signer's private key because only the signer's public key will verify a signature created with the signer's private key, and that the message was not altered since it was signed because of the computational match.

Authentication can be tied to a person’s body:

- *Biometric user authentication* identifies a human through a measurement of a physical feature of the individual.
- *Behavioral action user authentication* identifies a human through a measurement of a repeatable action of the individual.

Some administrators and practitioners are attracted to the possibility of biometric or behavioral authentication because it obviates the need to remember keys or passwords. These techniques vary in their reliability, expense, and social stigma; and the degree to which they are prone to error (i.e., failure to recognize a legitimate user or falsely identify an illegitimate user).

The audit trail for signatures depends on the documents being signed. For *medical records*, policies are elaborate. The computer system on which a patient record is maintained should record the date and time of each entry to a record so that the time of the entry can be shown in court. The computer should also record the identity of each person who makes an entry. When an error is corrected in a patient record, the system should preserve both the original entry and the correction. The identity of the person making each correction and the date and time of correction should be recorded by the computer in the same manner as this information is recorded for original record entries. A procedure should be in place that requires all users of electronic signature to certify in writing that they understand the implications of the identifier and state that they will be the only one that will use the identifier.

4.5.6 Example PKI

Several healthcare public key infrastructures (PKIs) have been developed. One such PKI, called CHIME-Trust, started in 1993 in Connecticut. CHIME-Trust well illustrates the technology and management issues germane to PKI. CHIME-Trust is managed by CHIME, an affiliate of the Connecticut Hospital Association. CHIME has established a trusted third-party service, which

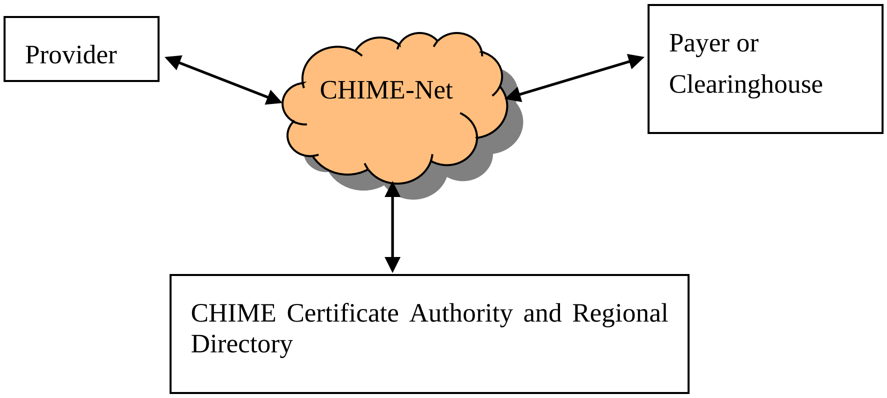


Figure “CHIME Architecture”: The connections among the Providers, Payers, and CHIME are depicted. Secure Socket Layer communication occurs among all parties.

establishes a common chain-of-trust among healthcare organizations, enabling HIPAA compliant communications of patient care data (Reed-Fourquet, 2000).

4.5.6.1 History of CHIME-Trust

In 1993 multiple efforts were under way within the state of Connecticut to establish connectivity for isolated communications among providers and between providers and payers. Specifically, this connectivity was intended to enable applications such as EDI for the eligibility and claims management process. Other applications were electronic mail and on-line access to a shared database of patient discharges. With this as a basis, the potential benefits of establishing a health information network for the provider and payer community were examined. A number of potential benefits to provider connectivity were identified including the ability to:

- share clinical information,
- transfer patient records,
- enable an emergency response system, and
- exchange electronic mail.

Based upon the benefits analysis, in 1994 the providers initiated a statewide health information network. This network was designed to establish a connection from each provider to a central router at CHIME, and a connection from *CHIME* to the Internet. This network has grown since its inception to include over fifty institutional connections including acute care hospitals, rehabilitation facilities, home healthcare providers, and long-term care facilities. The network is further extended through community-based connectivity efforts to include physicians, pharmacies and clinics.

Given that much of the benefit to this connectivity was to be attained by sharing and communicating confidential health information, the network infrastructure needed to be secure. In 1999 CHIME built a scaleable security infrastructure through the establishment of a *Healthcare Public Key Infrastructure*. This Trusted Third-Party Service incorporates a distributed registration process and a healthcare directory that includes the enrollment of users into roles. This infrastructure enables encryption, digital signature, non-repudiation, identification, authentication, and role-based access control.

4.5.6.2 Architecture

The statewide Healthcare Domain, Trusted, Third-Party Services architecture includes three primary components:

- Certificate Authority (CA),
- Registration Authority (RA), and
- Lightweight Directory Access Protocol (LDAP) directory server.

All three of these components are extensible and described further next:

- CHIME serves as the root CA for the healthcare providers and institutions within Connecticut. A large community network may wish to maintain its own subordinate CA which would be implemented as a branch of the tree that begins in the CHIME CA root. CHIME issues certificates to both healthcare professionals and organizations. Health information systems must be able to identify access to patient records by individual. Information may be sent to an organization for processing by one of many possible providers. Multiple certificate assurance levels are defined based upon the level of protection supported by the recipient. The highest level of certificate is intended to have a level of certainty sufficient to *practice medicine*. The lower level certificates serve to authenticate users to less sensitive health applications and to exchange communications, but may not be used for the delivery of medical orders. Certificates for signing and for authentication may be issued directly through CHIME or through one of the subordinates within the hierarchy. The Trusted Third-Party architecture also allows for this statewide CA to become a direct subordinate to a higher authority, such as a national entity.

- To sufficiently insure the credentials of the providers, RAs are at CHIME and at major organizations. The RAs are closely linked with member healthcare organizations. Within most hospitals, these processes are distributed between the *human resource area* for permanent staff and *medical staffing offices* for credentialed independent practitioners. There are several processes already in place to insure licensing credentials for all practitioners in the organization. The RAs tap into this process thereby insuring that proper controls and checks are in place, while minimizing the impact and cost to security implementation. An integral component of these assurances is validation of current licensing status with state and federal licensing boards.

- Another important component of the Trusted Third Party infrastructure is the LDAP directory server. This server has been augmented from the standard object model so as to include healthcare specific attributes as a part of the user registry. Certificates are associated with users registered in the directory. Users are also assigned to roles as defined through ASTM security standards. The directory configuration allows users to hold multiple roles at one or many institutions as is typical of the healthcare environment. This *user registry* may be distributed and replicated among the member locations.

Integration of the CA with the LDAP Directory Server supports the type of Enrollment and Registration infrastructure that will be required to appropriately identify users and assign privileges within the system. The CA and LDAP Directory Server provide a foundation for the registration of user roles in Role-Based Access Control.

In addition to the registration of people via the RA, entities need to be registered. To certify entities one must :

- validate against business incorporation records,
- check with the State Department of Health to insure that the organization is licensed for the appropriate category of medical practice, and
- verify that the organization is in good standing with the General Services Administration and the Office of the Inspector General.

More than the Human Resources Department is required to perform this certification.

For eligibility inquiries, CHIME provides a web-based interface to the end-user to assist in capturing the eligibility inquiry variables. This interface is secured through Secure Socket Layer-3 whereby the web server is authenticated to the client through a healthcare server certificate. The client is similarly authenticated to the server through presenting an individual certificate, typically an employee certificate. This certificate, issued on a smartcard by CHIME, is used to identify an entry within the community LDAP directory. The directory is then checked to identify the roles assigned to the individual. Role-based access control is thereby used to restrict access to the *eligibility application* users who are assigned the role of *Admission Clerk*. The actual eligibility inquiry is conducted on behalf of the user over a private network connecting the Web Server application to the provider of the eligibility information (see Figure “CHIME Architecture”).

4.5.6.3 Services

CHIME provides a number of services as a Trusted Third Party. These core CA services include management of Certificate Revocation Lists, Certificate Distribution, and time stamping. Some of these processes are unique to the healthcare professional certification environment, such as Credential Verification Process. Other services, such as education, assist organizations in implementation and integration of the Trusted Third Party infrastructure.

The Trusted Third Party Services enrollment entails several steps. The user first contacts a certified registrar in order to initiate the credential verification process. This typically takes place as an integral part of the staffing process. This *registrar* examines the identification and credential documentation of the user, insures directory registration of the user, and attests to the relative attribute and credential information. The user’s public and private key is then generated, and the certificate request is issued by the registrar to the CA.

4.5.6.4 Organizational Issues

A number of organizational issues need to be addressed in the process of configuring the CHIME-Trust Infrastructure. Inappropriate management of the CA can compromise the integrity of the infrastructure. As a result, strict physical access controls and measures are implemented. This involves coordination with building management personnel. Similarly, personnel responsible for management of the CA need separation of duties and multiple roles to execute certain sensitive functions. This imposes a level of training, background checking, and password protection not typically managed within the healthcare arena. Legal council was involved for changes to personnel policies for CHIME-Trust staff, as well as for contract development. Local RAs bring to bear additional organizational issues. Instituting a RA in this environment entails either the addition of *job responsibilities* to existing job functions, or a new job function.

Education is critical to the successful deployment of the Healthcare PKI. Numerous educational programs have been conducted for technical personnel, decision makers, and end users. The Health Services Librarians have also worked with CHIME to develop a ‘train-the-trainers’ program and to develop end-user training programs.

Change management is needed to develop an operational healthcare PKI. As an infrastructure, this involves management of change not only in the organization providing the service, but also in all participants in the chain-of-trust. This includes changes to operations, personnel management, physical security, and technology. Any organization interested in providing such a service should be sure to participate in *community-based efforts* so as to minimize the learning curve, and to maximize interoperability.

4.5.7 Example Internet Transactions

DHHS's Health Care Financing Administration (HCFA) established in 1998 Internet security requirements. In June 2001 DHHS changed the name of HCFA to Centers for Medicare and Medicaid Services; however in this section the name HCFA is used. HCFA established the basic security requirements that must be addressed for use of the Internet to transmit sensitive HCFA information. The term 'sensitive HCFA information' refers to data which, if disclosed, could result in harm to the agency or individual persons (HCFA, 1998) and includes:

- all individually identifiable data held in systems of records and
- payment information that is used to authorize or make cash payments to individuals or organizations.

HCFA's Internet policy covers all systems which interface with the Internet to transmit sensitive HCFA information.

User authentication or identification must be coupled with encryption and data transmission processes to be certain that confidential data is delivered only to authorized parties. There are a number of effective means for authentication or identification which are sufficiently trustworthy to be used. The generic model is that the encryption process takes place prior to information being presented to the *Internet* for transmission, and the decryption process after reception from the Internet (see Figure "Internet Connections"). A large organization would be very likely to have the Internet Server on its premises, while a small organization might have only the Internet Client on its premises with the Internet Server at an Internet Service Provider. The use of multiple authentication or identification approaches is permissible. The approach provides maximum user flexibility within the allowable limits of security and manageability. A complete Internet communications implementation must include adequate encryption, employment of authentication or identification of communications partners, and a management scheme to incorporate effective password/key management systems.

In the HCFA Internet Policy, *authentication* refers to generally automated and formalized methods of establishing the authorized nature of a communications partner over the Internet, generally called an 'in-band process'. Acceptable authentication approaches include:

- formal CA-based use of digital certificates,
- locally-managed digital certificates,
- self-authentication, as in internal control of symmetric private keys, and
- tokens or 'smart cards'.

Identification refers to less formal methods of establishing the authorized nature of a communications partner, which are usually manual, involve human interaction, and do not use the Internet data channel itself, but another "out-of-band" path, such as the telephone or US mail. Acceptable identification approaches include:

- telephonic identification of users,
- exchange of passwords and identities by U.S. Certified Mail or bonded messenger,

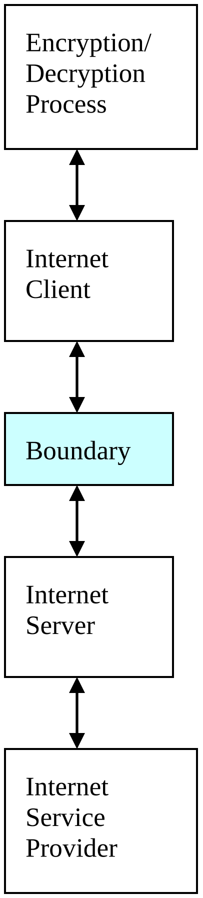


Figure "Internet Connections**":** The 'Boundary' on the diagrams represents the point at which security control passes from the local user. It lies on the user side of the Internet Server and may be at a local site or at an Internet Service Provider depending upon the configuration. The diagram does not intend to dictate how encryption is to be accomplished, only that it must take place prior to introduction to the Internet.

- direct personal contact exchange of passwords and identities between users, and
- tokens or 'smart cards'.

Acceptable encryption is either software-based or hardware-based. Software-based encryption could be:

- Secure Sockets Layer Version 3.0,
- S-MIME implementations of encryption in the e-mail layer,
- in-stream encryption implementations in the transport layer, such as pre-agreed passwords, or
- offline encryption/decryption of files at the user sites before entering the data communications process.

Hardware-based encryption is likely to be reserved for the largest traffic volumes at a very limited number of Internet sites.

All organizations must detail their methodologies and protective measures, if they decide to use the Internet for transmittal of sensitive HCFA information. HCFA reserves the right to audit any organization's implementation of and adherence to the requirements. This includes the right to require that any organization utilizing the Internet for transmission of HCFA sensitive information submit *documentation* to demonstrate that they meet these requirements. Organizations desiring to use the Internet for transmittal of sensitive HCFA information must notify HCFA of this intent.

4.5.8 Example Record Security

Careweb provides secure Internet access to clinical data at the Beth Israel and Deaconess Hospitals. The core elements of Careweb were designed in 1978 -- when it was the system of Beth Israel Medical Center. Upon the merger with Deaconess Hospitals, Careweb was developed as a middleware application that created object-wrapping around the merged organization's diverse legacy systems.

4.5.8.1 Security Architecture

The clinical data at the Beth Israel Hospital is stored in a comprehensive, custom-built system composed of 28,000 programs. The clinical data at the Deaconess is stored in a Sybase clinical data repository. CareWeb site servers operate behind the Web servers of each hospital and create a link to the underlying legacy systems at each institution. In a typical session a healthcare provider on a standard Web browser creates a query for information by specifying a patient identification. This information is submitted to a Consolidator. The Consolidator generates a HL7 request for information to both the Beth Israel and Deaconess site servers (see Figure "CareWeb Architecture"). The *site servers* return HL7 encoded demographics, problems, medications, allergies, notes and visits. The Consolidator interprets the incoming messages and creates a single unified presentation which it sends back to the healthcare provider as a series of Web pages.

The authenticity of each user is checked with Security Dynamics SecurID hardware tokens (see Figure "SecurID"). These tokens are small, handheld devices containing microprocessors that calculate and display unpredictable codes. These codes change at a specified interval, typically 60 seconds. Each user accessing CareWeb begins a session by entering a username, a memorized personal identification number (PIN) and the currently displayed password from the *SecurID* device. This information is transmitted to a security server which authenticates the user and verifies that the correct password was entered. The security server compares the user-entered password with its knowledge of what password should have been entered for that 60 second period. Once a password is verified, the user is authenticated for the duration of the web session or 15 minutes, whichever is less.

Figure "SecurID": This token from Security Dynamics is used for authentication in CareWeb.

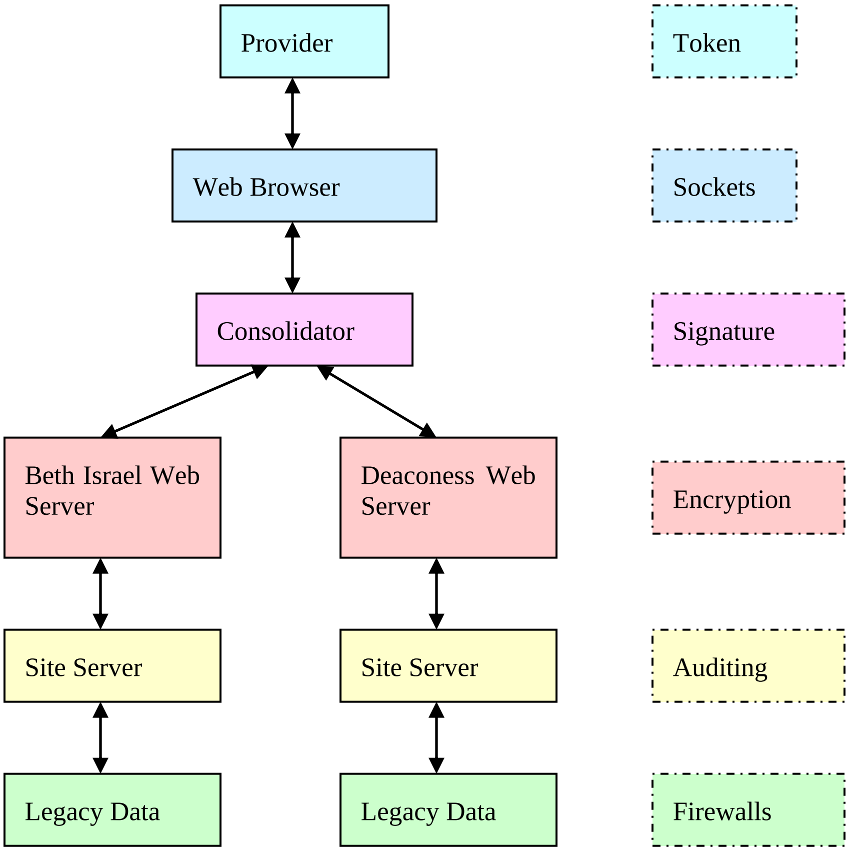


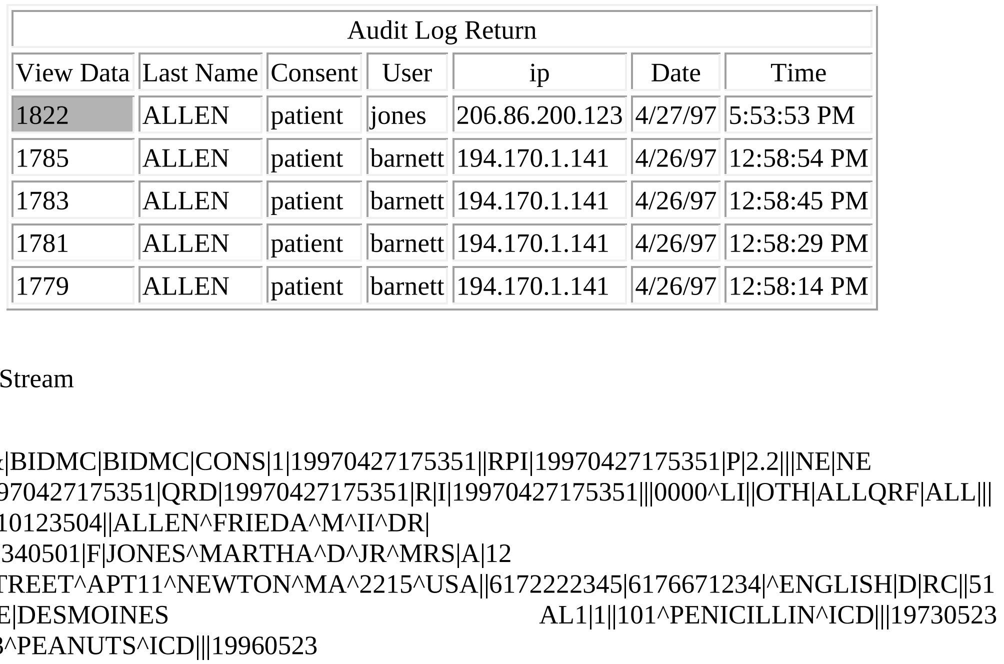
Figure "CareWeb Architecture": The communications paths are shown on the left and the security features on the right.

Access validation is related to roles. In addition to storing encrypted username and password information, the security cookie contains the job role of the user. Displays of healthcare information are generated dynamically to deliver healthcare information based on the *role* indicated by the cookie.

The existing legacy systems at the Beth Israel and Deaconess hospitals limit Internet transactions from outside the institution with routers and firewalls. To create security between a browser running on a user's desktop and the Consolidator web server, the Secure Sockets Layer protocol is used. The SecurID username and password are only exchanged after an encrypted connection has been established by the Secure Sockets Layer.

Encryption of public network transmissions supports communications between the Consolidator and site servers. RSA public key encryption is used for key exchange, session key cryptography for data exchange, and digital signature for confirmation of the veracity of the Consolidator request. Each Consolidator request is signed with the RSA private key of the Consolidator. This message is sent to the site server which has a record of the Consolidator's public key. The site server validates the *digital signature* through standard hashing and signature verification methods. The site server then generates a session key which it encrypts using the Consolidator's public key. The site server also encrypts all outgoing HL7 information using the session key. The encrypted session key and encrypted data are sent back to the Consolidator. The session key is decrypted using the Consolidator's private key. The encrypted HL7 message is decrypted using the decrypted session key. All decrypted site server messages are consolidated into a single web page and returned to the original requesting browser over the Secure Sockets Layer.

Other security measures include virus checking and security logs. Virus checking programs are in place on all CareWeb Systems and are executed daily by a



Audit Log Return

View Data	Last Name	Consent	User	ip	Date	Time
1822	ALLEN	patient	jones	206.86.200.123	4/27/97	5:53:53 PM
1785	ALLEN	patient	barnett	194.170.1.141	4/26/97	12:58:54 PM
1783	ALLEN	patient	barnett	194.170.1.141	4/26/97	12:58:45 PM
1781	ALLEN	patient	barnett	194.170.1.141	4/26/97	12:58:29 PM
1779	ALLEN	patient	barnett	194.170.1.141	4/26/97	12:58:14 PM

HL7 Data Stream

```
MSH|^~\&|BIDMC|BIDMC|CONS|1|19970427175351||RPI|19970427175351|P|2.2|||NE|NE
SA|AA|19970427175351|QRD|19970427175351|R|I|19970427175351|||0000^LI||OTH|ALLQRF|ALL|||
|A^1PID|||10123504||ALLEN^FRIEDA^M^II^DR|
SMITH|19340501|F|JONES^MARTHA^D^JR^MRS|A|12
MAPLESTREET^APT11^NEWTON^MA^2215^USA||6172222345|6176671234|^ENGLISH|D|RC||51
2341234|||E|DESMOINES                          AL1|1||101^PENICILLIN^ICD|||19730523
AL1|2||203^PEANUTS^ICD|||19960523
```

Figure "Audit Trail": An example return for a search on the audit trail for the patient Allen is shown. The column labels are in the first row. To view the actual HL7 data returned in response to the query,

system daemon. On the Consolidator, a security log lists all SecurID tokens used, all failed login attempts, and all changes made to the token database. *User logs* show all users who have entered the secured machine room and logged onto the Consolidator machine.

4.5.8.2 Auditing

Auditing is provided at the level of the specific patient queried and the individual menu selections used. An *Auditing Consolidator* queries the audit trails of the individual hospitals. It produces a consolidated report showing all flows of information about the patient for all institutions (see Figure "Audit Trail"). Not only does the 'Auditing Consolidator' display a multi-institutional audit log, it can optionally display the actual healthcare data which was originally requested. In this fashion, patients can be shown an exact duplicate of the information that was displayed to healthcare providers. The audit module is entered by requesting a patient name and providing again a username, PIN, and SecurId.

The *audit trail system* allows for identification not only of each individual clinician or staff member who has requested a patient's medical record, but the piece of the medical record that was seen. Further, the system makes it possible for employees who have been patients of the organization to view the full audit trail on their records online. Few organizations have these audit capabilities. However, the HIPAA security regulations call for such auditing.

By and large, the threat to patient confidentiality comes from inappropriate use by authorized users (Hagland, 1998b). The vast majority of intrusions into electronic patient records come from clinicians and staffers at provider organizations -- a nurse who is a neighbor, a doctor who is a colleague, and a records administrator who is a friend. The ability of users of the system to audit the look-ups of their own records is a strong *deterrent to intrusion*.

4.5.9 Review Questions

1. What is a trusted computing base and why is it important?
2. What is the meaning of a one-way function and how does it allow for public and private keys in the RSA Algorithm?
3. What is the role of Certificate Authorities in a Public Key Infrastructure?
4. Why might a Virtual Private Network be used by a healthcare organization?
5. Explain how an electronic signature works.
6. Describe the architecture of the CHIME PKI.
7. Where does HCFA expect the encryption to occur and where should the Internet Service

Provider be relative to the boundary and how is this different for a small versus a large organization?

8. How does Careweb use the SecurID?

9. Imagine a small doctor's clinic that is not computerized but decides to become computerized. What would be the extra cost, if any, in terms of hardware and software of computerization that supported public key encryption versus computerization that did not have such security protection. (Project Question)

10. The CareWeb system as presented in the text connects healthcare provider staff to clinical information at various locations of the CareGroup integrated delivery network. CareWeb also allows patient access. Would the conditions for patient access be different? (Project Question)

4.6 Conclusion

Healthcare organizations have insecure information systems. The Government Accounting Office has published its assessment's of government information security, and the results for government healthcare organizations show a consistent failure to appropriately implement information security.

4.6.1 Summary

The Security NPRM applies to each healthcare entity engaged in electronic maintenance or transmission of health information. Each organization must assess potential risks and vulnerabilities to the individual health data in its possession in electronic form, and develop, implement, and maintain appropriate security measures. Importantly, these measures must be documented and kept current.

Security has 3-levels:

- one level is people,
- another level is computer models, and
- the third level is technical mechanisms.

Computer security models themselves are typically decomposed into confidentiality, integrity, and availability models:

- Confidentiality is the most commonly discussed aspect of security and involves giving access to information only to appropriate people.
- Integrity means that information is only modified by appropriate people.
- Availability means that the information resources are reliably present when needed.

Availability is typically captured in a contingency plan that specifies how to recover computing capability when the primary resource becomes somehow non-functional.

As of this writing the security regulations from DHHS are still 'Notices of Proposed Rule Making'. If and when the NPRM should be finalized, organizations would have two years to comply with the Final Rule. The cost of implementing security regulations is difficult to predict since the current status needs first to be assessed and the means to accomplish security are varied.

4.6.1.1 Life Cycle

A real-world or human security policy begins with awareness. Awareness at the executive level is required. Information systems consultants might initiate awareness training.

Hand-in-hand with the need for awareness is the need to understand the gap between an organization's current security situation and the situation that would be desirable. Tools exist to guide the gap analysis. For instance, the Government Accounting Office has a freely available manual for assessing the gaps in information security in an organization based on the government standards for security. This GAO manual can be tailored to deal with the HIPAA security regulations. The 'North Carolina Healthcare Information and Communications Alliance' has developed about 500 questions that are specific to the HIPAA security regulations and has placed those questions in an interface to a Microsoft Access database so that people answering the questions can later see their answers through various database queries. Designing some *gap analysis tool* is fairly straightforward but collecting the appropriate data and then doing something useful with the data is not straightforward.

One natural step to take after a gap analysis is a risk analysis. The risk analysis looks at the potential costs to the organization of each of its security vulnerabilities. Then the costs to remedy each vulnerability or gap are estimated. Finally, a plan is made for the gaps to close based on a comparison of the costs of the various remedies versus the costs of the various vulnerabilities.

To implement security, the Security NPRM says that each organization should have a security officer. In a small organization, this *role* might be filled by a person with multiple other roles, while in a large organization, multiple people might discharge the Security Officer functions. Staff throughout an organization need to support the security work.

Training is vital to compliance with security regulations. All staff need to know about simple things such as changing passwords. Senior staff need specialized training appropriate to their responsibilities. This training might typically occur through the traditional channels of training in the organization, but opportunities exist to exploit the Internet in this training.

Compliance with DHHS's security regulations is largely a matter of working in a way that pays attention to security. In this sense implementing the compliance is similar to implementing the compliance for the international quality standard ISO 9000. ISO 9000 says that an organization should be clear about its objectives and should work in a way that regularly and consistently documents that it is trying to reach its objectives. The DHHS security regulations specify common approaches to security and are general. Each organization will have to make its own specific security objectives. DHHS requires that organizations consistently work toward their security objectives.

4.6.1.2 Real-world Policy

The DHHS security objectives focus on access control. Guidelines for a 'people policy' and a 'machine policy' are given. On the people side, the rules call for appropriately supervising staff to include closing accounts for terminated employees and properly granting access to new employees. Agreements with third parties need to be controlled with 'Chain of Trust' agreements.

Healthcare organizations typically want to perform like their peers -- to a level consistent with the performance of peer organizations. This book provides an example of a single clinic that has a 'people policy' focused on keeping medical records in the clinic not visible to patients or visitors. The '*people policy*' for a much larger organization is also illustrated and has diverse parts to account for treatment facilities, diagnostic facilities, paper records, electronic records, and so on.

Two organizations particularly advanced in their handling of security are Kaiser Permanente and the Mayo Clinic. Both organizations have shared publicly some of their security policies. *Kaiser Permanente* identifies major roles of user, manager, and trustee. Trustees make specific policy that managers implement for users to follow. Data is classified into the following categories: public, internal, confidential, and registered confidential. Policies exist that are specific to the category of the information and the role of the individual. The Kaiser policy also specifies how the local area network is to be accessed and how fax and email are treated. Kaiser's preparation for HIPAA compliance includes an elaborate organizational structure with a HIPAA Program Director coordinating the work of a HIPAA Business Director, a HIPAA Healthcare Director, a HIPAA Information Technology Director, and others who in turn work with corresponding regional directors to assure the appropriate plans and the execution of those plans throughout Kaiser. The *Mayo Clinic* approach is similar to that of Kaiser.

Complying with the Security NPRM is more a matter of *culture* than of technology. Most of the security abuses occur by employees of a organization who go beyond their intended task and breach security. For instance, a technician who normally does tape backups may create an extra copy for personal use. Preventing this breach requires training and quality control and depends on people more than on technology.

4.6.1.3 Computer Models

In the crudest case a computer, confidentiality model specifies for every person and every item of information whether or not the person can read or modify the information. Such a model is impractical for more than a few people and few items of information. So *security models* label the information and label the people and develop rules that relate information labels to people labels. The approaches that emphasize the labeling of information are sometimes called information flow models and are typical of what the military has emphasized in the classification of information according to its confidentiality or secrecy level. The people-based approach emphasizes roles.

Roles-based access control is a popular, modern approach to implementing security in large healthcare information systems. A simple classification of roles and *access privileges* might say that a patient see all information for the patient, the doctor sees all information, and the administrative staff see patient name and identification number. Role-based access control is typically extended to handle hierarchies of roles in which attributes are inherited from one role to a descendant role. The general goal in implementing role-based access control is to be able to describe the work of the organization in terms of roles and then to simply move people to and from roles as is necessary.

In addition to confidentiality, integrity, and availability, other concepts are useful in discussing computer security. The DHHS security regulations address authentication, authorization, and audit:

- authentication is determining who made a request;
- authorization determines whether a given individual has permission to perform a certain act; and
- audit keeps a record of acts performed.

Authentication typically occurs with userids and passwords but more sophisticated methods are possible, such as fingerprints.

The Patient Centered Access to Secure Systems Online (PCASSO) is a sophisticated role-based access control system that has been well-accepted by patients but less so by doctors. The system requires users to be associated with roles and gives them privileges based on their roles. The challenge of getting such systems to work smoothly with healthcare professionals is that the model of the workflow needs to accommodate the very flexible work patterns in a healthcare team.

DHHS provides an extensive example of how a *small healthcare provider* could adequately implement security. The example emphasizes low-cost, common sense approaches to managing the flow of information. In an office with just one person, a role-based access control system is unnecessary.

Generally, security is a matter of who does what when with information – this is workflow management. The popular concept of knowledge management is an instance of workflow management because the knowledge comes from and goes to the workflow -- knowledge is valuable to the extent that it impacts the work. Even ecommerce is intimately related to workflow. The goal of *ecommerce* in the first instance is to exchange money for products or services online but this is just part of an ongoing flow of activity or work.

4.6.1.4 Mechanisms

A Trusted Computing Base depends on a complex network of hardware and software operating together in such a way that entry into the system in one place cannot lead incorrectly to access anywhere else. Assuring such a Trusted Computing Base is very difficult and traces back to the originators of the software not having left any secret traps in the code. Building and maintaining a *Trusted Computing Base* depends on sound practices of software and hardware engineers both in development and maintenance of systems.

When a message is sent from one person to another across a computer network, the message's confidentiality can be increased by encrypting the message. Cryptography is the enciphering and deciphering of messages in *secret code*. The crude form of such an encryption is illustrated by 'Pig Latin' with adding the suffix 'ay' to every word. One challenge of encryption is to get the key to the recipient in such a way that no one else can intercept the key. To address this problem the public-key encryption method was developed. With public-key encryption, each person has a private and a public key. When Rosa wants to send Ray a secret message she uses Ray's public key to encode Rosa's message to Ray. When Ray receives it, he decodes it with his private key.

The challenge with public-key cryptography is partly one of managing the distribution of public and private keys. When a person says he is a doctor with certain credentials and gives his public key, how does someone else know whether or not that person is who he claims. Public Key Infrastructures support the distribution of keys and include a certificate authority. To get the original public and private keys from the certificate authority, the doctor needs to verify his credentials to the certificate authority. Each large organization may create its own *Public Key Infrastructure*, but then the problem becomes one of communicating among the different infrastructures.

The Public Key Infrastructure from the Connecticut Hospital Association (called the CHIME-Trust) evolved from the desirability of an electronic network among the partners in the Association and their connection with insurance companies. CHIME-Trust provides Certificate Authorities and tailors its certifications to the needs of the healthcare community. Thus a certificate to a physician may involve also a check on the physician's status with the state medical society. Likewise a certificate for a hospital may only be given after confirmation that the hospital is registered with the state department of health. Performing these checks on authenticity and getting the organizations to work smoothly with such electronic practices is more difficult than the technical task of implementing a PKI.

Virtual private networks mimic private networks but take advantage of the Internet. By placing messages inside an Internet envelop and encrypting the contents in a special way, an organization can arrange that messages go securely from one location to another across the Internet. Such an approach gives an organization a *low-cost alternative* to building and maintaining a private network.

Signatures authenticate the signer and evidence approval of a document. The law is increasingly recognizing that electronic signatures can be accepted in place of paper-based, hand-written signatures. An electronic signature could be as simple as a password or as complex as a retinal scan. The term digital signature is typically applied to encryption as the method of authenticating a message.

The *Health Care Financing Administration* developed a detailed requirement for security mechanisms to be used in communicating with it. Authentication may use digital certificates or smart cards. Encryption may occur in software or hardware.

The *Careweb* system in Boston is a sophisticated example of a secure medical record system that gives patients access to their medical records across the Internet. The computer model includes role-based access control and auditing. The audit facility allows the patient to know exactly what part of the patient's record was viewed by whom and when.

4.6.2 Direction

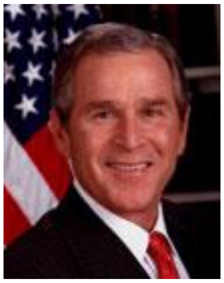
Information is typically collected, stored, and processed in all departments and locations of the healthcare provider, including within hospital facilities, clinics, research facilities, and pharmacies. Diverse types of media, systems, and networks are used for the storage and transmission of confidential patient and caregiver information. Because of the diversity of the organizational issues and the technical complexity of the systems and networks, protecting health information can be achieved most effectively with an organization-wide program. A comprehensive information security program consists of written policies, standards, training, technical and procedural controls, risk assessment, auditing and monitoring, and assigned responsibility for management of the information security program. Although often considered a component of the program, managing the program is unique in that the other components depend upon successful program management.

Management of the security program can only succeed when intimately connected with the overall management of the healthcare organization. Security depends on an organizational model that specifies who performs what operations on what data when. If the organization runs in a quality way so that in fact the planned performance is implemented, then security is a natural derivative of such a well-run organization. If the organization does not have such a clear vision and way of working, then all the specific security mechanisms will be wasted.

Naturally enough security has been important prior to HIPAA, but HIPAA's attempt to harmonize and regulate security nationally causes healthcare organizations to re-consider their approach to security. If security is seen primarily as a requirement to put a stronger *lock* on the door, then the investment in security will not show a profit to the implementing organization. If, instead, security is seen as precise, computer-supported workflow management, then investing in such security can be done in a profit-making way. The American healthcare system can seize this 'security call' as an opportunity to systematically improve the management of healthcare information.

Many healthcare organizations are adopting a '*wait and see*' approach, wanting to follow well-traveled paths rather than create new paths, as regards HIPAA-compliance. Whether an organization wants to create new trails or follow the well-traveled trail, understanding the existing map is vital. The preceding sections provide such a map.

> The health care industry is lobbying the Bush administration to delay, change or kill the [privacy] regulations. Hospitals, insurance companies ... said the rules ... of the Clinton administration, would impose costly burdens. But members of Congress said the privacy protections, ..., were immensely popular with consumers .... Bush administration officials, ..., said they were looking for ways to revise and simplify the Clinton rules ....
>
> Quote from the *New York Times* (Pear, 2001)



President George W. Bush

(www.whitehouse.gov/president)

5 Conclusion

Learning Objectives

- Predict the conflicts among organizational sub-cultures relating to a compliance program.
- Identify common peer practices in a HIPAA compliance program.
- Predict the conflicts among national constituencies in the perpetual struggle to have power over information and recommend steps that might balance the benefits and reduce the tensions.
- Predict new technological developments relative to HIPAA.

This concluding chapter looks to the future. One part of the future concerns other planned developments of ‘Administrative Simplification’, particularly the standardization of the medical record. That standardization of the medical record may be seen as largely a technical matter. However, the birth of HIPAA is a political event and its growth remains a hotly political activity. The political struggles are illustrated to prepare the reader for what is likely to be a never-ending political struggle. Finally, ‘Administrative Simplification’ is described as improved information flow and workflow.

5.1 Corporate Compliance

Main Points

- Corporations have complex individual cultures and subcultures that determine what kind of compliance program will succeed.
- The typical compliance program depends on 1) management commitment, 2) education, 3) implementation, and 4) control.
- Internal reviews are vital to planning and control of compliance but honest reporting is two-edged sword when litigious lawyers demand to see internal review documents.
- The vision of the entity should embrace compliance in a way that is positive for the entity’s service and profit.

Corporate compliance means different things to different companies. Yet, a typical compliance program has the same basic components of management commitment, education, implementation, and control. Internal reviews are vital to planning compliance and monitoring progress but have various foreseen and unforeseen potential consequences. Ultimately, the vision of the company should encompass the compliance requirements in a way that facilitates the company better serving its customers.

5.1.1 Corporate Culture

Each corporation has its culture. A compliance program good for one corporate culture might not be good for a different corporate culture. Firms that exhibit superior financial performance exhibit a strong set of core managerial values that condition the behavior of employees and define the way business is done. The way customers and employees are treated is another aspect of *culture*, as is respect for government regulation.

While a corporation will have an overall culture, inside a corporation there will exist numerous *subcultures*. For example, the legal department has distinctly different beliefs and customs from the billing department. An effective compliance program will address these differences and recognize natural alliances among certain subcultures.

For better or worse, corporations seldom approach compliance with the law in a generalized way. Rather compliance is approached on a piecemeal basis focused on separate areas of the law. One manager may be charged with compliance to OSHA, but that person would have little interaction with the person charged with compliance to HIPAA.

The profit motive may work against compliance inside a company. If success is measured by profitability, then to the extent that violation of a law is a shortcut to profitability, that route is inviting. In some corporate cultures, outfoxing government regulators is considered heroic whether or not it impacts *profits*.

5.1.2 Compliance Programs

A typical *compliance program* may be viewed as involving four steps:

1. management commitment,
2. education,
3. implementation, and
4. control.

An executive policy endorsement would be an appropriate sign of management commitment. Education for topics like privacy would go to all staff. Implementation is a complex process that begins with a gap and risk analysis and proceeds to detailed planning and execution. Control is the review of the results and must itself, like the implementation, be continual.

Complete privacy or security relative to the HIPAA privacy and security rules would be impossible to achieve. The degree of compliance will depend on the degree of management commitment. *Management commitment* is generally approached in the following ways:

1. The compliance program is presented to senior management during a workshop on the subject.
2. Compliance is included in the corporations overall high level goals and a top-level policy document is signed by the senior officer.
3. Every department of the entity would include in its annual plan a section on compliance.

Education for compliance likewise involves several steps:

1. A written guidebook that highlights the do's and don'ts should be distributed to relevant personnel and they should sign that they have read it.
2. Face-to-face seminars should be provided to groups of no more than 25 people at a time and attendance of relevant staff should be mandatory.

The seminars should involve some demonstration of competence by the student, such as passing a test.

Implementation requires assessment of the current situation and planning how to reduce gaps in compliance. Staff are assigned appropriate functions and supported in performing them. To assure that performance occurs, *controls* must be consistent. Bonuses should be awarded to those who are very successful in compliance, and employees who fail to contribute to compliance should not be eligible for promotion.

5.1.3 Internal Reviews

Tracking and documenting progress is a crucial part of HIPAA compliance. No matter how lofty the objectives or how laudable the work towards them, unless the work is documented, compliance is in doubt. One of the most significant compliance techniques is in the *internal review*. Usually such reviews will produce written reports intended for internal consumption and address problems that need to be remedied. HIPAA requires such internal vigilance, such documentation of information processing, documentation of training success, and so on.

Unfortunately, internal reviewers may take on the mantle of *enforcement officers* who want to make sure the company follows the rules. A moral force may develop among those conducting such reviews. Groups responsible for internal reviews tend to become clearly established as a compliance constituency. Their interests and values may clash with those of others in the corporation.

Any internal review group can find things that should be corrected. Any group of intelligent, motivated people charged with finding irregularities in a large institution can find irregularities. Furthermore, the group can be expected to want to bring attention to its successes by highlighting irregularities. How can the group charged at some considerable expense at

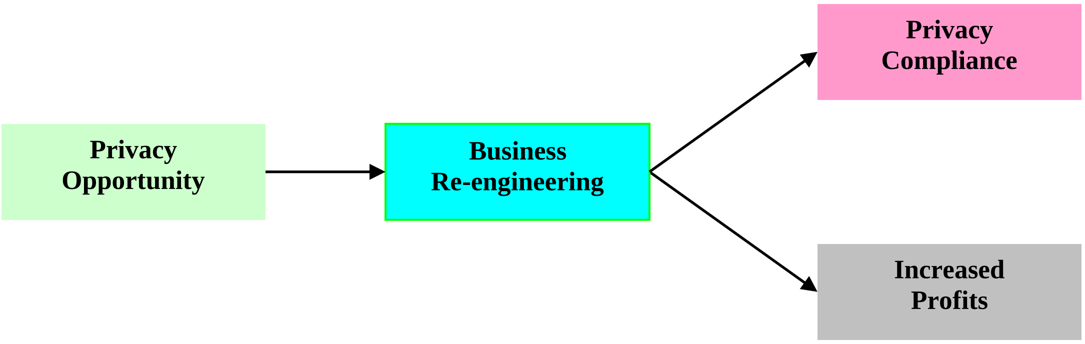


Figure: "Compliance + Increased Profits": through improved service.

identifying the scope of the internal problem justify its existence, if it reports that no problem exists? The healthcare entity needs to be careful to both

- encourage internal review and
- assure that such review does not assume an independent political life inside the entity and thrive unfairly at the expense of other legitimate activities.

Government intervention into healthcare operations has its upside and its downside.

The legal ramifications of documenting HIPAA compliance to the Privacy Rule create both incentives and disincentives to *honestly comply*. The results of a compliance committee report are invaluable to the realistic planning for a further compliance effort. However, such a report carries an unexpected risk. What happens if those who want to punish the company for non-compliance have a copy of the report and use it as evidence of the company's failure to comply? A plaintiff's lawyer might request all internal review documents, and the internal review could be used as evidence against the company.

Two approaches sometimes advocated to minimize the possible damages from leaked internal reviews are to invoke attorney-client privilege and to claim all identified problems are solved:

- To exploit attorney-client privilege, the review is coordinated by lawyers acting pursuant to a request for legal advice. The request for a review would come from senior management and be addressed in writing to the lawyers. If the communications are privileged, then they will not be available for use against the company.
- In conducting the review, the reviewer can be cautioned to minimize writing about unsolved problems. For any identified problems, the document might indicate that the solution has been identified. Strong statements about the positive activities of the company are included.

Invoking *attorney-client privilege* makes a review legalistic where it should not have to be. Likewise, an objective of reporting problems as solved may not be in the best interests of successful re-engineering. An entity must achieve a balance between the goals of

- directly seeking to behave as HIPAA suggests and
- working the compliance system the way attorneys and government regulators see it.

Hopefully, attention to the public good will lead to the right balance.

5.1.4 Vision

A compliance program requires resources. Training alone can consume thousands of hours of staff time. If all players in the industry make the same compliance investment, then the effect on *competitiveness* would be equally the same and the net effect competitively speaking would be zero. However, corporations invest different amounts in compliance and should consider the competitive impacts of a large compliance investment.

Achieving HIPAA compliance will entail different high-level goals for different aspects of HIPAA. The Transactions Rule largely impacts the billing department of a healthcare provider and the claims processing part of a health plan. The Privacy Rule and proposed Security Rule effect all departments of a covered entity.

Everyone agrees that success with the Transactions Rule will lead to large *cost savings* (or profit making, depending on what happens to the cost savings) across the healthcare industry. Most also agree that implementing the Privacy Rule will entail a great cost. However, some argue that compliance with the Privacy Rule could also itself be seen as profit generating. One component of the Privacy Rule, the minimum necessary standard, encourages business re-engineering. Through such steps as development and implementation of the organizational manual (as suggested by HIPAA) an entity can further automate. One can foresee semi-automation of some tasks that would otherwise remain purely manual and the full automation of some tasks that would otherwise remain semi-automatic. Such re-engineering could lead to improved business processes and complying with the law -- hand-in-hand. Some entities should be able to achieve HIPAA Privacy compliance and improve profits simultaneously (see Figure "Compliance + Increased Profits").

The challenge is to integrate HIPAA into top management's *vision* of a successful corporation that serves the public. This could come in the form of adding to the vision the ultimate driver of improved service. Strategically, an entity can conceive of its HIPAA efforts as an effort to improve service.

5.2 Peer Practices

Main Points

- HIPAA compliance projects at two integrated delivery networks show remarkable similarities.
- A framework for comparing and contrasting peer practices can be viewed from the perspective of the Rules, of the compliance life-cycle, or of the components of an entity.

The recent guidance from the Department of Health and Human Services emphasizes the importance of reasonable approaches to privacy (DHHS, 2001b). Reasonableness might be defined by a community of peers. DHHS in its privacy rule has emphasized the importance of peer entities sharing information and establishing their own entity-specific *best practices* (Rada, 2001). The challenge is to convert the national commitment to administrative simplification into practical guidance for individual entities, and the key to success is for peer entities to collaborate.

Numerous reports of individual entity approaches to HIPAA compliance have appeared at conferences (Henderson, 2000). Some have attempted to bring together views and generate a coherent guide; for instance:

- the Computer-based Patient Record Institute collected and published best practices (CPRI, 1999),
- a security summit produced recommendations from several sources (Kooney et al, 2000),
- fifteen academic medical centers produced a guide for Academic Medical Centers that collates input from the fifteen centers (AMC, 2001),
- state health departments are sharing their approaches (GIVES, 2001), and
- WEDI initiated the Strategic National Implementation Process (SNIP) to document industry best practices (WEDI, 2001).

The challenge is to identify what peer entities have in common about their approach to HIPAA compliance and to share that information. Here two entities are considered and then a framework described. The two entities are *Carilion Health Systems* and *Children's Health System*:

- Located in Southwest Virginia, Carilion Health System is an integrated delivery system of seven owned and three managed hospitals, long term care facilities and a health plan.
- Headquartered in Milwaukee, Wisconsin Children's Health System consists of a major pediatric hospital, two satellite hospitals, ambulatory clinics, a freestanding surgery center, primary care clinics, and a health education center.

The two entities have similarities, such as including more than one hospital each. They also have significant differences in that one includes a health plan and addresses all kinds of health care whereas the other does not include a health plan and is a specialty system.

5.2.1 The Beginning

Executive level awareness occurred at both entities first. Then a HIPAA Project Team was formed.

In January 2000, Carilion appointed the Information Security Officer as the HIPAA Project Team leader. Children's began with the hiring of an Information Security Officer who worked with the organization's Compliance Director to form the HIPAA Project Team.

The team leader organized a team and then sub-teams. The membership of the team was chosen to represent those areas of the entity most impacted by HIPAA and whose participation in compliance was particularly critical. For the case of Children's the areas represented on the committee include:

- Administration
- Information Systems
- Finance
- Legal

- Compliance
- Inpatient
- Ambulatory
- Medical Records
- Quality Improvement.

Having obtained members, the HIPAA Project Team next divided itself into sub-teams according to the HIPAA Rules. In other words, sub-teams were formed to address Transactions and Code Sets, Identifiers, Privacy, and Security.

5.2.2 Transaction and Code Sets

After the Transaction and Code Sets Rule was issued in August 2000, the corresponding HIPAA Project sub-team determined how the targeted transactions were used by what application systems. This included determining what code sets carried through, as necessary, to the transactions. The efforts of the sub-team resulted in a chart that documented:

- Application systems that sent transactions.
- Application systems that received transactions.
- Type of transaction(s) processed within the application system.
- How the transaction was sent, for example TCP/IP or FTP.
- Description of data sent.
- Application system owner and contact information.
- Who supported the application.

Current vendors were then approached to determine the extent to which they were dealing with problems identified. Response from vendors was not always enough to allow the covered entity to comfortably plan its compliance and business plan.

Carilion initiated the purchase of a mapper. This mapper will process in-bound and out-bound transactions and be EHNAC certified. Children's is examining the cost of continuing to use a clearinghouse versus the cost of processing native EDI transactions.

5.2.3 Privacy

Both entities reformatted and reorganized the Privacy Rule. One listing shows where documentation is required. One step in creating this listing is to search for occurrences of the word 'document' in the rule. The listing includes entries, such as:

- Covered entity must *document* the satisfactory assurances that business associates will safeguard PHI.
- A covered entity must *document* compliance with the Notice of Privacy Practices requirements by retaining copies of the notices issued by the covered entity as required.

Each entry in the list is augmented with a pointer to the specific section of the Rule from which the entry is copied.

One early undertaking by the Privacy sub-team was to document the flow of protected health information. A data collection sheet was designed to help identify the areas within the organization that collect or use protected health information, where the information comes from, who uses the information, how it is stored, and where it goes. While seemingly a massive undertaking, creation of this inventory progressed well, using a combination of interviews and allowing unit managers to complete the inventory on their own. Completed documents are shared among like units, so that only differences need to be recorded.

In each entity, the components of the Privacy Rule were then assigned to individuals who were responsible to analyze the entity's situation relative to the requirement. In many cases, the entity was doing what the regulation required, but it was not documented anywhere.

To avoid a completely new set of policies and procedures just for HIPAA, the practice is to fold into the existing organizational manual the HIPAA requirements where possible to avoid duplication of effort and the creation of a redundant, unwieldy organizational manual. At Carilion, the organizational manual contained three components that needed amending:

- Information Security and Privacy,
- Confidentiality of Patient Information, and
- Patient Rights and Responsibilities.

To deal with HIPAA an entirely new component of the organizational manual is also being created and is called 'Minimum Necessary Standard and Level of Access for Patient Information'.

While the privacy sub-team is proceeding with its work, the entity's Internal Audit unit contacted each department within the entity to document any internal deviations from the entity-wide organizational manual in the handling of protected health information.

5.2.4 Security

Both entities have made a preliminary assessment of their security system and are proceeding with technical and procedural plans to address perceived gaps. Since the security rule is not finalized, the approaches to security as regards HIPAA are diverse.

The Carilion Security sub-team is divided in turn into 4 sub-sub-teams:

- Technical – Digital Signature, Encryption and Authentication
- Data and Voice Communication – Servers, modems, Internet, E-mail
- Vendor Issues – Software changes, new releases of software required for compliance
- Contingency Planning – business resumption planning which includes backups and business recovery

At Children's, the security approach includes a comprehensive search for technical infrastructure vulnerabilities. Identified vulnerabilities will be patched and procedures will be implemented to eliminate the sources of the vulnerabilities. Children's is also aggressively implementing a full-scale disaster recovery plan. It performed a Business Impact Analysis to identify critical information systems, and the recovery timeframes required for these systems. This information was turned into a requirements document, and combined with a detailed inventory of the hardware and software holdings to produce a Request for Proposal that was sent to major *disaster recovery* vendors.

5.2.5 The Reuse Framework

Both entities believe that HIPAA compliance is important and must be achieved as cost-effectively as practical. Each entity wants to build on or reuse its existing organizational manual rather than attempt to create a new one from scratch. Part of the challenge to *reusing* information is the lack of a framework in which to discuss HIPAA compliance and the material that supports achieving such compliance.

A framework for HIPAA compliance begins with a conceptual model of what compliance entails. Three common views of this model are:

- the rules themselves,
- the compliance life-cycle, and
- the entity components.

The rules themselves are highly organized by the government. The headings and their hierarchical relations in a table of contents of a Rule provide a taxonomy for the rule (Rada, 2001a).

The classic cross-industry approach to compliance involves education, implementation, and audit. Some refine this into

- awareness,
- gap analysis,
- risk analysis,
- planning,
- implementation,
- training, and
- audit.

HIPAA practices for the compliance life cycle at Children's begins by organizing:

- an executive sponsor for the HIPAA project
- a project management team,
- a formal plan that addresses resources, tasks, milestones, and documentation,
- a high-level oversight committee, with representation from all affected areas,
- work groups for Transactions, Privacy, Security, and Identifiers, and
- documentation of all actions and accomplishments related to the HIPAA project.

The next phase is to investigate and analyze:

- policies and procedures related to transactions, security, and privacy,
- information flows that include protected health information (paper, electronic, oral),
- covered electronic transactions sent or received, and the formats used,
- information systems vendor's plans for producing HIPAA-compliant transactions,
- information systems vendor's plans for protecting health information, and
- differences between HIPAA and state laws.

The final phase is to form:

- HIPAA policies and procedures inside existing organizational policies and procedures,
- electronic transactions as supported by cost/benefit analysis,
- access levels for protected health information, and
- procedures to minimize the occurrence of system and network vulnerabilities.

In implementing any part of the compliance plan, individual units within an entity must go into action. This leads to the third view of the compliance process, namely what units will do what.

The provider at its simplest can be viewed as having three main *functional units*:

- reception,
- examination and treatment, and
- billing.

Certain parts of the rules would be particularly germane to certain units. For instance, a standard eligibility inquiry would go from reception. A standard claim would go from billing. Care in discussing patient information would apply in the examination room. Ultimately, the organizational manual and working to its mandate is the crux of HIPAA compliance. This organizational manual more closely reflects the functional breakdown of the entity than the structure of the rules or the life cycle of compliance.

As experiences are collected, one of the important boundary factors will be the *type of entity* sharing the experience. Practices will vary among entity types, but establishing peer practices will be invaluable for each type of entity.

5.3 Politics

Main Points

- Political struggles are continuing as the healthcare industry struggles with HIPAA.
- Understanding needs is one step towards appreciating cultural differences.

The implementation of new information systems in healthcare is in many ways political (Ruffin, 1999):

> Attend to the politics, and deal with them, and which vendors your organization selects will not matter much, because, in a setting of consistent political interests, almost any vendor’s product will perform well.

To succeed with implementing HIPAA is a political matter inside an entity . For HIPAA to succeed nationally will require political support nationally.

5.3.1 Views

The diversity of *political views* is reflected in excerpts from news reports in February 2001 (AHA, 2001 and Pear, 2001). In a February meeting of the U.S. Senate Committee on Health, Education, Labor and Pensions, Senators debated whether DHHS should reopen and thus delay the Privacy Rule. Some committee members questioned the cost and feasibility of the implementation schedule of the regulations. Others called for implementing, enforcing and expanding the privacy rules. Committee Chairman Jim Jeffords said he has asked the General Accounting Office to interview a variety of health care organizations and report the results in order to help the committee determine the need for additional *legislation* to change the regulations.

Senator Pat Roberts said he was stunned and terribly worried by the rules. He added that in parts of Kansas hospitals are short of doctors and nurses and are struggling to keep their doors open and they cannot cope with the new regulations. The healthcare industry is lobbying the government to delay, change, or kill the regulations.

On the side supporting the legislation come other voices:

- Senator Ted Kennedy said the burden of health care systems' compliance with the regulations is less than the burden of someone having to find a new job after being fired because of an employer's knowledge of the employee's health information.
- Senator Hillary Clinton said the regulations need to be stronger and expressed concern about the possible release of patient information for marketing purposes.

Janlori Goldman, director of the Health Privacy Project at Georgetown University, said the rules met a genuine need. She said that millions of Americans withhold information from doctors or provide inaccurate information in an effort to avoid the stigma or discrimination that might result from the disclosure of medical secrets.

Attorney John Houston testifying on behalf of the American Hospital Association said:

> Because nearly 50% of hospitals' patients are Medicare and Medicaid beneficiaries, we believe Congress should closely examine the high costs associated with implementing the privacy rule and supply the necessary funds to ensure that implementation does not put hospitals in financial jeopardy.

Hospitals, insurance companies, health maintenance organizations and medical researchers say the rules would impose costly burdens.

Ultimately, neither the providers nor insurance companies pay for healthcare, but patients, their employers, and government pay. If the problem is that healthcare providers cannot afford to implement the regulations, then perhaps their re-imbursement schemes should be modified so as to accommodate costs incurred for supporting standards and privacy. The government analysis says that the savings from implementing the Transactions Rule will offset the costs of implementing the Privacy Rule. If this analysis is wrong, then the options are to either reduce *expenditures* elsewhere in the healthcare system or to pay providers more to do this.

5.3.2 Needs and Values

To understand the political reaction of health professionals to government regulations, one might study history and culture. Traditionally physicians were solo practitioners charging a fee for service.

The economics of this led to a concern for pleasing the patient, giving them essentially the treatment they wished, and a referral system in which there was pressure on the specialist to please the general practitioner (Reader, 1966). The system leads to an increase in the number of services.

To deal with the increasing costs of healthcare, the health system has moved progressively to group practice. Group managers attempt to account for costs and to manage resources so as to balance the benefits of healthcare and its costs. The effective disposition of resources against objectives is critical, and this is the manager's job. The issue of values is critical not only because characteristic managerial decisions are value-based, but because any manager must be something of a politician to successfully reconcile the conflicting values of others. In the face of uncertainty and complexity, decisions require making simplifying assumptions about the world. These assumptions reflect personal values. This is often forgotten, and the assumption is treated as though based on fact rather than value.

Take the concept of need (Sheldon, 1975):

- The physician defines need as what he happens to treat and like treating (his territory).
- The epidemiologist defines need as what he happens to be able to measure, e.g. incidence and prevalence.
- The community defines need as those conditions that they wish would go away, like the drug addict on the corner.

Ironically, there may be innumerable alcoholics invisible in middle class living rooms, but there is much more fuss about the much smaller number of drug addicts. Need reflects values and is a relative concept. Need is not an absolute and objective phenomenon.

The simplifying assumptions about the world provide stability and continuity and reflect tradition as they become embodied in ways of operating. They inevitably fall short of reflecting the true complexity of the world, and so are impervious to change when the world changes.

When the ways of operating are challenged, what is at stake are values. Many physicians have a high value for autonomy. This is reflected in their protection of the doctor-patient relationship (e.g., in law). Challenges to methods of working potentially undermine that authority. What "loss of autonomy" or "evils of federalization" means, whether said by an industrial manager or physician, is "leave me alone".

The problem of differing values, expressed or unexpressed, based on different assumptions, may lead to conflict. A real attempt to comprehend the other's position and not only this but to demonstrate to them an acceptance of their point of view, while acknowledging that one's own is different, is crucial to effecting positive change across a complex system such as the healthcare system.

Privacy and security are not absolutes. No system can be perfectly private or secure and still be effective. If the medical record is locked in an inaccessible vault, then it may be very secure but also relatively useless. Inevitably, a compromise exists between what is considered adequate privacy or security and what is considered efficient healthcare.

The Privacy Rule and Proposed Security Rule both make abundantly clear that proper behavior on the part of a healthcare entity will depend on the type of entity. What is proper privacy practice for a 2-physician practice is different from what is proper privacy practice for a 300-hospital, integrated delivery network. Healthcare entities have an opportunity to define common practices among peers. For instance, small group physician practices should work together to define what they consider common practices. In this way, they can

- reduce their costs of establishing compliance methods and tools and
- protect themselves against attacks on their compliance by being able to say that their behavior is within the norm established by their peers.

Such establishment of common practices would be consonant with the desire of healthcare professionals to remain masters of their own destiny.

The American Hospital Association has said (AHA, 2000):

> HIPAA has the potential for changing every interaction between physicians and patients, physicians and hospitals, …. It's really a regulation that could reach into every interaction that occurs in the delivery of healthcare in the United States.

People concerned about healthcare and about information systems have an obligation to understand HIPAA. While the impact of any given legislation can come and go with the tides of new legislation, patterns in the legislation are predictable. Healthcare professionals and information specialists need to understand the legislation, help their organizations comply with the legislation, and help shape the next generation of *legislation*.

5.4 Technology

Main Points

- New technical developments are in the pipeline for HIPAA, including standardized patient medical record information.
- Technology can help an organization achieve compliance but seldom can the technology itself be HIPAA-compliant.
- While the privacy and security requirements do call for new developments at many healthcare entities, these developments could be done in such as a way as to be part of improving the efficiency of work processes.

The Administrative Simplification provisions call for much more standardization in healthcare than the government has had time yet to elaborate. For instance, the National Provider Identifier has not been finalized. However, on the standards side the most far-reaching development could be the standardization of the medical record, and this is also foretold in HIPAA.

The cost of the Privacy Rule is countered by the benefit of implementing the Rule as part of a *workflow management system*. Seeing privacy as part of workflow allows for an integration of privacy requirements into general requirements for improved efficiency.

5.4.1 Electronic Medical Records

An integrated delivery system is composed of healthcare providers, service providers, and facilities organized to provide a continuum of healthcare services to a defined population. To manage such delivery of care, a health system must have efficient and accurate ways of capturing, managing, and analyzing clinical data collected at all the different sites where care is provided. Payers and regulators are requesting *report cards* on quality, outcomes, and costs of care provided by the integrated delivery system. For example, the National Committee for Quality Assurance (NCQA) developed the Health Plan Employer Data and Information Set (HEDIS) as a standard report card to help employers evaluate different health plans. Initially focused more on administrative data, the evolving HEDIS criteria are increasingly targeting clinical processes and outcomes. Gathering the data to prepare these reports can be immensely time-consuming and costly when they are manually abstracted from paper records, but with an electronic medical record, reporting on aggregate data can be a byproduct of capturing data electronically. NCQA advised health plans to "move to fully implement the information framework, including the automated patient record" in order to meet the clinical reporting requirements of forthcoming regulations (National, 1997).

An electronic medical record (EMR) is electronically stored information about an individual's lifetime health status and healthcare. It replaces the paper medical record as the primary record of care, meeting all clinical, legal, and administrative requirements. An EMR system is the computer system that supports and extends the EMR. An *EMR system* is an evolving concept that responds to the dynamic nature of the healthcare environment and takes advantage of technological advances. For instance, an EMR system might provide reminders and alerts, linkages with knowledge sources for decision support, and data for outcomes research and improved management of healthcare delivery.

Beyond some general agreement about a high-level definition of EMR, few details have been agreed. For example, there is no common:

- data model,
- set of data elements,
- vocabulary, or
- set of scenarios.

Standards are fundamental, if developers are to create an EMR that links care across different sites, specialties, and circumstances.

HIPAA calls for standardization of claims attachment. This could be interpreted in the extreme to require the standardization of the medical record. However, in its preliminary work on the Claims Attachment NPRM, DHHS has taken a more modest approach to claims attachments and focused on standardizing the *envelope* in which the claim attachment is carried.

Separately from claims attachments, HIPAA directs the National Committee on Vital and Health Statistics (NCVHS) to study the issues related to the adoption of *uniform data standards* for patient medical record information and the electronic exchange of such information. NCVHS made recommendations for Patient Medical Record Information in July 2000. No Notice of Proposed Rule Making has appeared.

The NCVHS *recommendations* emphasize the process of working towards standardization of patient medical record information. NCVHS asks DHHS to support:

- future NCVHS recommendations about patient medical record information,

- government participation in standards development organizations,
- early adoption of patient medical record information standards in government agencies,
- development of implementation guides for standards recommended by NCVHS,
- impact analyses,
- research on healthcare informatics,
- United States' involvement in international health data standards development,
- equitable distribution of the costs for using standards among all major beneficiaries of the standards, and
- legislation to support patient medical record information.

The extent to which DHHS will provide the requested support remains to be seen.

The term *patient medical record information* is intentionally, significantly less comprehensive than the term *electronic medical record*. The focus is on the nomenclature in the record in terms of patient information. This is part of the broader agenda of improving workflow through electronic medical records.

Despite efforts in the public and private sectors, significant *barriers* impede the development and use of EMR systems in the United States (Sullivan and Mitchell, 1995). Technology has continued to move forward at a rapid pace. By comparison, the human and organizational sides of the challenges have remained relatively stagnant. Informational, organizational, and behavioral barriers must be addressed, and these barriers overshadow the technical barriers.

Many of the remaining critical barriers to EMR system development and routine use concern problems that are most effectively dealt with by cooperative, focused activity (Tang and Hammond, 1997). However, a cohesive federal policy to speed the development of a health information infrastructure and the diffusion of EMRs has not emerged in the United States (Shortliffe et al., 1996).

HIPAA calls only for recommendations on electronic medical records. There is no authority within the act to require the development of such a standard. Furthermore, any means for enforcing *compliance* with a standard are not specified.

5.4.2 HIPAA-Compliant Technology?

Vendors might tout 'my technology is HIPAA compliant'. Some providers and payers are demanding to get HIPAA compliant technology. Can a technology be HIPAA-compliant?

Might an IT vendor rightfully claim to be compliant with the Transactions Rule? The *Transactions Rule* calls for compliance with certain standards, particularly X12 formats. A health care provider might want to use information systems that support message formats to payers that are compliant with X12, and a vendor could claim to provide such X12-compliant forms. This is not to say that the entity buying the technology would have an instant fix to its 'Transactions' compliance problem. The Transactions Rule goes beyond the X12 formats to specify the codes that have to be used inside the fields of the format. Achieving compliance with some coding requirements may entail changes in behavior. However, technology could enforce the use of Transaction Rule formats and codes and thus support compliance with the HIPAA transaction rule.

Privacy calls for changes in the way an entity manipulates information. The *Privacy Rule* calls for information systems that represent and audit workflow. Exactly what the workflow should be is not precisely defined. The Privacy Rule broadly specifies what some of the privacy objectives are. An organization must document its objectives and document that its activities take it towards its objectives. Certifying compliance for privacy would require an analysis of the organizational manual and the way the organization implemented its manual. An IT tool should help a health care entity have and follow the appropriate organizational manual but the tool would not make the entity HIPAA compliant.

Security is the topic that comes closest to what an IT vendor feels is the special turf of the vendor. The typical healthcare entity may be violating various security mandates. For instance, the entity might transmit information over the Internet without encrypting it. A vendor can provide tools that encrypt messages before sending them across the Internet. The proposed security rule gives objectives of secure transmissions, reliable authentication, contingency preparations, and much more. However, the proposed security rule is neutral about particular technologies and gives flexibility to organizations in their choice of ways to achieve the objectives. The compliance argument about security is not dissimilar to the argument about privacy: when an organization uses a technology in a certain way to reach a certain objective, then the organization will have behaved in a compliant way as regards that HIPAA security objective.

The bottom line is that Administrative Simplification is about Administration, and technology can support that administration but not replace it. An information technology vendor should help its clients understand what parts of HIPAA compliance are supported by

Task	Priority	Required	Regarding	From	AssignedTo	Description
Category Documentation						
review chart	medium	July 29	Jones, John	Nurse, East	self	Review med list
Category Prescription						
drug renewal activity	medium	Aug. 3	Absen, C.	Nurse, East	self	renew drug

Figure “Clinical Workflow”: This sketch of the computer screen shows the product in which activity lists for staff are displayed. (Adapted from www.abaton.com).

the vendor's technology but should not claim that the technology is HIPAA compliant (Rada, 2001c).

5.4.3 HIPAA as Workflow

HIPAA’s Administrative Simplification profoundly impacts information systems for healthcare organizations. To see the new rules as reducing costs, one may see them as guidelines for *workflow management*. The new HIPPA rules provide a blueprint for workflow management for healthcare organizations (Rada, 2001a).

The Transaction Rule is predicted to save billions of dollars, while the Privacy Rule is predicted to cost billions of dollars. A workflow view puts a different light on these *costs*. Workflow management requires a clear organizational model and mechanisms for implementing that model. Workflow management should reduce costs, and the Privacy Rule can be seen as specifying workflow.

An example of a workflow management system follows. The system builds from the electronic medical record to support semi-automated workflow. The system provides work-list sorting and sequencing that lets users manage tasks (Abaton, 2000). It displays the to-do list for each staff member automatically, with underlying links to the information needed to get the work done (see Figure “Clinical Workflow”). Work-lists prioritize tasks and generate reminders to ensure follow-up with patients.

The Transaction Rule provides a part of the common language for organizations. The Privacy Rule and Proposed Security Rule give decision guides. Systematically defining and implementing these languages and *decision guides* is the basis of workflow management. Privacy and security are not about stopping people from doing things so much as making sure that the right people do the right thing.

The Privacy Rule has ‘minimum necessary use’ as a primary tenet. *Minimum necessary use* requires that people be grouped into roles and that those roles are related to certain actions that they must perform on certain categories of information. This modeling of roles is part of workflow management.

Patients have new rights to access and amend information under HIPAA’s Privacy Rule. These rights bring the patient into the healthcare workflow. The ‘authorization forms’ and ‘notices of privacy practices’ that HIPAA requires are also a reflection of information flow and workflow models.

Security may be seen at three different levels, and each of these levels may be viewed from the workflow perspective:

- Security in the real world is policies for how people work -- in other words, workflow policies.
- Computer security models are foremost about mapping people to information. The most popular way to model such computer security is through role-based access control, and role-based access control, in turn, supports workflow.
- Within the security mechanism realm are matters such as Public-Key Infrastructure. A Public-key Infrastructure supports encryption and connects people to roles and, in turn, manages the flow of information through roles (workflow management).

DHHS has made clear that cost-efficient implementation of HIPAA requires development of generic workflow models that can be shared across certain organization types. DHHS has requested that professional societies, state health departments, and others try to contribute to the body of shared *models*. Each organization type will have particular needs, and an organization should build on the experiences of similar organizations.

5.5 Epilogue

The driving forces behind Administrative Simplification are cost-containment and patient empowerment. The need for cost consciousness in healthcare drove the introduction of standardization in provider-payer transactions. The insistence of the patient on further control over his or her medical record gave birth to the Privacy Rule.

The Transaction Rule begins the definition of a common language. The Privacy Rule provides some decision aides. Now people have the opportunity to build onto this language and these decision aides a *coordinated healthcare system*.

The Privacy Rule provides an information flow and workflow blueprint for protected health information. While considerable flexibility is given to individual organizations to tailor this blueprint to their particular needs, the existence of a *blueprint has major implications* for the management of the healthcare enterprise. With a wider distribution of standard health information and blueprints for that distribution, the opportunities for efficiency in and involvement with the system grow.

The Transactions and Privacy Rules have been finalized. The challenge is now one of *diffusion* or implementation. As the Rules are derivatives of laws and laws can change, the challenge of successful diffusion is particularly complex. At the level of working with healthcare professionals, the common wisdom about successful diffusion includes:

- the changes proposed should be easy, and
- the benefits of the change should be obvious to the users.

Improved information systems will enhance the capability to track performance. If, however, this information is primarily used to identify ‘poor performers’ rather than to guide *improvement* efforts, health professionals may come to view the system with suspicion. Unless organizations can create such positive environments, they are likely to find that efforts to comply with HIPAA will backfire.

The new rules for transactions and privacy are born of the Internet age. The new rules can work to the advantage of enterprise and to society. Organizations will need help in adapting their information to be compliant with these new rules. Information systems professionals working with healthcare professionals and patients have an opportunity to bring these rules to life, if they proceed gently.

All of the developed countries have experienced powerful forces of demographic, cultural, and economic change that have shaped their healthcare systems. The industrial revolution and urbanization led to new health problems for the masses. The long-term result was the piecemeal development of state interventions into healthcare and the development of progressively more complex and specialized healthcare practices. This common heritage has led to patients wanting more and better care but society having difficulty to satisfy these demands. One hope is that an enlightened *citizenry* through the advantages of information systems might become better informed about health, more successfully treat itself, and turn the healthcare process into more of a collaborative process than it is now -- thus leveraging the energy of the masses to help solve the health problems of the masses. This focused information sharing is supported by HIPAA.

5.6 Review Questions

1. Explain why the statement “Corporate culture is monolithic” is false.
2. What are the basic steps in a compliance program?
3. Why are internal reviews potentially double-edged and how does lead to an insight about why some entities invoke client-attorney privilege when doing internal reviews?
4. How might the vision of a company simultaneously address service and compliance with HIPAA?
5. What organizations are opposed to HIPAA and what organizations support it?
6. What does HIPAA have to say about medical records standards?
7. Can a technology be HIPAA compliant?
8. Why is workflow an important concept for HIPAA?

6 Appendix

The Appendix give the Administrative Simplification Provisions of HIPAA, summarizes the provisions of the Privacy Rule and the Proposed Security Rule, and provides a competency quiz.

6.1 The Law

To facilitate navigating the logical structure, numbered, hierarchical headings have been added in shortened form. The majority of the Administrative Simplification section of HIPAA is copied here verbatim. Some sections have been removed when the author felt they were not critical to the arguments in this book.

PUBLIC LAW 104-191

AUG. 21, 1996

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

Public Law 104-191
104th Congress

An Act

To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and healthcare delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) **SHORT TITLE**--This Act may be cited as the Health Insurance Portability and Accountability Act of 1996.

(b) **TABLE OF CONTENTS**--The table of contents of this Act is as follows:

Sec. 1. Short title; table of contents.

TITLE I--HEALTHCARE ACCESS, PORTABILITY, AND RENEWABILITY

...

TITLE II--PREVENTING HEALTHCARE FRAUD AND ABUSE; ADMINISTRATIVE SIMPLIFICATION; MEDICAL LIABILITY REFORM

...

Subtitle F--Administrative Simplification

- Sec. 261. Purpose.
- Sec. 262. Administrative simplification.

Part C--Administrative Simplification

- Sec. 1171. Definitions.
- Sec. 1172. General requirements for adoption of standards.
- Sec. 1173. Standards for information transactions and data elements.
- Sec. 1174. Timetables for adoption of standards.
- Sec. 1175. Requirements.
- Sec. 1176. General penalty for failure to comply with requirements and standards.
- Sec. 1177. Wrongful disclosure of individually identifiable health information.
- Sec. 1178. Effect on State law.
- Sec. 1179. Processing payment transactions.

Sec. 263. Changes in membership and duties of National Committee on Vital and Health Statistics.

Sec. 264. Recommendations with respect to privacy of certain health information....

Subtitle F--Administrative Simplification

6.1.1 Purpose

SEC. 261. PURPOSE.

It is the purpose of this subtitle to improve the Medicare program under title XVIII of the Social Security Act, the Medicaid program under title XIX of such Act, and the efficiency and effectiveness of the healthcare system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.

SEC. 262. ADMINISTRATIVE SIMPLIFICATION.

(a) IN GENERAL--Title XI (42 U.S.C. 1301 et seq.) is amended by adding at the end the following:

PART C--ADMINISTRATIVE SIMPLIFICATION

6.1.2 Definitions

SEC. 1171. For purposes of this part:

(1) CODE SET.--The term 'code set' means any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes.

(2) HEALTHCARE CLEARINGHOUSE.--The term 'healthcare clearinghouse' means a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements.

(3) HEALTHCARE PROVIDER.--The term 'healthcare provider' includes a provider of services (as defined in section 1861(u)), a provider of medical or other health services (as defined in section 1861(s)), and any other person furnishing healthcare services or supplies.

(4) HEALTH INFORMATION.--The term 'health information' means any information, whether oral or recorded in any form or medium, that--

(A) is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and

(B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual.

(5) HEALTH PLAN.--The term 'health plan' means an individual or group plan that provides, or pays the cost of, medical care (as such term is defined in section 2791 of the Public Health Service Act). Such term includes the following, and any combination thereof:

(A) A group health plan (as defined in section 2791(a) of the Public Health Service Act), but only if the plan--

(i) has 50 or more participants (as defined in section 3(7) of the Employee Retirement Income Security Act of 1974); or

(ii) is administered by an entity other than the employer who established and maintains the plan.

(B) A health insurance issuer (as defined in section 2791(b) of the Public Health Service Act).

(C) A health maintenance organization (as defined in section 2791(b) of the Public Health Service Act).

"(D) Part A or part B of the Medicare program under title XVIII.

"(E) The Medicaid program under title XIX.

"(F) A Medicare supplemental policy (as defined in section 1882(g)(1)).

"(G) A long-term care policy, including a nursing home fixed indemnity policy (unless the Secretary determines that such a policy does not provide sufficiently comprehensive coverage of a benefit so that the policy should be treated as a health plan).

(H) An employee welfare benefit plan or any other arrangement which is established or maintained for the purpose of offering or providing health benefits to the employees of 2 or more employers.

(I) The healthcare program for active military personnel under title 10, United States Code.

(J) The veterans healthcare program under chapter 17 of title 38, United States Code.

(K) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), as defined in section 1072(4) of title 10, United States Code.

(L) The Indian health service program under the Indian Healthcare Improvement Act (25 U.S.C. 1601 et seq.).

(M) The Federal Employees Health Benefit Plan under chapter 89 of title 5, United States Code.

(6) INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION.--The term 'individually identifiable health information' means any information, including demographic information collected from an individual, that--

(A) is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and

(B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual, and--

(i) identifies the individual; or

(ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

(7) STANDARD.--The term 'standard', when used with reference to a data element of health information or a transaction referred to in section 1173(a)(1), means any such data element or transaction that meets each of the standards and implementation specifications adopted or established by the Secretary with respect to the data element or transaction under sections 1172 through 1174.

(8) STANDARD SETTING ORGANIZATION.--The term 'standard setting organization' means a standard setting organization accredited by the American National Standards Institute, including the National Council for Prescription Drug Programs, that develops standards for information transactions, data elements, or any other standard that is necessary to, or will facilitate, the implementation of this part.

6.1.3 Applicability

SEC. 1172. (a) APPLICABILITY.--Any standard adopted under this part shall apply, in whole or in part, to the following persons:

(1) A health plan.

(2) A healthcare clearinghouse.

(3) A healthcare provider who transmits any health information in electronic form in connection with a transaction referred to in section 1173(a)(1).

6.1.4 Standards

STANDARDS FOR INFORMATION TRANSACTIONS AND DATA ELEMENTS

SEC. 1173. (a) STANDARDS TO ENABLE ELECTRONIC EXCHANGE--

(1) IN GENERAL--The Secretary shall adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically, that are appropriate for--

(A) the financial and administrative transactions described in paragraph (2); and

(B) other financial and administrative transactions determined appropriate by the Secretary, consistent with the goals of improving the operation of the healthcare system and reducing administrative costs.

(2) TRANSACTIONS--The transactions referred to in paragraph (1)(A) are transactions with respect to the following:

(A) Health claims or equivalent encounter information.

(B) Health claims attachments.

(C) Enrollment and disenrollment in a health plan.

(D) Eligibility for a health plan.

(E) Healthcare payment and remittance advice.

(F) Health plan premium payments.

(G) First report of injury.

(H) Health claim status.

(I) Referral certification and authorization.

(3) ACCOMMODATION OF SPECIFIC PROVIDERS--The standards adopted by the Secretary under paragraph (1) shall

accommodate the needs of different types of healthcare providers.

(b) UNIQUE HEALTH IDENTIFIERS.--

(1) IN GENERAL--The Secretary shall adopt standards providing for a standard unique health identifier for each individual, employer, health plan, and healthcare provider for use in the healthcare system. In carrying out the preceding sentence for each health plan and healthcare provider, the Secretary shall take into account multiple uses for identifiers and multiple locations and specialty classifications for healthcare providers.

"(2) USE OF IDENTIFIERS--The standards adopted under paragraph (1) shall specify the purposes for which a unique health identifier may be used.

(c) CODE SETS.--

"(1) IN GENERAL--The Secretary shall adopt standards that--

(A) select code sets for appropriate data elements for the transactions referred to in subsection (a)(1) from among the code sets that have been developed by private and public entities; or

(B) establish code sets for such data elements if no code sets for the data elements have been developed.

(2) DISTRIBUTION--The Secretary shall establish efficient and low-cost procedures for distribution (including electronic distribution) of code sets and modifications made to such code sets under section 1174(b).

(d) SECURITY STANDARDS FOR HEALTH INFORMATION--

(1) SECURITY STANDARDS--The Secretary shall adopt security standards that--

(A) take into account--

(i) the technical capabilities of record systems used to maintain health information;

(ii) the costs of security measures;

(iii) the need for training persons who have access to health information;

(iv) the value of audit trails in computerized record systems; and

(v) the needs and capabilities of small healthcare providers and rural healthcare providers (as such providers are defined by the Secretary); and

(B) ensure that a healthcare clearinghouse, if it is part of a larger organization, has policies and security procedures which isolate the activities of the healthcare clearinghouse with respect to processing information in a manner that prevents unauthorized access to such information by such larger organization.

(2) SAFEGUARDS--Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards--

(A) to ensure the integrity and confidentiality of the information;

(B) to protect against any reasonably anticipated--

(i) threats or hazards to the security or integrity of the information; and

(ii) unauthorized uses or disclosures of the information; and

(C) otherwise to ensure compliance with this part by the officers and employees of such person.

(e) ELECTRONIC SIGNATURE.--

(1) STANDARDS.--The Secretary, in coordination with the Secretary of Commerce, shall adopt standards specifying procedures for the electronic transmission and authentication of signatures with respect to the transactions referred to in subsection (a)(1).

(2) EFFECT OF COMPLIANCE.--Compliance with the standards adopted under paragraph (1) shall be deemed to satisfy Federal and State statutory requirements for written signatures with respect to the transactions referred to in subsection (a)(1).

(f) TRANSFER OF INFORMATION AMONG HEALTH PLANS--The Secretary shall adopt standards for transferring among health plans appropriate standard data elements needed for the coordination of benefits, the sequential processing of claims, and other data elements for individuals who have more than one health plan.

6.1.5 Compliance Requirements

REQUIREMENTS

SEC. 1175. (a) CONDUCT OF TRANSACTIONS BY PLANS.--

(1) IN GENERAL.--If a person desires to conduct a transaction referred to in section 1173(a)(1) with a health plan as a standard transaction--

(A) the health plan may not refuse to conduct such transaction as a standard transaction;

(B) the insurance plan may not delay such transaction, or otherwise adversely affect, or attempt to adversely affect, the person or the transaction on the ground that the transaction is a standard transaction; and

(C) the information transmitted and received in connection with the transaction shall be in the form of standard data elements of health information.

(2) SATISFACTION OF REQUIREMENTS.--A health plan may satisfy the requirements under paragraph (1) by--

(A) directly transmitting and receiving standard data elements of health information; or

(B) submitting nonstandard data elements to a healthcare clearinghouse for processing into standard data elements and transmission by the healthcare clearinghouse, and receiving standard data elements through the healthcare clearinghouse.

(3) TIMETABLE FOR COMPLIANCE.--Paragraph (1) shall not be construed to require a health plan to comply with any standard, implementation specification, or modification to a standard or specification adopted or established by the Secretary under sections 1172 through 1174 at any time prior to the date on which the plan is required to comply with the standard or specification under subsection (b).

(b) COMPLIANCE WITH STANDARDS.--

(1) INITIAL COMPLIANCE.--

(A) IN GENERAL.--Not later than 24 months after the date on which an initial standard or implementation specification is adopted or established under sections 1172 and 1173, each person to whom the standard or implementation specification applies shall comply with the standard or specification.

(B) SPECIAL RULE FOR SMALL HEALTH PLANS.--In the case of a small health plan, paragraph (1) shall be applied by substituting '36 months' for '24 months'. For purposes of this subsection, the Secretary shall determine the plans that qualify as small health plans.

(2) COMPLIANCE WITH MODIFIED STANDARDS.--If the Secretary adopts a modification to a standard or implementation specification under this part, each person to whom the standard or implementation specification applies shall comply with the modified standard or implementation specification at such time as the Secretary determines appropriate, taking into account the time needed to comply due to the nature and extent of the modification. The time determined appropriate under the preceding sentence may not be earlier than the last day of the 180-day period beginning on the date such modification is adopted. The Secretary may extend the time for compliance for small health plans, if the Secretary determines that such extension is appropriate.

..

6.1.6 Transaction Penalties

GENERAL PENALTY FOR FAILURE TO COMPLY WITH REQUIREMENTS AND STANDARDS

SEC. 1176. (a) GENERAL PENALTY.--

(1) IN GENERAL.--Except as provided in subsection (b), the Secretary shall impose on any person who violates a provision of this part a penalty of not more than $100 for each such violation, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000.

..

(3) FAILURES DUE TO REASONABLE CAUSE.--

(A) IN GENERAL.--Except as provided in subparagraph (B), a penalty may not be imposed under subsection (a) if--

(i) the failure to comply was due to reasonable cause and not to willful neglect; and

(ii) the failure to comply is corrected during the 30-day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred.

6.1.7 Privacy Penalty

WRONGFUL DISCLOSURE OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

SEC. 1177. (a) OFFENSE.--A person who knowingly and in violation of this part--

(1) uses or causes to be used a unique health identifier;

(2) obtains individually identifiable health information relating to an individual; or

(3) discloses individually identifiable health information to another person,

shall be punished as provided in subsection (b).

(b) PENALTIES.--A person described in subsection (a) shall--

(1) be fined not more than $50,000, imprisoned not more than 1 year, or both;

(2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and

(3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

6.1.8 Privacy

SEC. 264. RECOMMENDATIONS WITH RESPECT TO PRIVACY OF CERTAIN HEALTH INFORMATION.

…

(b) SUBJECTS FOR RECOMMENDATIONS.--The recommendations under subsection (a) shall address at least the following:

(1) The rights that an individual who is a subject of individually identifiable health information should have.

(2) The procedures that should be established for the exercise of such rights.

(3) The uses and disclosures of such information that should be authorized or required.

(c) REGULATIONS.--

…

(2) PREEMPTION.--A regulation promulgated under paragraph (1) shall not supercede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation.

6.2 Privacy Rule in Brief

This section summarizes key provisions of the Privacy Rule in list form. A few topical headings, such as ‘use and disclosure’ are given and within those topics a list of items is provided, each beginning with a key term.

6.2.1 Uses and disclosures

Minimum necessary: A covered entity must make reasonable efforts to limit use and disclosure of information to “the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.” This standard does not apply to disclosures between providers in the context of treatment.

De-identify: Individual health information loses its HIPAA protections and may be used or disclosed freely if it cannot be used to identify an individual. The safe harbor specifies 18 identifiers to be removed.

Business associates: Disclosures may be made to business associates under contracts If the covered entity becomes aware of a material breach by a business associate, it is required to take reasonable steps to cure the breach or terminate the contract of a business associate.

6.2.2 Authorization

Authorization: A valid authorization must be written in plain language and contain specific elements.

Objection: A covered entity may use or disclose protected health information without the individual's authorization in facility directories and to family members. In these cases, the individual should be informed in advance of the use or disclosure and have the opportunity to prohibit or restrict the disclosure.

No Objection: A covered entity may use or disclose protected health information without the individual’s authorization and without giving the individual the opportunity to agree or object in certain circumstances. Such uses and disclosures include, but are not limited, to those required by law or for public health activities.

Research: A covered entity may use or disclose protected health information for research, if it has been approved by an institutional review board.

Marketing: Providers may use limited patient information (demographics and dates of service), without authorization for marketing and fundraising activities

6.2.3 Communications

Notices of Privacy Practices: Covered entities must provide individuals with a notice of privacy practices and should obtain a signed acknowledgement from the individual of receipt of the Notice. A provider that has a direct treatment relationship with the individual must provide the notice no later than the date of the first service delivery.

Restrictions: A covered entity must allow an individual to request that the covered entity restrict uses and disclosure for treatment, payment and operations but the entity is not obligated to agree.

Confidential communications: A provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information (PHI) by the provider by alternative means or at alternative locations.

6.2.4 Access and Amend

Access: The individual has a right to inspect and copy his or her PHI that is used, in whole or in part, to make decisions about the individual, for as long as the covered entity maintains the information.

Amend: An individual has the right to have a covered entity amend his or her PHI.

Accounting: An individual has the right to receive an accounting of the disclosures of protected health information.

6.2.5 Administration

Applicability: The Privacy Rule applies to covered entities.

Privacy Official: Covered entities must designate a Privacy Official who is responsible for the development and implementation of the policies and procedures of the entity

Training: A covered entity must train members of its workforce about privacy.

Safeguards: A covered entity must have in place appropriate administrative, technical, and physical safeguards.

Complaints: A covered entity must provide a process for individuals to make complaints concerning its policies and procedures.

Sanctions: A covered entity must have and apply appropriate sanctions against its employees who fail to comply with the entity’s privacy policies and procedures.

Policies: A covered entity must develop and implement policies and procedures relating to PHI that are designed to comply with the elements of the regulations.

Compliance date: April 24, 2003.

6.3 Security Rule in Brief

The Security Notice of Proposed Rule Making gives requirements for:

Administrative Procedures,
Physical Safeguards,
Technical Security Services,
Technical Security Mechanisms, and
Electronic Signatures.

Each requirement is associated with implementation details. The Electronic Signatures provision has been widely agreed to be premature and is not further summarized here.

6.3.1 Administrative Procedures

Administrative procedures are required to guard data integrity, confidentiality, and availability. These procedures must be carefully documented. The Table “Administrative Procedures” gives the requirements and implementation details. Formal practices must be used to manage the

- selection and execution of security measures to protect data and
- conduct of personnel in relation to the protection of data.

These practices also must be well documented and audited.

Table: "Administrative Procedures"

Requirement	Implementation
Certification	
Chain of trust partner agreement	
Contingency plan	• Applications and data criticality analysis. • Data backup plan. • Disaster recovery plan. • Emergency mode operation plan. • Testing and revision.
Formal mechanism for processing records	
Information access control	• Access authorization. • Access establishment. • Access modification.
Internal audit	
Personnel security	• Assure supervision of maintenance personnel by authorized, knowledgeable person. • Maintenance of record of access authorizations. • Operating, and in some cases, maintenance personnel have proper access authorization. • Personnel clearance procedure. • Personnel security policy/procedure. • System users, including maintenance personnel, trained in security.
Security configuration management	• Documentation. • Hardware/software installation and maintenance review and testing for security features. • Inventory. • Security Testing. • Virus checking.
Security incident procedures	• Report procedures. • Response procedures.
Security management process	• Risk analysis. • Risk management. • Sanction policy. • Security policy.
Termination procedures	• Combination locks changed. • Removal from access lists. • Removal of user account(s). • Turn in keys, token, or cards that allow access.
Training	• Awareness training for all personnel (including management). • Periodic security reminders. • User education concerning virus protection. • User education in importance of monitoring log in success/failure and how to report discrepancies. • User education in password management.

6.3.2 Physical Safeguards

Physical safeguards (see Table "Physical Safeguards") relate to the protection of physical computer systems and related facilities from fire and other natural hazards, as well as from intrusion. Physical safeguards also cover the use of locks, keys, and administrative measures used to control access to computer systems and facilities.

Table: "Physical Safeguards"

Requirement	Implementation
Assigned security responsibility	
Media controls	• Access control. • Accountability (tracking mechanism). • Data backup. • Data storage. • Disposal.
Physical access	• Disaster recovery.

controls (limited access)	• Emergency mode operation. • Equipment control (into and out of site). • Facility security plan. • Procedures for verifying access authorizations prior to physical access. • Maintenance records. • Need-to-know procedures for personnel access. • Sign-in for visitors and escort, if appropriate.
Policy/guideline on work station use	
Secure workstation location	
Security awareness training	

6.3.3 Technical Security Services

Technical security services to guard data integrity, confidentiality, and availability include the processes that are put in place to protect and to control and monitor information access (see Table “Technical Security Services”).

Table: “Technical Security Services”

Requirement	Implementation
Access control (The procedure for emergency access must be implemented. In addition, at least one of the following three implementation features must be implemented: context-based access, role-based access, user-based access.)	• Procedure for emergency access • Context-based access. • Role-based access. • User-based access. • Encryption.
Audit controls	
Authorization control (At least one of the listed implementation features must be implemented.)	• Role-based access. • User-based access.
Data Authentication	
Entity authentication (Automatic logoff and unique user identification must be implemented. In addition, at least one of the other listed implementation features must be implemented.)	• Automatic logoff. • Biometric. • Password. • PIN. • Telephone callback. • Token. • Unique user identification.

6.3.4 Technical Security Mechanisms

Technical security mechanisms include the processes that are put in place to prevent unauthorized access to data that is transmitted over a communications network (see Table “Technical Security Mechanisms”).

Table: “Technical Security Mechanisms”

Requirements	**Implementation**
Communications/network controls (If communications or networking is employed, then integrity controls and message authentication must be implemented. In addition, access controls or encryption must be implemented. In addition, if a network is used, then the following four features must be implemented: alarm, audit trail, entity authentication, and event reporting.)	• Access controls. • Alarm. • Audit trail. • Encryption. • Entity authentication. • Event reporting. • Integrity controls. • Message authentication. ● Electronic Signature.

6.4 Competency Test

This is a sample multiple-choice test that the reader might visit before reading the book or after. If the reader knows the answers to these questions, then he or she has probably mastered the knowledge offered in this book. The answers are at the end of the list of questions.

Transactions

Question 1. The Administrative Simplifications provisions began life when

a) health insurance companies tried but failed to standardize provider-payer transactions

b) privacy of patient records was deemed important

c) the healthcare industry wanted a standardized medical record and sought government help

Question 2: What is technically not true about EDI transactions?

a) A transaction set has logically related data in units called segments.

b) A data element separator precedes each data element in the transaction.

c) All data element fields are free form, that is, no specific value is required.

d) Similar transaction sets, called functional groups, can be sent together within a transmission.

Question 3: Given the following field names for the 'Information Receiver Name' loop in an X12 transaction “Entity Identifier Code; Entity Type Qualifier; Name; Identification Code” and that the field separator is '*', and the message “1P**Welby*12345” is received. Then which is NOT true:

a) Name is ‘Welby’

b) Type Qualifier is 1P

c) Entity Identifier Code is 1P

Question 4: Facts about conversion to EDI standards include:

a) Small health care providers typically hire consultants to convert their software to existing standards.

b) Health plans and large health care organizations primarily use off-the shelf software that was developed and maintained by a vendor.

c) There is a need for more clearinghouses to offer more variety of translators.

d) An alternative to system redesign is to purchase a translator to reformat existing system outputs into standard transaction formats.

Question 5: Which is not a code set expected to be used in completing certain fields of X12 transactions:

a) CPT-4

b) ICD-9-CM

c) HCPCS

d) MeSH

Privacy

Question 1: What is NOT the American Medical Association position on privacy?

a) patients own the medical record but doctor's have a right to use it with patient permission

b) the rules would place too many burdens on physicians if they have to be responsible for how their business associates use patient information

c) small physician offices would not be financially affected the same as other types of offices when implementing the proposed regulation

d) the physician has control over the information because when the patient enters into a relationship with the physician, they effectively transfer authority to the physician

e) the proposed regulation doesn't hold accountable those who misuse information

Question 2: Comparing state privacy laws with the HIPAA rules, the following can be said about state laws:

a) states currently require covered entities to make their privacy and access policies available to patients

b) not all states permit patients to inspect and copy their records

c) every state has laws that provide the same level of protection of sensitive information

Question 3: What is not true of The Privacy Act of 1974

a) if the information is released for routine use, then it can be disclosed without the patient's consent

b) individuals have to file civil suits for damages

c) the Act applies only to Federal agencies

d) in practice little ambiguity exists about what it means

Question 4: For an entity to use psychotherapy notes for treatment purposes requires:

a) consent

b) authorization

c) no consent or authorization, but the individual must have an opportunity to object,

d) no consent or authorization, and the individual does not need to be given an opportunity to object.

Question 5:

If a patient requests a copy of his or her protected health information, which of the following is not true. The entity:

a) may charge a reasonable, cost-based fee for the copying, including the labor and supply costs of copying.

b) may charge fees for retrieving or handling the information

c) must provide the information in the format requested, if it is readily producible in such format.

d) may deny a patient access to the patient's record, only if access endangers the patient's life.

Security

Question 1: The Government Accounting Office did a security audit of the Veterans Health Administration in the year 2000 and determined that

a) the hospitals in the VHA used sound security procedures

b) an integrated computer security management program was never adequately established

c) responses to the audit of the previous year had demonstrated major progress on all fronts since that time

d) the lack of biometric authentication devices was the major impediment to adequate authentication

Question 2: Consider three threats T1, T2, and T3 and one countermeasure C1. The following are the specifics for each threat (T1, T2, T3), its severity (1, 2,..., 5), and the percent reduction of the threat by the countermeasure (10%, 20%, ..., 70%):

T1..........2........... 20%

T2..........5............10%

T3..........1............70%

What is the total severity reduction by C1 against these threats:

a) 0.1

b) 0.8

c) 1.6

d) 3.2

e) 8.0

Question 3: All of the statements below are correct about role-based access except

a) permits users to perform certain operations based on membership in a particular role

b) the privileges in a role do not overlap with privileges in another role

c) has role hierarchies which may contain other roles

d) once established, the major task to maintain the operation is to grant and revoke membership in roles

Question 4: What is true about authentication?

a) grants rights to users to access information

b) is used to determine who is trusted for a given task

c) healthcare systems predominantly use password systems as user-identity authentication

Question 5: An office procedures document for a rural provider should NOT

a) include an audit of all system accesses

b) include procedures for who should be notified in case an unauthorized person has accessed the system

c) be required reading for new employees

Question 6: If Nurse Ray is going to send to Doctor Rosa and Nurse Sue an encrypted message that only they can read, then Ray needs to take his message and

a) encrypt it with Ray's public key and send it to Rosa and Sue

b) encrypt it with Rosa's private key and send it to Rosa and separately encyrpt it with Sue's private key and send it to Sue

c) encrypt it with Rosa's public key and send it to Rosa and separately encrypt it with Sue's public key and send it to Sue

d) encrypt it with Ray's private key and send it to Rosa and Sue

Question 7: What can NOT be said about the Connecticut Hospital Association (CHIME) architecture?

a) Registration Authority is set up at CHIME and the major healthcare centers and organizations to insure provider's credentials

b) the lower levels of certificates allow for communications such as the delivery of orders

c) LDAP servers supports the identification of users and the privileges they have within the system

d) Secured Socket Layer communication occurs between the provider, CHIME and the payer

Answers

Transactions: 1. a, 2. c, 3. c, 4. d, 5. d.

Privacy: 1. a, 2. b, 3. d, 4. b, 5. b.

Security: 1. b, 2. c, 3. b, 4. c, 5. a, 6. c, 7 b.

7 References

7.1 A-D

ABA (1996) *Digital Signature Guidelines*, Chicago: American Bar Association.

Abaton (2000) *Advancing your Clinical Web Strategy*, last accessed at http://www.abaton.com/ in December 2000.

AHA (2000) “Standards for Privacy of Individually Identifiable Health Information” American Hospital Association, http://www.aha.org/ar/ privacystandards99.html last accessed July 2000.

AHA (2001) “Venues vary for HIPAA delay debate: Senators disagree over need to hold up privacy regulations” *AHA News*, at www.ahanews.com, February 16, 2001

Amatayakul, Margret (1998) “Setting Standards in Healthcare Informatics” from CPRI Toolkit Section 3.6, http://healthcare.3com.com /securitynet/hipaa/toc.html.

AMA (2000) “Medicare Fraud and Abuse” by American Medical Association, letter to all members of the US Senate, September 12, 2000, http://www.ama-assn.org/ama/basic/ article/202-664-1.html.

AMA (2000b) “AMA agrees in principle with privacy effort; Cautions that the devil is in the details” by American Medical Association, news release, December 21, 2000, http://www.ama-assn.org/ama/pub/article/1611-3625.html

AMA (2001) “AMA Position Paper on HHS Final Rule on Privacy of Medical Records”, published March 2, 2001 and available at http://www.ama-assn.org/ama/basic/article/238-693-1.html

AMC (2001) *Guidelines for Academic Medical Centers on Security and Privacy Practical Strategies for Addressing the Health Insurance Portability and Accountability Act (HIPAA)* written by Academic Medical Centers (AMC) HIPAA Workgroup, sponsored by Association of American Medical Colleges, Internet 2, National Library of Medicine, Object Management Group, available at http://www.aamc.org/members/ gir/gasp/

Anderson, E. Ratcliffe (2000) “Comment Letter to HHS on proposed privacy rule” from Chief Executive Officer of AMA to Secretary of HHS, available at http://www.ama-assn.org/ ama/basic/article/238-574-1.html, dated Feb. 20, 2000.

Armey, Dick (2001) “Is the Government a Threat to Medical Privacy” Letter from Majority Leader of US Congress to Secretary of Dept. Health and Human Services, published March 5, 2001, available at www.freedom.gov/library/ technology/medletter.asp

ASTM (1996) E1762 Guide for Electronic Authentication of Healthcare Information, American Society for Testing and Materials

Australian Institute of Health and Welfare (2000) “National Health Information Agreement” http://www.aihw.gov.au/nhik/owa/nhik_main_menu.entire_page

Bacard, André (1986) *Hunger for power : who rules the world and how* Heroica Books: San Rafael, Calif. (also available from http://www.andrebacard.com/power.html last accessed July 2000)

Bacard, André (1995) *The Computer Privacy Handbook* Peachpit Press: Berkeley, CA.

Bacard, Andre (2000) PGP, from http://www.andrebacard.com/pgp.html last accessed June 2000.

Barkley, John (1998) "RBAC in Healthcare" Software Diagnostics and Conformance Testing, National Institute of Standards and Technology, http://hissa.ncsl.nist.gov/rbac/rbac-slides-omg.ppt

Bass, Steve, Lisa Miller, and Bryan Nylin (2002) *HIPAA Compliance Solutions: Comprehensive Strategies from Microsoft and Washington Publishing Company*, Microsoft Press: Redmond, WA.

Blumberg, Linda (1999) “Expanding Health Insurance Coverage: Are Tax Credits the Right Tack to Take?” August 12, 1999 http://www.urban.org/health/tax_credits.html.

Bogen, Jonathan (2002) *HIPAA IT Handbook: Strategies to Protect Health Information*, HCPro: Marblehead, Mass.

Boerg (1997) “An Overview of the DOD Trusted Computer System Evaluation Criteria” http://www.gasullivan.com/boerg/00000/000ce.htm, Que Corporation

Brandeis, Louis (1928) “Olmstead versus U.S.”, U.S. Supreme Court, *277 U.S. 438, 478.*

Britten, Alexander, Alan Brown, and John Tedesco (1999) “Understanding HHS’s Proposed Health Information Policy Standard” *BNA’s Health Law Reporter, Vol. 8, No. 47*, pp. 1949-1957.

Britten, Alexander (2001) *PrivacySecurityNetwork’s Model Business Associate Contract*, published by McKenna & Cuneo, L.L.P. at http://privacysecuritynetwork.com/healthcare/, last accessed June 10, 2001.

Britten, Alexander, Dana Pashkoff, and John Tedesco editors (2000) *The HIPAA Handbook: What your Organization should know about the proposed Federal Security Standards*, American

Accreditation HealthCare Commission: Washington, D.C.

Britten, Alexander and Dennis Melamed editors (2001) *The HIPAA Handbook: What your Organization should know about the Federal Privacy Standards*, American Accreditation HealthCare Commission: Washington, D.C.

Brutscher, Martin A. (2001) "Realizing Savings from the HIPAA Transaction Standards: How to Get There from Here" McBee Associates, available at www.mcbeeassociates.com, written November 7, 2001, last accessed September 2002.

Business & Health v. 17 no 4, (1999) "Confidentiality and the virtual pharmacy" April 1999, p. 7

Bush, G W (2001) "Statement by the President" http://www.whitehouse.gov/news/releases/2001/04/text/20010412-1.html

Carpenter, Dave (2000) "HIPAA Lessons in Y2K" *Hospitals & Health Networks, Vol. 74 Issue 2*, p16-18

CISCO (2000) "Network Security Solutions for Healthcare" http://www.cisco.com/warp/public/cc/cisco/mkt/security/tech/hippa_rg.htm

Clinton, William (2000) "Statement by the President" on the release of the Transactions Rule on August 11, 2000, The White House, Office of the Press Secretary, available at aspe.hhs.gov/admnsimp/final/whpress1.htm

Clinton, William (2000b) "Remarks by the President on Medical Privacy" on the release of the Privacy Rule on December 20, 2000, The White House, Office of the Press Secretary, available at aspe.hhs.gov/admnsimp/final/whpress2.htm

Collmann, Jeff (1999) "Reconciling European and American Approaches to Privacy" of Georgetown University from CPRI Toolkit Section 3.8

Commerce (2000) "Safe Harbor Overview" U.S. International Trade Administration, Department of Commerce, www.export.gov/safeharbor/SafeHarborInfo.htm, last accessed November 2000.

Committee (1997) *For the Record: Protecting Electronic Health Information* Committee on Maintaining Privacy and Security in Health Care Applications, National Research Council, published by National Academy Press: Washington, D.C.

Cooley, Thomas (1883) *A Treatise on Constitutional Limitations, 5th edition,* Boston: Little, Brown & Co., p 365.

Coronel, Susan (1997) "LTC insurance: Clarifying the tax clarifications" *Nursing Homes Long Term Care Management, Vol. 46 Issue 9*, p57, 2p

Cotter, Cornelius (1960) *Government and Private Enterprise* New York: Holt, Rinehart & Wilson.

CPRI (1996) "Security Features For Computer-Based Patient Record Systems" available at http://www.cpri-host.org/resource/docs/features.html, last accessed July 2000.

CPRI (1996b) "Guidelines for Information Security Education Programs at Organizations Using Computer-based Patient Record Systems" www.cpri-host.org/resource/docs/educatio.html, last accessed July 2000.

CPRI (1996c) "Electronic Signatures" http://www.cpri-host.org/resource/docs/e-sig.html, last accessed July 2000

CPRI (1999) "Mayo Clinic" from *CPRI Toolkit*, Chapter 4 "Developing Policies, Procedures, and Practices, Section 4.3 Sample Security Policies" www.cpri-host.org/resource/toolkit/toolkit.html

CPRI (1999b) "Kaiser Permanente Northern California" from *CPRI Toolkit*, Chapter 4 "Developing Policies, Procedures, and Practices, Section 4.3 Sample Security Policies" www.cpri-host.org/resource/toolkit/toolkit.html

CPRI-HOST (2000) "Sample Confidentiality Statements and Agreements for Organizations Using Computer-based Patient" from www.cpri-host.org/resource/docs/ agreemen.html, last accessed July 2000.

CRAMM (2000) "CRAMM Users Group Home Page" www.crammusergroup.org.uk/

Cupito, Mary Carmen (1998) "Paper cuts? HIPAA's new rules" *Health Management Technology, Vol. 19 Issue 8*, p34, 5p.

Cys, Jane (2000) "HIPAA reg drafters urged to learn from Maine's privacy law mistakes" *AHA News, Vol. 36 Issue 10*, March 13, 2000, p 3.

Cys, Jane (2000b) "AHA, others claim HHS overstepped bounds in its proposed HIPAA regs" *AHA News, Vol. 36 Issue 8*, February, 28, 2000, p 3.

Davidson, Dick (2000) "Statement on the Administration's Final Rule on Privacy" press release December 20, 2000 from President of American Hospital Association and available from www.aha.org.

Davis, Robert (1995) "Online Medical Records Raise Privacy Fears," *USA Today*, March 22, 1995, page 1.

DHHS (1997) *Confidentiality Of Individually-Identifiable Health Information* Recommendations of the Secretary of Health and Human Services, pursuant to section 264 of the Health Insurance Portability and Accountability Act of 1996, submitted September 11, 1997, available http://aspe.hhs.gov/admnsimp/pvcrec.htm, last accessed January 2001.

DHHS (1998) *Notice of Proposed Rule Making for Standards for Electronic Transactions and Code Sets* http://erm.aspe.hhs.gov/ora_web/plsql/erm_rule.rule?user_id=&rule_id=14 last accessed January 2001.

DHHS (1998b) "Process for Developing National Standards" *National Standard Healthcare Identifier: Supplementary Information* http://erm.aspe.hhs.gov/ora_web/plsql/erm_rule.rule_text?user_id=&rule_id=3

DHHS (1998c) *Notice of Proposed Rule Making for National Standard Healthcare Provider Identifier* http://erm.aspe.hhs.gov/ora_web/plsql/erm_rule.rule?user_id=&rule_id=5, last accessed June 2000.

DHHS (1998d) "Code Sets" *Notice of Proposed Rule Making for Electronic Transactions* http://erm.aspe.hhs.gov/ora_web/plsql/erm_rule.rule_text?user_id=&rule_id=19, last accessed June 2000.

DHHS (1998e) "Notice of Proposed Rule Making for Security and Electronic Signature Standards*" Federal Register: August 12, 1998 (Volume 63, Number 155), Page 43241-43280, FR Doc. 98-21601*; also available at http://aspe.os.dhhs.gov/admnsimp/nprm/seclist.htm from which last accessed October 2000.

DHHS (2000) *Notice of Proposed Rule Making for Standards for Individually Identifiable Health Information*, Department of Health and Human Services, http://erm.aspe.hhs.gov/ora_web/plsql/erm_rule.rule?user_id=&rule_id=228

DHHS (2000b) *Health Insurance Reform: Standards for Electronic Transactions* Department of Health and Human Services, Office of the Secretary, 45 CFR Parts 160 and 162, http://aspe.hhs.gov/admnsimp/final/txfin00.htm

DHHS (2000c) *Frequently Asked Questions About Electronic Transaction Standards Adopted Under HIPAA*, Department of Health and Human Services, http://aspe.hhs.gov/admnsimp/faqtx.htm, last accessed June 2001.

DHHS (2001) "Standards for Privacy of Individually Identifiable Health Information: correction of effective and compliance dates" *Federal Register: February 26, 2001, (Volume 66, Number 38),* Department of Health and Human Services, http://aspe.hhs.gov/admnsimp/final/FR010223.htm, last accessed June 2001.

DHHS (2001a) *Final Privacy Regulation Text*, Department of Health and Human Services, http://aspe.hhs.gov/admnsimp/final/PvcTxt01.htm, first published in the Federal Register on Dec. 28, 2000, web site last accessed March 2002.

DHHS (2001b) *DHHS Issues First Guidance on the Final Privacy Rule*, Department of Health and Human Services, published July 6, 2001, http://aspe.hhs.gov/admnsimp/final/pvcguide1.htm, last accessed July 2001.

DHHS (2002) "Proposed Changes to Privacy Rule" from Department of Health and Human Services, March 27, 2002, available at http://www.hhs.gov/ocr.

DHHS (2002a) "Health Insurance Reform: Standard Unique Employer Identifier", 45 CFR Parts 160 and 162, by Centers for Medicare and Medicaid Services, Department of Health and Human Services, in *Federal Register, Vol. 67, No. 105*, pp. 38009-38020, Friday, May 31, 2002.

DISA (2000) "About the HIPAA Draft Standards" Data Interchange Standards Association, available at http://www.disa.org/conference/HIPAA99/index.html, last accessed June 2000.

Dobson, Allen, and Bergheiser, Matthew (1993) "Reducing Administrative Costs in a Pluralistic Delivery System through Automation;" Lewin-VHI Report prepared for the Healthcare Financial Management Association.

DoD (1985), "Trusted Computer Security Evaluation Criteria," Department of Defense DoD 5200.28-STD.

Donovan, Frances and Jennifer M. Gangloff (2000) "The HIPAA law: Your rights to health insurance portability" http://www.insure.com/health/hipaa.html, last accessed June 2000.

Dowling, Alan F. (1987) "Do Hospital Staff Interfere With Computer System Implementation?" in James G. Anderson and Stephen J. Jay, eds., *Use and Impact of Computers in Clinical Medicine*, New York: Springer-Verlag.

Duke University Medical Center (1996) "X12N Links" Health Informatics Standards from http://www.mcis.duke.edu/standards/X12N/x12.htm last accessed June 2000.

DWT (2002) "Analysis & Comments on Major Changes to HIPAA Patient Privacy" Davis Wright Tremaine Law Firm, available at www.dwt.com, last accessed September 2002.

7.2 E-M

Editor (1994) "Who's Reading your Medical Records?" *Consumer Reports*, October 1994, page 628-632.

EPIC (1996) "Many Companies Fail to Protect Electronic Information" report on a survey by David Linowes, available at *Electronic Privacy Information Center*, www.epic.org/

privacy/workplace/linowespr.html, published April 22, 1996.

Etzioni, Amitai (1999) *The Limits of Privacy*, Basic Books: New York.

FDA (2000) *National Drug Code Directory*, from Food and Drug Administration, DHHS, available for free in full form at http://www.fda.gov/cder/ndc/index.htm

Ferraiolo, David; Janet A. Cugini, and D. Richard Kuhn, "Role-Based Access Control (RBAC): Features and Motivations", *11th Annual Computer Security Applications Proceedings*, 1995.

Ferraiolo, David (2000) "Role-Based Access Control" National Institute for Standards and Technology, http://hissa.ncsl.nist.gov/ project/rbac.html.

Flinn, Patrick and James Jordan (1997) "Using the RSA Algorithm for Encryption and Digital Signatures: Can You Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent?" copyrighted by Alston & Bird LLP, published on July 9, 1997 at http://www.cyberlaw.com/ rsa.html last accessed July 2000.

Gallup (2000) *Public Attitudes Toward Medical Privacy*, submitted to The Institute for Health Freedom on September 2000 by The Gallup Organization of Princeton, New Jersey, available at www.forhealthfreedom.org/Gallupsurvey/IHF-Gallup.html, last accessed May 25, 2001.

GAO (1999) *Federal Information System Controls Audit Manual*, Government Accounting Office, Accounting and Information Management Division, GAO/AIMD-12.19.6 also available from http://www.gao.gov/policy/guidance.htm

GAO (2000) *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*, Government Accounting Office, report to the House of Representatives, GAO/AIMD-00-295, September 2000, also available from http://www.gao.gov/new.items/ai00295.pdf.

GAO (2000b) *VA Information Systems: Computer Security Weaknesses Persist at the Veterans Health Administration*, Government Accounting Office, report to the Acting Secretary of Veterans Affairs, GAO/AIMD-00-232, September 2000, also available from http://www.gao.gov/new.items/ai00232.pdf.

Garguilo, John and Paul Markovitz (1996) *Guidelines for the Evaluation of Electronic Data Interchange Products* NIST Special Publication 500-231, available at http://www.nist.gov/ itl/div896/ipsg/eval_guide/evaluation_guid.html, written January 1996, last accessed July 2000.

Gates, Bill (1999) *Business @ the Speed of Thought: Using a Digital Nervous System*, Warner Books and http://www.speed-of-thought.com/.

Gatty, Bob (1997) "Improper medicare payments reach $23 billion, angering feds" *Physician's Management, Vol. 37 Issue 12*, p22, 4p.

Gatty, Bob (1998) "Government aims to clean up fraud and abuse in Medicare" *Dermatology Times, Vol. 19 Issue 2*, p 1-3.

GCD (2002) "Final Modifications to HIPAA Privacy Rule: Client Memorandum" Gardner, Carton, and Douglas Law Firm, Chicago, IL, available from www.gdc.com, last accessed September 2002.

GIVES (2001) *HIPAA Government Information Value Exchange for States (GIVES)*, www.hipaagives.org, last accessed Aug. 31, 2001.

Gorman, Christine (1996) "Who's Looking at your Files?" *Time Magazine*, May 6, 1996.

Graaf, Willem de (2000) "Cryptology" published April 2000 at http://www-groups.dcs.st-and.ac.uk/~wdg/slides/node105.html

Griew, A. and R. Currell, "A Strategy for Security of the Electronic Patient Record," Institute for Health Informatics, Aberystwyth, Draft Version 2.1, March 8, 1995.

Gue, D'Arcy and Steve Fox (2002) *Guide to Medical Privacy & HIPAA*, Thompson Publishing Group: Tampa, FL.

Gunter, Booth (1996) "It's No Secret: What you tell your doctor--and what Medical Documents Reveal about you -- may be open to the Scrutiny of Insurers, Employers, Lenders, Credit Bureaus, and others" *Tampa Tribune*, Oct. 6, 1996, pg. 1

Gustafson, Bobette (2000) "Patient Financial Services" *Healthcare Financial Management Vol. 54, Number 4*, p. 74-6.

Hagland, Mark (1997) "Confidence and confidentiality" *Health Management Technology, Vol. 18, Issue 12*, p 20-25

Hagland, Mark (1998) "Six Opinions on IT security" *Health Management Technology, Vol. 19 Issue 12*, November 1998, p16-21

Hagland, Mark (1998b) "The gap: HIPAA and secure IT" *Health Management Technology, Vol. 19, Issue 6*, p24-29

Halberg, Ross and Eric Saff (2002) "Meeting the Transaction and Code Set Requirements in a Multi-entity Health System Environment" in *HIPAA Summit West Conference Proceedings*, occurred March 2002 in San Francisco, CA, available via www.hipaasummit.com.

Hall, Mark A. (2000) "The Geography of Health Insurance Regulation: A guide to identifying, exploiting, and policing market boundaries" *Health Affairs,* April, 2000

Hann, Leslie Werstein (1999) "Standing firm on new turf" *Best's Review (Life/Health Insurance Edition) vol. 100, no. 1,* p. 44-7.

HCFA, 1998 "Internet Security Policy Memo" November 1998, obtained from WEDI Internet Pilot Report.

HCFA (2000) "HIPAA Insurance Reform" http://www.hcfa.gov/medicaid/HIPAA/topics/more.asp, last accessed June 2000.

HealthAxis (2002) "The MEGA Life and Health Insurance Company Makes Significant Advances in Electronic Claims Processing Capabilities" http://www.healthaxis.com/temps/CI/study/MEGA.pdf

Health Privacy Project (1999) "The State of Health Privacy: An Uneven Terrain," Georgetown University, published July 1999 at www.healthprivacy.org.

Health Privacy Project (2001) "Myths and Facts about the New Federal Privacy Regulation" Georgetown University, published March 6, 2001 at www.healthprivacy.org.

Health Privacy Project (2002) "Marketing: Modified Privacy Rule" Georgetown University, published August 2002 at www.healthprivacy.org.

Hebert, Bryan (2001) "CSC Practices and Tools" *HIMSS HIPAA SIG Newsletter, Volume 1, Issue 12*, June 7, 2001, pp 9-20, distributed by listserv HIPAA@listproc.umbc.edu and available on SIG web site at www.himss.org and flex.ifsm.umbc.edu/HIPAA/.

Hellerstein, David (1999) "HIPAA's Impact on Healthcare" *Health Management Technology, Vol. 20, Issue 3,* p10-15.

Henderson, Mary (2000) "Case Study in HIPAA Compliance for Health Plans" presented at the HIPAA National Summit (www.hipaasummit.com) in Washington, D.C. on October 18, 2000.

HFM (2000) "OIG Announces New Safe Harbors" *Healthcare Financial Management, Vol. 54 Issue 1,* from the editorial staff, p10-12.

HHIC (2001) "Email Policy", *HIPAA Readiness Collaborative Pilot Policies* Hawaii Health Information Corporation (HHIC), last accessed June 20, 2001 from http://www.hhic.org/hipaa/pilots.html.

HHIC (2001b) "Information Steward Policy", *HIPAA Readiness Collaborative Pilot Policies* Hawaii Health Information Corporation (HHIC), last accessed June 20, 2001 from http://www.hhic.org/hipaa/pilots.html.

HHN (2000) "Confronting Hipaa" *Hospitals & Health Networks, Vol. 74 Issue 3,* written by the editorial staff, March 2000, p58, 5p.

Hollingsworth, David (1995) *The Workflow Reference Model*, Workflow Management Coalition, Document Number TC00-1003, Document Status - Issue 1.1, 1995. available at http://www.aiim.org/wfmc/mainframe.htm

Huyink, David and Craig Westover (1994) *ISO 9000,* Irwin Professional Publishing, New York.

IBM (2000) "Transaction Standards: Implications for the Healthcare Industry" http://houns54.clearlake.ibm.com/solutions/healthcare/helpub.nsf/detailcontacts/Health_Insurance_Portability_and_Accountability_Act_HIPAA_?OpenDocument.

Institute of Medicine (1997) *The Computer-Based Patient Record: An Essential Technology for Health Care*, revised edition. Washington, D.C.: National Academy Press.

ISO (1999) *Specification and Standardization of Data Elements, ISO/IEC 11179,* from International Organization for Standardization and the International Electrotechnical Commission, http://www.jtc1.org/.

Joseph, Andrew and Christopher Coleman (2002) *HIPAA Self-Assessment and Planning: A Guide to the Privacy and Security Standards, Second Edition*, HcPro Publishers: Marblehead, MA.

JCAHO/NCQA (1999) "Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment" by the Joint Commission on the Accreditation of Healthcare Organizations (JCAHO) and the National Committee on Quality Assurance (NCQA) revised October 14, 1999 obtained from http://wwwb.jcaho.org/pphi/pphi_frm.html, last accessed June 2000.

Kim, Anya; Marion C. Meissner, Lance J. Hoffman, Jeff Collmann, Seong K. Mun (1997) "Risk Analysis of Electronic Renal Care Patient Management System" from Project Phoenix - Protecting the Security and Confidentiality of Patient Information, published March 31, 1997, available from http://healthcare.3com.com/securitynet/hipaa/4_5_1.html and last accessed June 2000.

Kohn, Linda, Janet M. Corrigan, and Molla S. Donaldson, Editors (2000) *To Err Is Human: Building a Safer Health System*, Committee on Quality of Health Care in America, Institute of Medicine, National Academy Press: Washington, D.C. available for free at http://www.nap.edu/books/ 0309068371/html/

Kooney, Jim, Shannah Koss, Terri Kinney, Bill Rider, Chuck Reeves, Jon Zimmerman, Ted Park

(2000) “Draft HIPAA Security Summit Guidelines”, http://www.smed.com/hipaa/events-hss99draft.htm, last accessed June 2000.

Kopp, Carlo (2000) “A Fundamental Paradigm of Infowar” *Systems Enterprise Computing* February 2000 also available at http://www.infowar.com/info_ops/00/info_ops033000b_j.shtml

Lagrasse, Carol (1998) “Ex-Con Caregivers” *City Journal*, pp 8-9, Summer 1998.

Lindberg, Donald A. B. (1979) *The Growth of Medical Information Systems in the United States*, Lexington Books: Lexington, Massachusetts.

Lindberg, Donald A. B. (1995) “The High-Performance Computing and Communications Program, the national information infrastructure, and healthcare” *Journal of the American Medical Informatics Association, Vol. 2,* p 156-159.

Lindsey, Bonnie (1980) *The Administrative Medical Assistant*, Robert Brady Co (a Prentice-Hall Co.): Bowie, Maryland.

LoC (2002) “Administrative Simplification Compliance Act” Thomas Legislative Information on the Internet, Library of Congress, http://thomas.loc.gov

Lowenbergh, John (2000) “Comments on Coding”, personal communication, Oct. 6, 2000 from jlwnbrgh@mailcity.com.

Macintosh, Ann; I Filby, and John Kingston, “Knowledge Management Techniques: Teaching & Dissemination Concepts” *Journal of Human Computer Studies*, September/October 1999.

Malone, Thomas (1987) “Modelling Coordination in Organizations and Markets”, *Management Science 33*, pp 1317-1332.

Meisner, Deborah (2000) “Envoy Experiences with Implementing HIPAA Transactions” presentation to National Committee on Vital and Health Statistics, July 13, 2000.

Mercer, Johnny (2000) “Something’s Gotta Give” last accessed at http://lemonadelounge.com/lyrics/lyrics83.html in November 2000, the song was originally written and performed several decades earlier.

Michailidis, Antonios and Roy Rada “Multimedia and Virtual Organizations”, *Handbook of Internet and Multimedia Systems and Applications*, Borko Furht (ed.), Boca Raton, Florida: CRC Press, 1998.

Mick, Stephen and Ira Mosovice (1993) “Health Care Professionals” pp 269-296, in *Introduction to Health Services* edited by S. Williams and P Torrens, Delmar Publishers: Albany, New York.

Microsoft (1998) "Virtual Private Networking: An Overview" http://msdn.microsoft.com/workshop/server/feature/vpnovw.asp last accessed July 2000.

Mill, David (1985) “Insurers Use Police Tactics to Snare Doctors Who File False Claims”, *Wall Street Journal*, Apr. 26, 1985.

Morrissey, John (2000) “Politics makes maze of HIPAA” *Eye on Info: The HIPAA Connection, a supplement to Modern Healthcare,* October 2, 2000, pp 13-20.

Mowshowitz, Abbe “Virtual Organization”, *Communications of the ACM*, Vo. 40, No. 9, pp. 30-37, 1997a

Moynihan, James and Marcia McLure (2000) “HIPAA Brings New Requirements, New Opportunities” *Healthcare Financial Management, Vol. 54, Issue 3*, pp 52-56.

Muth, Peter; Jeanine Weissenfels, and Gerhard Weikum “What Workflow Technology Can Do For Electronic Commerce” *EURO-MED NET Conference*, http://paris.cs.uni-sb.de/public_html/leute/peter/Euro-Med.ps, 1998.

7.3 N-Z

Nahra, Kirk (2000) “The Gramm-Leach-Bliley Act: Privacy Confusion, Concerns And Short Deadlines” published in *Legal Affairs Bulletin* December 2000 also available from http://www.wrf.com/publications/publication.asp?id=15243412152000

NAMIC (2000) “Electronic Signatures in Global and National Commerce” National Association of Mutual Insurance Companies, from http://namic.org/f/ki/es.htm

National Center for Health Statistics (1998) *International Classification of Diseases, Ninth Revision, Clinical Modification* (ICD-9-CM) available in its entirety for free from ftp://ftp.cdc.gov/pub/Health_Statistics/NCHS/Publications/ICD9-CM/1998/.

NCVHS (1998) “Year 2 Report” from the National Committee on Vital and Health Statistics, available at http://www.ncvhs.hhs.gov/yr2-rpt.htm, last accessed June 2000.

NCVHS (2000) *Uniform Data Standards for Patient Medical Record Information*, National Committee on Vital and Health Statistics, delivered to Secretary of Department of Health and Human Services, July 6, 2000 (also available via http://www.ncvhs.hhs.gov/).

NCVHS (2001) “February 2001 Committee Minutes” from the National Committee on Vital and Health Statistics, available at http://www.ncvhs.hhs.gov/lastmntr.htm, last accessed August 2001.

NCHICA (2000) “HIPAA EarlyView” from North Carolina Healthcare Information and Communications Alliance, available at http://www.nchica.org/activities/EarlyView/nchicahipaa_earlyview_tool.htm

National Committee for Quality Assurance (1997) *A Road Map for Information Systems: Evolving Systems to Support Performance Measurement*

NHCAA (2000) “Guidelines to Healthcare Fraud” National Healthcare Anti-Fraud Association, http://www.nhcaa.org/ factsheet_guideline.htm.

Nichols, Len M.; Blumberg, Linda J. (1998) “A different kind of `new federalism'? The Health Insurance Portability and Accountability Act” *Health Affairs, vol. 17, no. 3,* p 25-43, also available at http://newfederalism.urban.org/ html/haffairs/nichols.pdf and last accessed January 2001.

NIST (1995) "An Introduction to Role Based Access Control" NIST CSL Bulletin on RBAC. http://csrc.ncsl.nist.gov/nistbul/csl95-12.txt

Nolan (1999) *Cost and Impact Analysis of Common Components of Confidentiality Legislation*, Robert E Nolan Company: Management Consultants, available at http://www.renolan.com/healthcare/privacy.pdf last accessed July 2000.

NRC (1991) *Computers at Risk: Safe Computing in the Information Age*. System Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council Washington, DC: National Academy Press.

Owens, Karen “The Proposed Federal Standard for Privacy of Individually Identifiable Health Information” June 18, 2000.

Owen, Richard Zon (2000) “A History and Overview of HIPAA” Hawaii Medical Service Association, last modified on March 2000, available from http://www.hipaadvisory.com/regs/HIPAAHistorybyZon.htm

Pangalos, G; D. Gritzalis, M. Khair, L. Bozios, (1995) “Improving the security of medical database systems” *Proceedings IFIP/SEC'95 international conference on information systems security*, edited by Jan Eloff and Sebastiaan von Solms, Chapman & Hall: London. pp 11-25.

Pear, Robert (2001) “Medical Industry Lobbies to Rein In New Patients Privacy Rules” *New York Times*, Feb. 12, 2001.

Per-Se (2001) *Business1*, www.per-se.com, last accessed July 2001.

Peters, Kurt (1997) *Health Data Directory*, Faulkner & Gray: New York.

Pfeiffer, James (2002) “HIPAA Case Study: Long Term Care Industry” *American Health Care Association Annual 2002 Conference*, October 7, 2002, New Orleans, LA.

Pritts, Joy; Janlori Goldman, Zoe Hudson, Aimee Berenson, and Elizabeth Hadley (1999) “The State of Health Privacy: An Uneven Terrain/A Comprehensive Survey of State Health Privacy Statutes”, Institute for Health Care Research and Policy, Georgetown University Medical Center, July 1999 at http://www.healthprivacy. org/resources/statereports/contents.html, last accessed January 2001.

Privacy Protection Study Commission (1977) *Report of the Privacy Protection Study Commission*, Superintendent of Documents, U. S. Government Printing Office, Washington, D.C., Stock No. 052-003-00395-3.

Qui Tam Online (2000) “What is the False Claims Act” http://www.quitamonline.com /whatis.html.

Rada, Roy and Lynn Evans (1979) “Automated Problem Encoding System for Ambulatory Care”, *Computers and Biomedical Research, 12*, pp. 131-139.

Rada, Roy (1993) “Standards: the Language for Success” *Communications of the ACM, 36, 12* pp 17-18.

Rada, Roy, George S Carson, Chris Haynes (1994) “Standards: the Role of Consensus” *Communications of the ACM, 37, 3* pp 15-16, April 1994.

Rada, Roy (1996) “ISO 9000 Reflects the Best in Standards” *Communications of the ACM, 29, 3* pp 17-20, March 1996.

Rada, Roy (2001) “Online HIPAA Training” *Proceedings Health Information and Management Systems Society '2001 Annual Conference* available online via www.himss.org and on CD-ROM, meeting in New Orleans, LA, occurred Feb. 4-8, 2001.

Rada, Roy (2001a) “HIPAA as Workflow” *Proceedings 2nd National HIPAA Summit* available online via www.hipaasummit.com, March 4-5, 2001, in Washington, D.C.; also distributed to all participants and others via CD-ROM.

Rada, Roy editor (2001b) *HIPAA Security: from the Proceedings of the 2001 Annual HIMSS Conference*, Health Information and Management Systems Society: Chicago, IL.

Rada, Roy (2001c) “How HIPAA-Compliant can Any Technology Be?” *HIPAALERT Vol. 2 No. 7* May 7, 2001 listserv with 14,200 members, subscription available via www.hipaadvisory.com/alert/.

Rada, Roy and D'Arcy Gue (2001) "What Is Happening to Health Privacy?" *HIPAALERT, Vol. 2 No. 6*, March 26, 2001, listserv with 14,200 members, subscription available via www.hipaadvisory.com/alert/.

Rada, Roy, Peter Haigh, Bryan Hebert, Chuck Klawans, and Tom Newton (2002) "HIPAA Best Practices and Best Tools" to appear *HIMSS'2002 Conference Proceedings*, also in HIMSS HIPAA SIG Newsletter, and available from the authors (contact rada@hipaa-it.com).

Rada, Roy, Charles Klawans, Tom Newton (2002) "Comparing HIPAA Practices in two Multi-Hospital Systems" *Journal of Health care Information Management, Vol. 16, Number 2* pp 40-45.

Rada, Roy (2002a) "Air Force Privacy Officers" *HIPAA@IT Monthly Update, Vol. 1, No.. 9*, August 2002, pp 9-10.

Reader, W. J. (1966) *Professional Men*, Basic Books: New York.

Reed-Fourquet, Lori; John T. Lynch, Michael K. Martin, Wing-Yan Leung, Philip P. Ruenhorst (2000) "The CHIME-Trust Healthcare Public Key Infrastructure and Trusted Third Party Services: A Case-Example" CHIME Inc., Wallingford Connecticut from http://chime.org/ security/PKITrusted.PDF last accessed June 2000.

Root, Jan (2000) "Healthcare Transactions" ANSI ASC X12N Insurance Sub-Committee, Work Group 2 Healthcare Modeling, presented on June 29, 2000 at the DISA HIPAA Conference in McLean, Virginia

Ruffin, Marshall de Graffenried Junior (1999) *Digital Doctors*, American College of Health Executives: Tampa, Florida.

Schwartau, Winn (1996) *Information Warfare: cyberterrorism: protecting your personal security in the electronic age* Thunder's Mouth Press: New York.

Senate (2001) "Financial Services Modernization" from U.S.A. Senate Banking Committee, available at http://www.senate.gov/~banking/ conf/grmleach.htm**,** last accessed March 2001.

Sheehan, James G. (1999) "Public-Private Information Sharing in Healthcare Fraud Investigations" *Journal of Health and Hospital Law Fall, Vol. 32, No. 4,* Pg. 593

Sheldon, Alan (1975) *Organizational Issues in Health Care Management*, Spectrum Publications: New York.

Shortliffe, E. H., H. L. Bleich, C. G. Caine, D. R. Masys, and D. W. Simborg (1996) "The federal role in the health information infrastructure: A debate of the pros and cons of government intervention" *Journal of the American Medical Informatics Association, Vol. 3*, p 249-257.

Sigler, Jay and Murphy, Joseph (1988) *Interactive Corporate Compliance: An Alternative to Regulatory Compulsion* Quorum Books: New York.

Simers, Kim and Charles Hamilton (1999) "HIPAA--Why Bother?" *Health Management Technology, Vol. 20 Issue 3*, p16-18.

Staden, Heinrich Von (1996) "In a pure and holy way: Personal and Professional Conduct in the Hippocratic Oath," *Journal of the History of Medicine and Allied Sciences, vol. 51,* pp. 406-408.

Stipe, Suzanne (1996) "Genetic Testing Battle Pits Insurers Against Consumers" *Best's Review-Life/Health Insurance Edition*, August 1996, pg 38.

Stoneburner, Gary (2000) *Information System Security Engineering Principles* http://csrc.nist.gov/publications/drafts/issep.html

Sullivan, Janet Grady (1997) "Unusual suspects" *Contemporary Longterm Care, Vol. 20 Issue 8,* p52-57

Sullivan, F., and E. Mitchell (1995) "Has general practitioner computing made a difference to patient care? A systematic review of published reports" *British Medical Journal 311*, p 848-852.

Summers, Rita (2000) *Secure Computing: Threats and Safeguards*, McGraw-Hill: New York.

Sybase (2001) *New Era of Networks Adapter for EDI*, www.Sybase.com, last accessed July 2001.

System Security Study Committee (1991) *Computers at Risk: Safe Computing in the Information Age*, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, National Academy Press: Washington, D.C.

Tang, Paul C. and W. Ed Hammond (1997) "A Progress Report on Computer-Based Patient Records in the United States" in *The Computer-Based Patient Record: An Essential Technology for Healthcare*, editors Richard S. Dick, Elaine B. Steen, and Don E. Detmer, published by National Academy Press Washington, D.C. 1997.

Thompson, Tommy (2001) "Remarks about HIPAA" speech made by Secretary Thompson of Department of Health and Human Services on March 1, 2001 to the *2nd National HIPAA Summit* (the transcript here was made by Roy Rada and the audiotape is accessible at www.hypermediasol.com).

Thompson, Tommy (2001) "Statement By HHS Secretary Tommy G. Thompson Regarding The

Patient Privacy Rule" April 12, 2001, http://www.hhs.gov/news/press/2001pres/20010 412.html

Thornton, D McCarty (1999) "Perspectives on Current Enforcement: Sentinel Effect Shows Fraud Control Effort Works" *Journal of Health and Hospital Law Fall*, *Vol. 32*, *No. 4*, p. 493.

Tomes, Jonathan (1999) *The Compliance Guide to HIPAA and the HHS Regulations*, Veterans Press: http://www.veteranspress.com/

USHIK (2000) *United States Health Information Knowledgebase* maintained at the US Military at http://hmrha.hirs.osd.mil/registry/, last accessed December 2000.

Verisign (2000) "Understanding PKI" Verisign Corporation, http://verisign.netscape.com/ security/pki/understanding.html

Voehl, Frank, Peter Jackson, David Ashton (1994) *ISO 9000: An Implementation Guide for Small to Mid-Sized Businesses*, St. Lucie Press, Delray Beach, Florida.

Warren, Samuel and Louis D. Brandeis (1890) "The Right to Privacy" H*arvard Law Review*, *Vol. IV*, *No. 5*, December 15, 1890 (this article is available online in its entirety at http://www.lawrence.edu/fac/boardmaw/Privacy _brand_warr2.html).

WEDI (2001) "Transactions Sequencing" a draft white paper authored by SNIP Transactions Group, Sequencing Subgroup, published June 2001, available from http://snip.wedi.org.

WEDI (2001a) "Certification" a draft white paper authored by SNIP Transactions Group, Testing Subgroup, published March 2001, available from http://snip.wedi.org.

WPC (1998) *Healthcare EDI Transactions: A Business Primer*, Washington Publishing Company, available from http://www.wpc-edi.com/models/PrimerHome.html, last accessed January 2001.

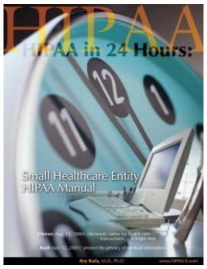
Yoffe, Emily (2001) "Can the Bush Administration Drop the Microsoft Suit?" *Slate*, March 7, 2001, available at http://slate.msn.com/

8 Index of Terms

Other HIPAA-IT Books

The following page is copied from www.hipaa-it.com. There you can select the links and get the full table of content of each publication, the prices, and samples of pages.

HIPAA in 24 Hours



- *full title*: HIPAA in 24 Hours: Small Healthcare Entity HIPAA Manual
- *updated*: September 2002; *ISBN*: 1-901857-11-5
- *length*: 35 pages
- *facilities targeted*: small group physician practices, dental offices, nursing homes, assisted living facilities, and so on
- *readers*: executives and managers
- click here for full text outline and here for PowerPoint overview

Privacy and Health, HIPAA 2003

- *released*: October 2002 *ISBN*: 1-901857-18-2
- *length*: 225 pages and 125,000 words long (click here for full text outline)
- *audience*: anyone responsible for privacy.

Health Ecommerce, 2003

- *full title:* Health Ecommerce, HIPAA Transactions 2003
- *first released*: September 2002; *ISBN*: 1-901857-15-8
- *length*: 172 pages and 70,000 words long (click here for full text outline and here for more images)
- *audience*: professionals with financial, technical, or operational responsibilities, particularly implementing transactions.

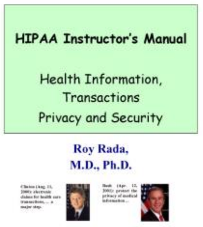
HIPAA@IT Monthly Updates

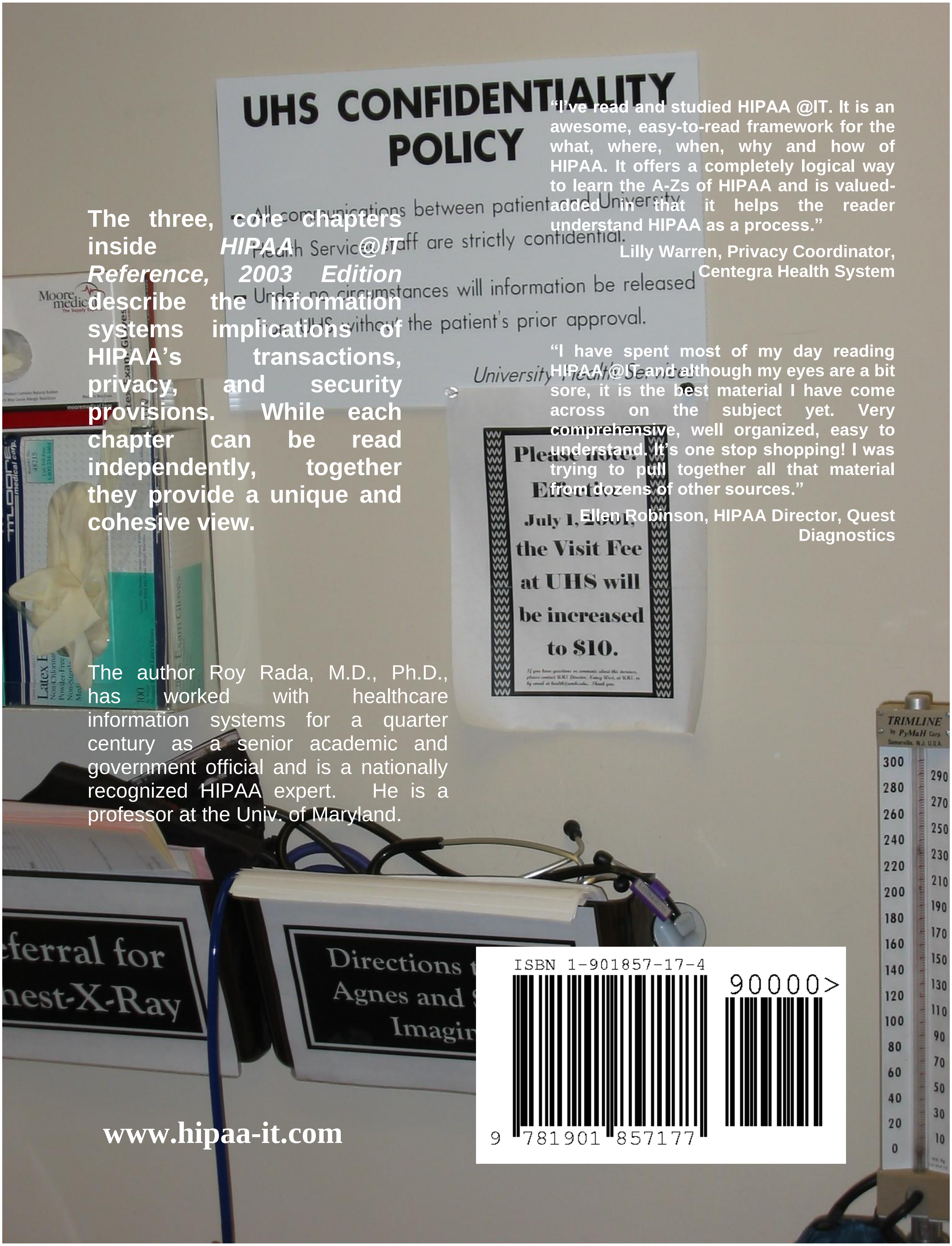
- *topic*: highlights changes in regulations and best practices for transactions, privacy, and security
- *length*: each issue is about 10,000 words long; *ISSN*: 1541-5260.
- click here for issue-by-issue front covers, tables of contents, and excerpts.
- click here for a partial index article-by-article.

Privacy for Long Term Care

- *full title*: Privacy for Long Term Care: HIPAA in 48 Hours
- *released*: October 2002; *ISBN*: 1-901857-14-X
- *length*: 22 pages
- *facilities targeted*: small, independent long-term-care facilities
- *readers*: executives and managers
- click here for full text outline

Information Systems
for
Health Care Enterprises,
2nd Edition
Roy Rada, M.D., Ph.D.


HIPAA Instructor's Manual
Health Information,
Transactions
Privacy and Security
Roy Rada,
M.D., Ph.D.


UHS CONFIDENTIALITY POLICY
Under no circumstances will information be released
the patient's prior approval.
University Health Service
the Visit Fee at UHS will be increased to $10.
Referral for Chest-X-Ray
Directions to Agnes and Imaging
TRIMLINE

The three, core chapters inside *HIPAA @IT Reference, 2003 Edition* describe the information systems implications of HIPAA's transactions, privacy, and security provisions. While each chapter can be read independently, together they provide a unique and cohesive view.

"I've read and studied HIPAA @IT. It is an awesome, easy-to-read framework for the what, where, when, why and how of HIPAA. It offers a completely logical way to learn the A-Zs of HIPAA and is valued-added in that it helps the reader understand HIPAA as a process."

Lilly Warren, Privacy Coordinator, Centegra Health System

"I have spent most of my day reading HIPAA @IT and although my eyes are a bit sore, it is the best material I have come across on the subject yet. Very comprehensive, well organized, easy to understand. It's one stop shopping! I was trying to pull together all that material from dozens of other sources."

Ellen Robinson, HIPAA Director, Quest Diagnostics

The author Roy Rada, M.D., Ph.D., has worked with healthcare information systems for a quarter century as a senior academic and government official and is a nationally recognized HIPAA expert. He is a professor at the Univ. of Maryland.

www.hipaa-it.com

ISBN 1-901857-17-4
90000>
9 781901 857177