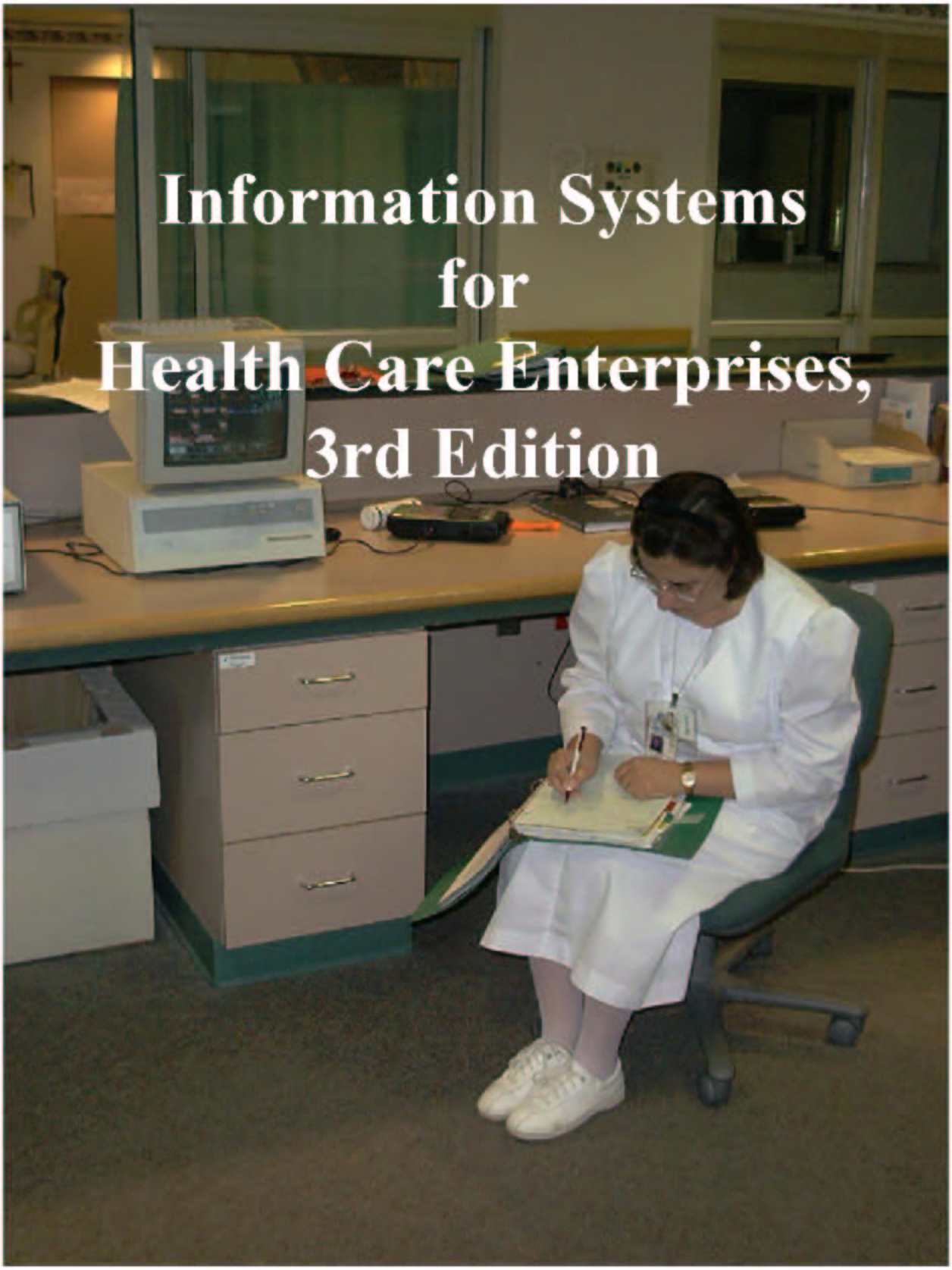


Information Systems for Health Care Enterprises, 3rd Edition

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

Information Systems
for
Health Care Enterprises,
3rd Edition

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

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

Email: rrada@comcast.net

Surface: 1101 South Rolling Road, Baltimore, MD 21228, USA

Phone/fax: 410-747-6712

Rada, R. (Roy), 1951-

Information Systems for Health Care Enterprises, 3rd Edition

ISBN: 1-901857-26-3

Printed July 2005

Preface

The health care industry in the United States consumes about 20% of the Gross National Product, touches everyone, and is information intensive. Information systems have spread slowly from the billing room to the examination room. Successful *information systems applications* must be managed by people knowledgeable in the issues relevant to both health care and information systems. This book examines those special issues.

This book is an introduction to health care information systems for people with some background in *health care* and *information systems*. While no particular knowledge of the reader is expected, the book does not comprehensively define the basic concepts of either health care or information systems. Instead, the reader can expect to become immersed quickly into the challenging issues of getting information systems to work in health care organizations.

Many books have been written about health information systems with usually a distinct audience for each book. For instance, one can find books for

- physicians with practical tips on how to use computers in the private office or
- nursing students on record keeping.

This book is for students of information systems and of health care administration and for professionals responsible for decisions about information systems in health care enterprises.

The book has sixteen chapters. These are grouped into 7 main parts as follows:

- Challenges and Design,
- Providers and Payers,
- Compliance and Fraud,
- Networks and Transactions,
- Privacy and Security,
- Personnel and Vendors, and
- Knowledge and Diffusion.

The reader is asked to address the issues that should lead to the ability to do the following as regards health information systems:

1. identify needs for development of health information systems,
2. manage a design team,
3. delineate the typical components of a health information system and how they are integrated in new systems spanning diverse organizations,
4. identify the people who create and use information systems, and
5. anticipate the factors that determine whether or not a system will be adopted by its users and thus diffuse through the target population.

The book goes into detail about the Administrative Simplification provisions of the *Health Insurance Portability and Accountability Act*. These provisions have been deemed the most important influence on information systems in American health care. They require standardization of provider-payer transactions and privacy and security of protected health information. The book also explains how fraud occurs and the role of information systems in fighting fraud. While many books examine the staff involved in health care information systems, few consider in detail the role of information technology vendors and consultants, as this book does. While the focus is on provider organizations, particularly hospitals, fair attention is given to health insurance companies. The book is used in teaching university students and includes tools for facilitating instruction.

The author, Roy Rada, is a *Professor* of Information Systems at the University of Maryland Baltimore County. Previously, he was Boeing Distinguished Professor of Software Engineering at Washington State University, Editor of *Index Medicus* at the National Library of Medicine, and Professor of Computer Science at the University of Liverpool. Rada has worked as a consultant on computer-supported diagnosis in pathology and radiology, led a team developing medical informatics standards, developed online training material for doctors, and consulted with insurance companies and hospital networks about compliance with government regulations related to information systems. Rada's educational credentials include a Ph.D. from University of Illinois in Computer Science and a M.D. from Baylor College of Medicine. He has authored hundreds of scientific papers. His first journal article appeared in 1979 in *Computers and Biomedical Research* and described a novel coding system for medical problem statements.

Yours,

Roy Rada

Table of Contents

1 Introduction

Learning Objectives

- Distinguish health information systems from management information systems
- Describe the history of information systems in health care.
- Contrast the health care subsystems serving middle-income, poor, military, and veteran patients.
- Identify the diverse textbooks that address health care information systems based on audience.

Health care is one of the greatest single *cost* items for citizens in many developed countries. Information is fundamental to health care. Yet information systems to support health are underdeveloped.

1.1 What it is

The discipline of *Health Information Systems* (HIS) involves a synergy of three other disciplines (Tan, 1995), namely, health, organization management, and information management:

- Health is the end-purpose of HIS applications. The ultimate goal in applying HIS solutions is to improve the health status of people.
- Organization management provides the managerial perspective on developing and using HIS applications for health service organizations.
- Information management is how the information is used. To achieve their goals, health managers must rely on health information.

HIS is based partly on the application of *Management Information Systems* (MIS) concepts to health. One difference between HIS and MIS is that HIS objects are more specialized though derived substantially from MIS (see Table "HIS versus MIS"). Of course, a health care organization has to deal with general problems, like resource management, and in another perspective the discipline of HIS contains the discipline of MIS.

Lindberg (1979) created an analytical framework for comparing HISs. His taxonomy included seven dimensions. For each dimension, values that might identify the position in the dimension of a particular HIS are indicated here:

1. *patient population*: healthy patients versus ill patients; acutely ill versus chronically ill; general population versus special population.
2. *organizational setting*: office versus institution; individual versus group practice; public versus private; screening clinic versus general clinic; general hospital versus specialist hospital.
3. *medical service area*: admissions office; ambulatory care facility; clinical laboratory; dietetics department; intensive care unit; mental health center; operating room; pharmacy; radiology department.
4. *data elements collected*: patient identification; health provider location; demographic information; past hospitalizations; diagnosis; time qualifiers; billing information; patient

Table "HIS versus MIS" (from Tan, 1995)

Characteristics	HIS	MIS
object of cognition	clinical and health management decision making	general management decision making
object of systems	health delivery systems, patient populations, health providers, third parties	organizational systems, consumer populations, business professionals, corporations
subspecialties	medical informatics, dental informatics, nursing informatics, pharmacy informatics	management technology, data processing, office automation, tele-communications
reference disciplines	MIS, health sciences, information science	behavioral science, computer science, management science, information economics

complaints; laboratory results; health care professional interpretations.
5. *functions performed*: retrieval of patient records; patient monitoring; fiscal controls; differential diagnosis; therapy recommendations.
6. *uses of output*: immediate health care team; consultant; researcher; administrator.
7. *financial basis*: patient fee-for-service with individual insurance coverage; patient prepays; insurance carrier; federal government intermediary; state or municipality.

One may define a HIS by selecting one or more values from each of the seven dimensions.

Along these dimensions one famous HIS, called HELP, is described as it existed in 1979 at University of Utah, Salt Lake City, Utah:

1. patient population: acutely ill.
2. health care setting: institution; individual and group practice; private and public; general hospital.
3. medical service area: admissions office; clinical laboratory; surgical recovery room; intensive care unit.
4. data elements collected: patient identification; hospital location; demographic information; past hospitalizations; diagnosis; time qualifiers; billing information; patient complaints; laboratory results; health care professional interpretations.
5. functions performed: retrieval of patient records; patient monitoring; differential diagnosis; therapy recommendations.
6. uses of the output: immediate health care team; consultant; researcher.
7. financial basis: patient fee-for-service with individual insurance coverage; federal government intermediary.

HELP included an integrated patient record system with input from more than 100 ports in the hospital. The data content included demographic admitting data, diagnoses, screening data such as EKGs, history, test values from other cardiology tests, pathology laboratory results, and more. The system monitored the patient physiological signs when in intensive care and was capable of generating alerts for problem situations.

1.2 History

Before *1850*, health care in the United States was a loose collection of individual services functioning independently without much relation to each other or to anything else. The history of the American health system can be depicted in four stages (Torrens, 1993):

- 1850-1900: first large hospitals established,
- 1900-1940: science and technology introduced into health care,
- 1940-1980: attention to social and organizational structure of health care, and
- 1980-now: reorganization of the methods of finance and delivery to try to manage cost.

In the period 1850-1900 only a very *rudimentary technology* was available for the treatment of disease, and the large hospitals, such as Bellevue in New York City, which first appeared in that period, were merely places of shelter for the sick poor who had no home. Indeed, the hospitals were a threat to life, since they were crowded, dirty, and disease-ridden.

After *1900* conditions began to change, stimulated by new discoveries of technologies to help diagnose and treat disease. As more technology developed, it tended to be concentrated in hospitals, with the result that patients and physicians began going to hospitals for the technology to be found there.

Another major change in this period is attributed to the *Great Depression* of the 1930s. The Depression shook the belief in being totally and personally responsible for all aspects of one's life. The government began slowly to assume some responsibility for health care.

With the advent of *World War II*, new antibiotics, new surgical techniques, and new approaches to transportation of wounded people were some of the myriad of improvements created by the massive government investment in improved techniques of care. After World War II, new procedures and new equipment flourished to such a degree that technology became the motivating force for hospitals, and most major decisions were based on that technology. This in turn called for waves of new workers, each more specialized and highly skilled than the last. This increasing *specialization* also called for increasing interdependence and a reliance on health care systems to integrate the work of many separate groups.

Not only did World War II accustom the country to large-scale health care programs, it also encouraged the growth of the *health insurance industry*. During the War, the government froze wages, but did encourage health insurance. This provided the American public with a new form of social organization, the fiscal intermediary or third party. The Blue Cross and Blue Shield plans appeared as nonprofit, community-based health care plans that

insured against medical costs. With the push also by commercial insurance carriers, the percentage of Americans covered by health insurance rose from less than 20 percent prior to World War II to 70 percent by 1960. In the 1960s also the government became a major force in the insurance business by creating Medicare and Medicaid.

Developments of the past two decades in health care financing, planning, policy, and regulation have served to reinforce the increasingly powerful central role played by the *federal government* in the direction of health services. The federal government now controls a significant amount of the financial support for health care (approximately one-third of the total health care expenditures from all sources). By using these massive resources in a unified and centralized manner, the federal government is able to set many of the rules by which health care, governmentally funded or not, is provided.

1.3 Populations

There is not any single '*American health care system*'. There are many separate subsystems serving different populations in different ways. Sometimes they overlap; sometimes they are entirely separate from one another. Four subsystems of health care in the US address four different subpopulations. These subpopulations are (Torrens, 1993):

1. regularly employed, middle-income families with continuous programs of health care insurance,
2. poor, unemployed or underemployed families without continuous health insurance coverage,
3. active-duty military personnel and their dependents, and
4. veterans of US military service.

An endless set of variations is possible from different combinations of these four.

1.3.1 Middle-Income Families

The most striking feature of the *employed, middle-income system* of care is the absence of any formal system. Each family puts together an informal set of services and facilities to meet its need. The service aspects of the system focus on physicians in private practice. The system is financed by nongovernmental funds.

For public health needs the family benefits from the services of *public health departments* for services like sewage disposal. Those public health services that target the individual, such as vaccinations, have to be arranged by the family through the family physician.

Ambulatory patient services are also obtained from *private physicians*. When laboratory tests are ordered or medications prescribed, private for-profit laboratories or pharmacies are used. Typically the patient pays some of the cost of these services out-of-pocket.

Inpatient hospital services are usually provided by a local *community hospital* that is usually voluntary and nonprofit. The specific hospital to be used is determined by the physician. Long-term care is most likely obtained at home through the assistance of a visiting nurse. If institutional long-term care is needed, it is probably obtained in a for-profit nursing home.

When emotional problems are confronted, first private services via the physician are utilized. If hospitalization is required, it might first be in the psychiatric section of the local hospital. In those cases in which very extended institutional care is required and the patient's financial resources are relatively limited, the family may request hospitalization in the *state mental hospital* (the US has about 300 state mental hospitals). This event usually represents the first use of government health programs by the middle-income family and frequently shocks the family for the style of care provided.

The patient has considerable latitude in this system. On the other hand, the system of care is poorly linked. The system can be very *wasteful of resources* and usually has no central control or monitor to determine whether it is accomplishing what it should. One approach to providing further system coordination has been through Health Maintenance Organizations (HMOs) that contract to provide an organized package of health services in an integrated and intentionally coordinated program.

1.3.2 Poor Families

If it was important to study the system of health care for middle-income families because it represents the 'best' of American medicine, then to study the system of health care for underemployed or *poor families* is important for it represents the 'worst' of American medicine. Again there is no formal system per se and the family must put together what services it can. However, the poor do not have the resources to choose where and how they obtain their health services. The great majority of services are provided by local government agencies, such as the county hospital. The patients have no continuity of service as the middle class family has from its family doctor.

When a poor family's newborn baby needs its vaccination, the family goes to the district health center of the health department, not to a private physician. To obtain ambulatory services, the poor family frequently turns to the *emergency room* of the county hospital. The county hospital is the analogue to the 'family physician' for the poor. The emergency room serves as the port of entry to the rest of the health system. To gain admission to the county hospital clinics, the poor typically first go to the emergency room and then get referred to the clinic.

When the poor need inpatient hospital services, they again turn first to the emergency room of the *county hospital* which refers them. The teaching hospitals associated with medical schools also often have wards that are free for the poor, and the poor may go to the emergency rooms of these facilities to get referred to these wards.

The long-term care of the poor begins usually with extended stays in the county hospital. This is not by design but because the hospital is reluctant to discharge them when no responsible other care seems available. For nursing home type care, the major difference between the middle income and poor families is that some government program, such as Medicaid, usually covers the long-term care of the poor.

1.3.3 Military

Military personnel enjoy a well-organized system of health care at no cost. The military health system goes where active-duty military personnel go, and assumes responsibility for total care that is unique among American health care systems. No initiative is required by the individual to start the system. For instance, vaccinations on induction into the service are mandatory. The system emphasizes keeping people well. Great stress is placed on preventive measures, such as vaccinations, regular physical examinations, and education. Unlike any other health care system in the US, the military health system provides health care and not just sickness care.

Routine ambulatory care is usually provided by *medical corpsmen* in a dispensary, sickbay, first aid station, or similar unit that is very close to the military personnel's actual place of work. These same medical corpsmen are responsible for the preventive and education aspects of the care and physicians or nurses typically supervise them. For hospital services the person is referred to a small base hospital, but if the problem requires more specialized attention, then the patient is referred to a military regional hospital. These regional hospitals offer extensive, state of the art services. For long-term psychiatric problems, the patient is probably given a medical discharge.

In general, the military medical system is closely organized and highly integrated. A single patient record is used, and the complete record moves from one health care service to another with the patient. When the need for care is identified, the system arranges for the patient to receive the care and provides any necessary transportation. The system is *centrally planned*, uses non-medical and non-nursing personnel to the utmost, and is entirely self-contained. Generally, the patient has little choice regarding the manner in which services will be delivered, but this drawback is counterbalanced by the assurance that high-quality services will be available when needed.

Dependents and families of active-duty military personnel have access to the regular military health care system services when such services are not fully utilized by the active duty personnel. In addition, the military provides health insurance to the dependents through its *Civilian Health and Medical Program of the Uniformed Services* (CHAMPUS). CHAMPUS is provided, financed, and supervised by the military, but dependents access care in the same way that other middle-class families would access it from private facilities.

1.3.4 Veterans Administration

Parallel to the system of care for active duty military is another system, the *Veterans Administration Health Care System*, operated within the continental US for retired, disabled, or otherwise deserving veterans of previous military service. This VA system focuses on hospital care, mental health services, and long-term care. It operates close to 200 hospitals and more than 200 outpatient clinics.

Patients typically also have a variety of other social services and benefits outside those provided by the VA Health Care System. A further feature of the system is its unique relationship with organized consumer groups in the form of local and national veterans' clubs and associations. In no other health care system in this country does organized consumer interest play such a constant, important, and influential role.

Admission to the *VA hospitals* can be gained through its ambulatory patient care services or via referral from physicians in private practice. Salaried, full-time medical and nursing personnel provide the services in VA hospitals. The VA system is the largest single provider of health care services in the US.

Without an understanding of the interaction among these four major components (the middle-income, poor, military, and VA) of the American health care system, one cannot design appropriate information systems to serve an integrated health care system. Additionally, the competition among the four subsystems of health care creates unfortunate patterns of usage. Although the four systems are separate from one another, they all *compete* for the same resources since they are all dependent on the same economy and the same supplies of health personnel. This competition tends to mean that the services for the underemployed get the smallest share of the resource pie. The competition for resources also creates some waste. For example, in the same region, a county hospital, a teaching hospital, a military hospital, and a VA hospital may all be operating exactly the same kind of expensive service, although only one facility might be needed. Because each institution is part of a separate system, serves a different population, and approaches the resource pool through a different channel, no purposeful planning or controlled allocation of resources is possible.

1.4 Biographical Perspective

The history of computerized health information systems can be relived through the eyes of those who created the *history*. In particular, excerpts from the writing of Donald Lindberg, Kerry Kissinger, and Octo Barnett are provided. From Lindberg is evidenced the 'ah-ha' experience that motivated this medical pioneer to enter the field of information systems. Thirty-year old writings from Barnett about the key factors to success in health information systems are as true today as they were then.

1.4.1 The Insight

Donald *Lindberg*, M.D. in 1960 at University of Missouri was doing research on bacteria and collecting data with a computer. Simultaneously, he was directing clinical chemistry and microbiology at the medical center. The biggest practical problem was getting correct reports from the laboratories to the clinics and wards. From the microbiology lab the pathologists personally signed the report slips, which usually contained a great assortment of spellings of the bacteriological names. Furthermore, the Record Room had at all times hundreds of lab reports on which patient names did not match the patient identifier, and these reports were not permitted to be placed in the charts and hence were lost forever. Lindberg (1990) says:

> It suddenly occurred to me that the computing system I was using for the antibiotic sensitivity experiments could be used to solve my clinical laboratory problem as well. After all, I reasoned, computer programs always spelled things the same way day after day, and the tabulating printer certainly was faster than the folks running the laboratory typewriters. In addition, I could establish limits, so that at least some of the ridiculous errors could never again be reported out and truly life-threatening findings could be identified for telephone reporting. Once one yielded to this line of thinking, it became immediately obvious that the product of the clinical labs was purely information: hundreds of thousands of items per year. Tables outside the program could contain editing and limit values, pointers to other medical record elements, pricing and quality control data, etc.

Lindberg's experience was unusual in the 1960s. More recently, such insights, as documented for Lindberg, have become more common, and thousands of physicians are now actively advancing the use of computers.

1.4.2 Accounting Systems

Kerry *Kissinger* began work with IBM and in the early 1960s installing patient accounting systems. Kissinger's first patient *accounting system* used an IBM 1440 with 16 kilobits of main memory and punched card input. The technological changes since then have been phenomenal, but the basic challenges to the organization remain the same.

The *billing program* had been written by programmers at IBM and was distributed free to hospitals that leased or purchased the IBM 1440. By 1965, 20 hospitals in the US were utilizing this patient billing system. Each decade has spawned a *new generation* of hardware and software capable of doing more things at lower unit cost. The watchword of the 1990s was client server computing and the watchword of the 2000s is Internet-enabled computing.

Despite the many improvements in technology, the human struggles have retained a certain *commonality* and in some ways have become more difficult. Each new generation of users struggles with learning how to deploy the technology. Kissinger's team spent 8 months in 1964 working with the hospital to achieve full operation of the billing system. The payback for the hospital was self-evident. The number of technicians and clerks involved in billing operations

was reduced by half. Bills were produced sooner and more accurately, and hospital cash flow improved.

Implementation of a health care organization patient accounting system in the 1990s took two years to complete and employed a 35-person project team. Everything about the project was more *complex* than earlier projects. The regulatory environment, the number of interfaces to other systems, the network requirements, the testing and data conversion, the procedural changes and training requirements, and coping with multiple, new vendors were all complex and costly in human effort.

The costs and benefits of this 1990s implementation were difficult to measure. The previous system had become too difficult to maintain and had to be replaced. This was a necessary cost of doing business, just as an old building may need to be replaced. The hospital had become locked into a vendor system with little flexibility. The executives did not approve incremental improvements that might have been attempted earlier and that would have avoided massive *one-time costs*. Unfortunately, this scenario is more the norm than the exception in health care (Kissinger and Borchardt, 1996).

1.4.3 Evolutionary Development

Octo *Barnett*, M.D. was the leader of the Massachusetts General Hospital Computer Laboratory for over 30 years. The Laboratory developed the COSTAR clinical information system and its underlying operating system called the '*Massachusetts General Hospital Utility Multiprogramming System*' (MUMPS). In reviewing the history of information systems in clinical care, Barnett (1990) had occasion to reflect on how little the basic issues have changed over the decades. Barnett's 1968 article in the New England Journal of Medicine contains an analysis that applies equally well today:

> Early interest in bringing the revolution in computer technology to bear on medical practice was plagued with over enthusiasm, naiveté, and unrealistic expectations. The use of computers would allow rapid and accurate collection and retrieval of all clinical information, perform automatic diagnosis, collect, monitor and analyze a variety of physiological signals perform and interpret all lab tests immediately and replace the telephone and medical record by fulfilling their function. However attempts to apply computer methods to medicine have had only limited success with numerous failures. … The initial wave of optimism and enthusiasm, generated by beguiling promises of an immediately available, total hospital computer system, passed. Now, efforts are directed towards the painful, slow, evolutionary process of developing and implementing modules or building blocks for individual functions.

The process of convincing people to build a system, building it, and then successfully using it remains the painful, slow *evolutionary process* that Barnett described in 1968.

In another article of the same vintage, Barnett and Greenes (1969) elaborate three recurring problems for system development as follows:

> First the magnitude of the problem is usually grossly underestimated and there is almost always inadequate concern for defining objectives and for planning. Hospital and medical staffs have had little prior experience in innovation in the area of information processing and in many situations the critical decisions are made by individuals in isolated departments who do not process a broad view of the needs of the hospital.
>
> Second, the computer industry has often displayed a considerable lack of understanding and of sophistication. On a number of occasions the sales and promotional aspects of marketing hospital computer systems have been quite misleading and have led to false expectations.
>
> Third, the hospitals have rarely made the depth of commitment of both administrative and professional staff that is required to develop and implement a viable system. The commitment must be in terms of years in order to provide the exposure and experience necessary to cope with the complexity of the problems.

From these problems, the observation is made that an *evolutionary systems development* approach is critical. This issue of developing systems in pieces and integrating them across time versus building whole systems in one swoop has often arisen as contentious in HIS discussions. On the one hand, the systems cannot be completely effective without integrated information, and on the other hand, the amount of change at any one time is typically best kept small.

1.5 Related Work

When this author *Rada* taught his first course on medical informatics in 1981, there were no textbooks per se on the subject. The field was still new as an academic discipline. The two books that the author used as textbooks in 1981 were:

- Lindberg's (1979) *The Growth of Medical Information Systems in the United States* and
- Warner's (1979) *Computer Assisted Medical Decision Making*.

Warner's book is about his landmark health information system that emphasized decision support. Lindberg's book is an overview of the HIS field conceptually and an analysis of the state of the art in 1979.

There are several kinds of publications in the area of health information systems. One kind is aimed at the *practicing professional*, another kind at students, and another kind at researchers. Within each category certain books target specific subcategories. For instance, some books are for medical students, some for nursing students, some for students of medical records, and so on. Of course, some books claim to satisfy the information needs of many different audience types.

On the professional side, naturally, there are also further divisions of the audience. For *health care executives*, *Information Technology for Integrated Health Systems: Positioning for the Future* edited by Kissinger and Borchardt (1996) has an organization not unlike this book in that it goes from vision to design to implementation. The book assumes a reader knowledgeable in health care and information technology and emphasizes the important, broad, practical issues to guide decision-making about information systems acquisitions in health care organizations. Some books targeting the health care manager may focus on particular techno-managerial topics. For instance, Worthley's (2000) *Managing Information in Healthcare: Concepts and Cases* focuses on security management.

Some books target the practicing physician. An example is Ruffin's (1999) *Digital Doctors*. Ruffin argues that physicians need to take care of health care information systems and presents detailed technical and political information as to why physicians should be Chief Information Officers for health care systems.

The United States employs over three million *nurses* – more than triple the number of physicians. Targeting various health care information systems professionals and particularly nurses and nursing students is the extensive series 'Computers in Health Care'. A book from that series is Hannah and Ball's (2000) *Nursing Informatics: Where Caring and Technology Meet, 3rd edition* which addresses nursing students.

Medical records professionals are intimately involved with computerized information systems. An example of a book targeting medical records students is Mattingly's (1997) *Management of Health Information Functions & Applications*. That book gives the students a rather broad introduction to general principles of management along with specifics of how a medical records department works and should be managed.

A book from the management side that teaches HIS assuming that the reader is a *health administration student* is Tan's (2000) *Health Management Information Systems: Methods and Practical Applications*, *2nd Edition*. This book presents a comprehensive, theoretical view of what management means in the context of health care information systems. Much of what is presented is elementary as regards information systems.

Health Management Information Systems: A Handbook for Decision Makers (Smith, 2000) targets students of public health. The book presents background principles from various disciplines and augments them with brief case studies. The case studies come from Britain, Australia, and the United States, and the book attempts indirectly to compare and contrast the health care information systems of the three *countries*.

A large collection of books comes from the medical informatics community. People in *medical schools* typically author these books and target students or staff of medical schools. Thus the emphasis tends to be on topics like medical expert systems, patient monitoring systems, and medical library information systems. There have been many conferences of academics that include published proceedings that are a kind of book. The well-known conferences series that produce book-like proceedings are the American-dominated 'American Medical Informatics Association' conference series and the European-dominated 'MedInfo Conference' series. This portion of the health care information systems community tends to use the term 'medical informatics' in preference to health information systems or health informatics. A popular textbook for medical students studying informatics is Shortliffe et al's (2000) *Medical Informatics: Computer Applications in Health Care and Biomedicine*. As a textbook for students of medical computer science, the book emphasizes concepts,

such as medical data, medical reasoning, evaluation of medical systems, and ethics.

In addition to the books targeting professionals, students, and researchers, there may be other categories. For instance, targeting the *general public* is Karen Duncan's (1994) *Health Information and Health Reform* that provides a layman's rationale for a national health information system and attempts to politically move people to do something about it.

1.6 Questions

Reading Questions

1. What are the similarities and differences between Health Information Systems as a discipline and Management Information Systems as a discipline?
2. Summarize the history of technology in American health care from 1850 till now.
3. Lindberg and Barnett are physicians working in research environments. Kissinger is an information systems specialist working for a vendor of information systems. Their histories show a greater concern for accounting by Kissinger and on diagnosis and treatment by Lindberg and Barnett. Explain why these different emphases might exist.
4. What views on the critical interfaces for success of HIS were espoused several decades past but remain true today?

Doing Question

The textbook provides a sub-section called 'Related Work' that introduces a simple taxonomy of book types in the subject matter area of the book. This assignment should be submitted with 3 parts as follows:

First, reproduce the taxonomy and list under each category the author or editor (this exercise may use the term 'author' to refer to authors and/or editors) and book title for those entries in that category from the book. Use hierarchical format with indentations to indicate different levels. Do this in Microsoft Word or html. Use black text on white background.

Second go to www.amazon.com and find books that can be retrieved with key words of 'health care information systems'. Select 5 books (not mentioned in our textbook 'Related Work' section) that fit each into a distinct category of the taxonomy. You can extend the taxonomy if you find a book that does not fit into the taxonomy from step 1. Provide the taxonomy in indented hierarchical form and list the author and title of each of your five books in the appropriate location in the taxonomy. Mark all you additions in red ink. In other words, the books you enter should be in red and any new terms that you add to the taxonomy should be in red.

Third provide an explanation for each book as to why it belongs where you put it in the taxonomy. This explanation might relate to the professional position of the author(s), the reviews of the book, the authors preface, or something else that indicates directly or indirectly the intended audience.

Part I: Challenges and Analysis

2 Challenges

Main Points

- Escalating costs are a major problem with the American health care system and seem bound to continue.
- The high costs do not mean the absence of errors but might be related to problems in coordination.
- Trends in health care and in information systems influence the strategy of a particular organization, which in turn determines the information systems needs of the organization.
- The level of information systems investment in health care had been well below the average in many other industries but is now growing rapidly.
- Poor data quality threatens lives and better information systems can help.
- New government regulations, new technologies, and new expectations of patients require new information systems.

New technologies of care are in abundance but the ability to cope with them cost-effectively is in short supply. This leads also to problems of data quality and coordination. In other words:

- New technologies demand new skills, but
- If new skills are in short supply, then new technologies may be incorrectly used.

Information systems could be helpful tools in dealing with data quality and coordination of services. More generally the need for information systems in health care is predicated on the trends in the health care industry, trends in information systems, and the specific strategies of any given health care organization. Those trends are outlined along with the typical expectations that those trends imply for health information systems. Improvements are needed by way of further investment, further quality data, and linkages.

2.1 Problems

Salient problems facing the health care system include rising costs, medical errors, and coordination. Each of these is addressed in the next three subsections.

2.1.1 Rising Costs

New diagnostic *technologies*, such as magnetic resonance imagining devices, lead to increased costs of health care. The rapid rise in health care costs sets off a series of events. Briefly stated, the rise in costs forces the insurance programs and employers to contain costs. These efforts of the *payers* to contain health care expenditures have an impact on the hospitals and physicians. They find their sources of revenue being constrained as a result of the payer's health care containment efforts, so they then take actions of their own in reaction to the efforts of the payers. These actions of the health care providers, in turn, often affect patients and communities which must take actions to lessen the impact (Torrens and Williams, 1993).

The result of this chain of events is a circular system that passes along the effects of one particular set of changes to another part of the system, which in turn takes actions of its own to pass the problem along further. This system forces each individual part of the system to determine how to play the game. Each part solves its particular limited problems and very often does so with an elaborate display of talent, energy, and sophistication. Tragically, the need for each individual part to

- deal with its limited problems and
- treat other parts as adversaries

prevents the individual parts from coming together to cooperatively solve system-wide problems. The ultimate irony of this *'gaming' system* is that it not only does not solve the initiating problem of rising costs but it works against broad, cooperative efforts to solve the problem.

The *precipitating factors* for these escalating costs are not failures but successes. Despite various problems evident in the quality of care, American health care is considered worldwide to offer some of the most sophisticated medical care in the world. The product is highly desired by patients who can afford to pay for it.

Healthcare expenditures grew 6.9 percent in 2000 and 9.3 percent in 2002. A survey of employers, health care providers, and health plans showed that

- Employers plan largely to share cost increases with employees through increased employee premiums,
- Health plans expect to pass much of their cost on to employers, and
- Healthcare providers intend to increase preauthorization efforts.

The technology of information along with sound human practices is one of the few new technologies

Avoidable Error

The health care industry is not perfect. The people administering health care are also not perfect. They tire after 12-hour shifts. They at times must make quick decisions with very little support around them. Their handwriting at times is less than ideal and above all else they are human and whether we want to admit it or not, humans make mistakes. Because we in the health care industry are aware of our human characteristics that leave us exposed to the possibility of making mistakes we do everything possible to prevent those mistakes from occurring in the first place. Information technology can help. Medication errors in hospitals are frequent and may harm patients. Medication errors include incorrect dosing, incorrect drug given, or incorrect timing of drug administration. Medication administration is a primary responsibility of nurses, and error prevention is taught during their training. Still, competent nurses may make mistakes. An example of a device and information system that is in widespread use in hospitals today and that has dramatically decreased the number of medication errors is called Pyxis. Pyxis is a medication-dispensing computer that is maintained by the pharmacy, is located on each unit, and is stocked with medications for each patient on that unit. The patient's medication administration profile is updated in the system by the pharmacy and when medications are due to be given, a nurse, using password entry, signs into the system and obtains the medication. Medications can be obtained only when due and only in the correct dose required. The Pyxis system can be overridden, but the nurse must then take extra steps which in itself is a safety check. This computer-supported dispensing helps to prevent errors by nurses who are rushing and tired and who might otherwise be reading orders written in difficult to read hand-writing. Medication errors can still occur but are less frequent due to the enforced double check (pharmacy and nursing).

Figure "Avoidable Error": The drug administration system can help reduce error. This example is from a practicing nurse Lisa Bragg.

that could both improve care and reduce costs. If people agree to standardize data collection, to integrate networks of data, and to semi-automatically monitor practice by criteria both of low cost as well as quality care, then a system could evolve that would work against the negative, gaming situation currently in place. The primary obstacles to such an *information systems solution* are, however, not technological but rather political.

2.1.2 Medical Errors

Some estimates show that about 100,000 people die each year in the United States from *medical errors* that occur in hospitals. That's more than die from motor vehicle accidents, breast cancer, or AIDS. Indeed, more people die annually from medication errors than from workplace injuries. Add the financial cost to the human tragedy, and medical error easily rises to the top ranks of urgent, widespread public problems.

The startling statistics of medical error are at odds with the public perception of the incidence of error. Legitimate liability concerns on the part of health care professionals discourage reporting of errors. The Institute of Medicine (Kohn, et al, 2000) concluded that the problem is not bad people in health care--it is that good people are working in *bad systems* that need to be made safer.

Existing information systems, designed primarily for billing purposes, often fail to record important information about a patient's condition. A comparison of claims and patient records reveals that claims do not accurately reflect over half of the clinically important patient conditions. Even when information system software allows for the entry of additional information, that information often is incorrectly entered. The National Committee for Quality Assurance's audits comparing reported performance data with patient records have uncovered average error rates as high as 20 percent. These *audits* have uncovered a number of data quality problems, including missing encounter data, homegrown codes, and missing information in patient records (NCQA, 1997).

Important to *patient safety* is the ordering, transcribing, and administering of medications (see Figure "Avoidable Error"). A very common

A Failure to Share

by Han Trien

My grandmother died because there was no medical history available so that the physician could be aware of her condition and provide appropriate treatment to save her life. She always went to Washington Adventist Hospital for surgery and other procedures. All of her medical histories were at this hospital, and this is where her primary care physician was affiliated. One tragic weekend my grandmother went to see my mom in Burtonsville. That morning my grandmother told my mom that she was having stomach pain, and about noon the pain was still there and my grandmother felt tired and short of breath. My mom called the ambulance to take my grandmother to the emergency room. When the ambulance personnel arrived, they took her to Holy Cross Hospital. My mom said "no we want you to take us to Washington Adventist Hospital". The ambulance personnel replied "we must take her to the nearest hospital". When my grandmother got to Holy Cross Hospital the medical staff didn't know what to do. They asked us to give them my grandmother's medical history. Our family gave all the information that we knew to the nurse. After a few hours, my grandmother cried and asked why for medication. The nurse responded that the ER physician was trying to contact her primary care provider for further information so that the ER physician could determine the best treatment. Another hour passed and nothing was done to stop the pain. The ER physician decided to admit my grandmother to the hospital for further evaluation. After they took my grandmother to her room, still nothing had been done for the pain. My grandmother lay in bed and cried. Two hours later my grandmother went into cardiac arrest. Nurses gave her CPR and were able to bring her back, but she was in a coma and connected to numerous machines. For 10 days my grandmother never awoke or responded to the family. Finally, our family had to make the painful decision to remove the machine that was keeping her alive.

The problem was that Holy Cross did not have any medical records of my grandmother so the ER physician was not able to determine a treatment for her. Her primary care physician wasn't affiliated with the hospital; he didn't have privileges to access the facility. Think of the senseless deaths that are the result of an ER physician being unable to make an accurate decision on which care to give a patient.

Figure "A Failure to Share": A student Han Trien provided this story in response to an exercise about coordination problems in health care.

iatrogenic injury to the hospitalized patient is the adverse drug event, yet about half of all adverse drug events would be relatively easy to prevent. The most common error is in dosing which occurs three times more frequently than the next type. The top causes of failure include:

- prescribing errors due to deficiency in drug knowledge related to incorrect dose, form, frequency, and route;
- order transcription errors due to manual processes;
- allergy errors due to the systems poor notification to healthcare providers;
- poor medication order tracking due to a cumbersome, inefficient system, i.e. dose administration is recorded in more than one location; and
- poor interpersonal communication, i.e. illegible orders.

Proper information systems could reduce the incidence of these errors. For instance, computers could help by reducing the number of choices in the *Physician Order Entry* system so that physicians are only shown acceptable drug doses and frequencies.

2.1.3 Coordination

Because of its decentralized nature, the health care industry has a very complex business model consisting of a fragmented community of trading partners (i.e., hospitals, providers, group purchasers, pharmacies, clearinghouses, and others). Few other industries are *decentralized* to the same degree. The auto industry, for example, has a tightly coupled set of commerce partners. The mutual fund industry has employers, shareholders, and stock exchanges. In contrast, the health care industry is so fundamentally decentralized and yet so critically in need of data-sharing that the use of common or cooperating information systems and databases becomes an operational imperative.

Improvements in information systems also are needed to support the coordination of care. Health professionals and providers need access to a patient's treatment history, test results, and related information if they are to provide effective care. In most cases, paper records cannot be easily transferred between organizations. The problems are both technical and administrative (see Figure "Failure to Share"). Even in cases where computer records are kept, the use of different hardware and software configurations makes file sharing difficult.

Improved information systems must be able to generate *population-level data* that can assess the performance of the health system in caring for discrete populations. Public health officials would be better able to monitor disease outbreaks or the adverse effects of medications, procedures, or other products. Most existing information systems are not designed for these purposes.

Table: "Environmental Determinants of Organizational Structure"

Pace of Change	Environmental Complexity	
	Simple	Complex
Stable	Machine Bureaucracy	Professional Organization
Dynamic	Entrepreneurial Startup	Adhocracy

2.2 Professional Organizations

An organization's structure is affected by the variety one finds in its environment. Environmental variety in turn depends on both environmental complexity and the pace of change. Mintzberg (1979) identifies four types of *organizational form*, which are associated with four combinations of complexity and change (see Table "Environmental Determinants of Organizational Structure"). Each of the four organizational forms in Mintzberg's scheme depends on fundamentally different mechanisms for coordination.

The *professional bureaucracy* relies for coordination on the standardization of skills. Training and indoctrination first instill those skills in the new professional, and interaction with colleagues through time maintains the standardization (Beshears, 2001). The organization hires trained professionals for the operating core, and then gives them considerable control over their work. Control over his own work means that the professional works relatively independently of his colleagues, but closely with the clients he serves. Most necessary coordination between the operating professionals is handled by the standardization of skills and knowledge (see Table "Form and Coordination").

The *machine bureaucracy* generates its own standards. Its techno-structure designs the work standards for its operators and its line managers enforce them. The standards of the professional bureaucracy originate largely outside its own structure, in the self-governing association its operators join with their colleagues from other professional bureaucracies. The professional

bureaucracy emphasizes authority of a professional nature.

The professional organization is a specific organizational structure with a large operational core, a small middle line, a very small techno-structure for planning and standardizing organizational performance and a considerable support area to relieve the *highly-paid professionals* from as much routine work as possible. The structure is what distinguishes professional bureaucracies from both machine bureaucracies and innovative organizations.

The strategies of the professional bureaucracy are largely ones of the *individual professionals* within the organization, as well as of the professional associations on the outside. The professional bureaucracy's strategies represent the cumulative effect over time of the projects that its members are able to convince it to undertake.

The professional's technical system cannot be highly regulating, certainly *not highly automated*. The professional resists the division of his skills into simply executed steps because that:

- makes them programmable by the techno-structure,
- destroys his basis of autonomy, and
- drives the organizational structure to the machine bureaucratic form.

Like the machine bureaucracy, the professional bureaucracy is an *inflexible structure*, well suited to producing its standard outputs but ill-suited to adapting to the production of new ones. Change in the professional bureaucracy does not sweep in from new administrators taking office to announce major reforms. Instead, change seeps in by the slow process of changing the professionals - changing who can enter the profession, what they learn in its professional schools (norms as well as skills and knowledge), and thereafter how willing they are to upgrade their skills.

Table: "Form and Coordination"	
Organizational Form	**Coordination Mechanism**
Machine Bureaucracy	Standardize procedures and outputs
Professional Organization	Standardize professional skills and norms
Entrepreneurial Startup	Direct supervision and control
Adhocracy	Mutual adjustment of ad-hoc teams

The dominance of expert work affects the administrative structure in professional organizations. The administration lacks power relative to machine or entrepreneurial organizations and is *decentralized*. It provides professionals with more control over their own work as well as collective control over administrative decisions. The administrators typically spend their time handling disruptions and negotiations. Nevertheless, administrative structures serve a key role in creating the boundary of the organization. Often through this boundary creation, the administration gains power.

A small technical structure and a weak administration lead to a distinctive strategy process. The conventional way, in which central administrators develop detailed, integrated plans seldom works in the professional organization. Many strategic issues are controlled by individual professionals or require the participation of a variety of members in a complex *collective process*. The resulting fragmentation of activity discourages initiatives. This is one reason for the remarkable degree of stability in professional organizations (Wetzel, 2001).

2.3 Trends

Health care trends influence an organization's strategy and help drive the relevant information systems trends (see Figure "Trends"). The organization's strategy along with accessible information technology tools determines what the information systems needs are.

Structurally, the health care industry trend is to *integration*. Physicians who once practiced in solo groups are increasingly practicing in large groups. In the past, the boundary between providers and payers was sharp but that boundary is becoming fuzzy as providers offer health plans and insurers develop

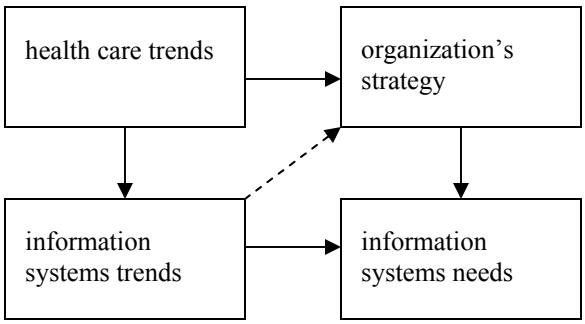


Figure "Trends": The national trends influence a particular organization's strategy and its information systems needs.

provider networks.

In the past, information systems were focused on collecting *billing data* from patient encounters. In the future these systems will pay attention to clinical data that is important in the delivery of care. Financial and clinical data will be collected and maintained.

In the past decision-support tended to rely on data archives and reflect patterns determined retrospectively. In the future, information systems should monitor data in real-time and provide decision support at the moment of care. Examples of this are *alerts* that are built into a system and let health care professionals know immediately upon doing something whether or not the system perceives this action as dangerous somehow.

Given an understanding of industry trends and of information system capabilities, an organization needs to have a realistic strategy as to how it will distinguish itself for its customers. One *business strategy* is to emphasize the development of physician networks. For a hospital this can be critical to getting patients referred to the hospital and treated by the doctors in the hospital. Primary care networks serve as important gatekeepers to hospitals.

Ambulatory care is typically less expensive than hospital-based care. Contemporary reimbursement schemes give preference to those who provide such ambulatory care. Thus primary care centers, diagnostic laboratories, outpatient surgical facilities, and other ambulatory care systems might be the strategic goal of a provider to emphasize. Likewise, home health care may be targeted.

Having reviewed the trends in health care and information systems and having established a strategy for the health care organization, the organization can specify its information systems needs. These needs can be viewed as common applications, specific applications, or technical infrastructure.

The common *applications* include things like data repositories that contain patient information. Information about the patient is needed in most other transactions in the health care organization. Specific applications would be, for instance, for the diagnostic laboratories, such as pathology and radiology, in an organization. A need for physician office systems is another example of a specific application need.

The *technical infrastructure* needs must be delineated. Does the organization need to have high-speed networks connecting all its components or can it rely on phone modems for connecting some entities? Must large database systems for handling thousands of simultaneous queries be available or is something much less robust adequate? These and other technological infrastructure questions must be answered before the full requirements can be specified.

While the information systems needs of any particular organization are highly context dependent, the general industry and technology trends allow the identification of weaknesses in the current information systems implementations. There is a need for a significant increase in *investment* in health information systems. Improvement in data quality and linkages between different health databases are also needed.

2.4 Questions

Reading Questions

1. In what sense are the escalating costs of health care the result of a gaming system? Identify the components of this system and how they interact.
2. Provide evidence for this statement: One of the tragedies of medical errors that cause death is that proper use of good information systems might prevent those errors.
3. How does the money invested in information technology by health care compare to that in other industries? How is this health care investment changing?

Doing Question

Relate two incidents where medical errors occurred and where better use of information systems might have reduced the likelihood of the error. Your incidents can come from the literature, your own experience, a personal acquaintance, or some other source, but you should note in the answer also your source. Explain the incident in enough detail that a layperson can understand. Structure your answer as follows:

- introduce your answer by providing the overview of the error situation and motivating your approach.
- describe incident ONE in a paragraph or more,
- describe how use of information systems might have reduced the likelihood of incident ONE.
- describe incident TWO in a paragraph or more.
- describe how use of information systems might have reduced the likelihood of incident TWO.
- generalize one of your incidents and describe technical approaches to it.

3 Analysis

Learning Objectives

- Construct a preliminary analysis and design for a health information system.
- Distinguish between approaches that successfully involve the client and approaches that do not.
- Compose a method of collecting requirements from health care professionals that visually presents information to them that they readily understand.

3.1 Life Cycle

An example of an admissions process for a patient as seen by a nurse depicts a typical use of computers in health care (see Figure "A Typical Case"). While the process is impressive in many ways, it also leaves open the possibility of improvement through re-design of workflow and introduction of further automation.

The *system development life cycle* remains largely unchanged over the years, though it calls increasingly for end-user involvement. The system development life cycle includes both the conceptual design and technical, functional and operational strategies. The conceptual design includes a vision statement that explains the intent of the information system. Assumptions about the organizational model and the environment in which it functions, as well as the interfaces and the potential problems, should be

In the Ambulatory Surgery Unit where I work, the registration process begins with the infamous "white card." This card is completed by the physician who requests that the patient be registered and/or admitted for her/his surgical procedure. The white card contains pertinent patient information such as demographics, insurance, medical service to which the patient is to be admitted, and procedure. The physician is affiliated with the hospital and usually sends the white card to admissions via inter-hospital mail from the clinic.

Admissions then generates a medical record and a medical record number for the patient by entering this information into a patient management information system. A "red card" (small plastic addressograph plate, like a credit card) is also produced for the patient, which includes the patient's name, medical record number, date of admission, and physician name. This red card, a demographics fact sheet, physician orders, previous test results, and old records are sent to our unit the day before surgery. The unit secretary then prepares a paper chart for the patient which includes the necessary paper documentation forms.

The patient is telephoned the day before the procedure and told to come directly to our unit the day of surgery. On the day of surgery, the patient registers with our unit secretary. The secretary asks the patient her/his name. The secretary then gets the patient's chart to see the medical record number. The secretary enters the medical record number into the patient management information system to verify that the required information is completed. The secretary also makes the patient sign an admission consent form which includes the patient's rights and insurance information. The paper chart then follows the patient's medical records.

On our unit almost all other documentation is done by paper. The only clinical information system to which we have access is a pathology laboratory system but only to view results and not to make orders. Lab tests and medications are ordered with a paper form. Radiology tests can be ordered by the physician entering the request for the test into a radiology clinical system or via paper.

Converting to an automated system on this unit would involve extreme process reengineering. I would hope that eventually this would happen. In two years, the unit will be in a brand new "state of the art" building, and I asked my manager if she knew if we would be using a computer system and she said that it was discussed, but all of the details were not finalized.

Figure "A Typical Case": These are the observations of an experienced Registered Nurse about the use of information systems in her unit.

explicit.

The *functional strategy* describes generic functions of the organization and specific clinical functions grouped by categories. The interrelationships among application areas and their current level of development should indicate what is not automated, what is moderately supported, and what is currently well supported. A technical strategy provides an overview of the technical environment and technical characteristics of the infrastructure. Integration considerations, particularly for heterogeneous systems, must be addressed. Evaluation criteria should specify the ability to meet functional user requirements under cost constraints. The acquisition strategy gives ground rules for in-house development versus outside sourcing. Selection criteria for outside sourcing include historical vendor performance. Responsibilities of the user, managers, and vendors must be clear.

The system development life cycle is basically the same in health care as in numerous other industries. However, what to expect in implementing the life cycle in a health environment is different from what to expect in other environments. The unique characteristics of the health environment and of health information systems are the focus of this book. The intention is to cover the principles and the applications of health information systems so that health care professionals, information systems specialists, and students of either discipline can better understand the constraints and opportunities that are shared.

3.2 Sample Requirements

The U.S. *Department of Defense* (DoD) has one of the world's largest health care systems and is typically in some stage of a major system upgrade. The deliberations and documents of the DoD process were available to the public. The detail at which the public could see the plans for a major HIS were phenomenal.

The vision and strategic initiatives of the *Military Health Services System* focus on accomplishing goals which:

- maintain readiness for joint operations in a global environment,
- improve health, and
- right-size the medical work force.

The *Clinical Business Area*, which comprises all clinical business processes and functions, supports delivery of health services and supports the vision of a computer-based patient record.

The Business Process Reengineering of the *Department of Defense Vision Information Services* (DVIS) addresses:

- three functional areas of Business Process Improvements (BPIs), functional system requirements, and product evaluation scenarios and
- three functional areas of Optometry, Ophthalmology, and Optical Fabrication Laboratory.

The DVIS workgroup included doctors, laboratory professionals, technical, and health records representatives from the Vision, Optical, and Eye Health disciplines.

The *DVIS workgroup* met for two, one-week workshops. The workgroup validated and augmented a previously defined DVIS Functional Area Model-Activity (FAM). In addition to discussion and presentations, the DVIS workgroup utilized groupware as a tool to facilitate the workgroup process.

The workgroup identified *process improvements* based on the DVIS FAM. The workgroup identified several hundred improvements to their business processes. Analysts refined them to 80 improvements. These improvements were then separated into eight categories, with each category further divided into system and non-system BPIs. The system BPIs were used in the development of the DVIS Functional System Requirements.

The analysts focused on mapping the Vision, Optical, and Eye (VOE) Health providers' *workflow* to the DVIS FAM. After this validation of the FAM, the workgroup separated into four subgroups. The subgroup topics were:

- Group 1. Develop Direction and Manage Resources;
- Group 2. Deliver Clinical Services;
- Group 3. Manage Optical Fabrication Process; and
- Group 4. Deliver Preventive Services.

The four subgroups then generated BPIs. The entire workgroup then reconvened to share findings. This process allowed the workgroup, as a whole, to propose the necessary BPIs, considering both their particular work and FAM. The group suggested approximately 200 BPIs.

The final *BPI statements* were organized into the following eight categories:

- VOE-wide Processes: There is a need for broad VOE process improvements, ranging from on-

line information to standardization of policies and procedures throughout DoD and the individual services. Improvements in this BPI category affect all areas of VOE service and its environment.

- Ensure Readiness: Readiness is the current ability of forces or systems to deploy and perform their planned mission. The current ability of forces to deploy and perform planned mission based on their vision, optical, and eye health status is a major BPI area that can be enhanced by the DVIS application. This provides automated query and reports regarding active duty personnel's VOE readiness status. Units and individuals must ensure they have the right information, supplies, and instructions to be VOE ready.
- Increase Productivity and Ensure Quality Care: The DVIS system supports diverse ways to increase productivity and ensure quality care. These options must be compiled, viewed, evaluated, and implemented. Use of multiple types of studies, analyses, outcome measurements, and benchmarks will determine how best to use resources to ensure efficiency and quality care.
- Manage and Trend Patient Encounter and Patient Information: To increase efficiency and improve service, there is a need to improve the tracking of patients and their orders. There is also a demand for the ability to trend different functions and variance tracking throughout the clinical encounter and healthcare facility.
- Manage Appointments, Access, and Scheduling: Automation of scheduling is of utmost importance. This type of support, with its automatic notifications, would allow the clinics to have more flexibility and increase productivity. The automated system would use diagnostic codes to prioritize appointments. There is a need to allow patients to gain access to the automated system to improve care.
- Manage Equipment, Facilities, Consumables, and Fiscal Resources: Proper management of equipment, facilities, consumables, and fiscal resources are vital to quality care.
- Prevent and Record Eye Injury: Historically, 10 percent of war injuries are eye-related. Further studies have shown that in peace time, and increasingly so in wartime, 90 percent of eye injuries were preventable. Fact-based effective countermeasures require a central database for eye injuries and diagnoses. This database will track personal and unit eye injury history, and specific eye hazard sites, to enable decision makers to identify effective protection.
- Promote and Organize Education and Training: Education regarding vision conservation and VOE readiness is important in order to have a VOE ready force. Plans, training programs and manuals must be developed to facilitate patient education using various training methodologies (automated patient instruction sheets, handouts, interactive software, and videos).

The eight categories identify *overall improvements needed* in the VOE system. Each category focuses on one main topic that affects the workflow of VOE professionals.

The delineation of requirements for a vision system in the military indicates at the top level the kinds of requirements that one can expect for a major component of a health care information system. Other components of the military health system might have similar requirements.

3.3 Collective Participation

Designing or redesigning processes in order to better meet customer needs is vital to business adaptability. Over 60 percent of all U.S. hospitals are involved in reengineering activities and billions of dollars are being spent in the name of reengineering (Walston and Kimberly, 1997). The professional character of health care providers has profound implications for how a systems analyst must proceed to analyze and design a system to support the organization. Whoever is involved in information systems (IS) development in health care has to nurture *collective participation* (Wetzel, 2001). Decisions cannot be made

- solely by a centralized administration nor
- based upon detailed in-house knowledge provided by a large techno-structure.

Neither the administration nor the techno-structure possess the required power, work resources, or available knowledge of organizational processes.

The low motivation among professionals to participate in collective efforts may also aggravate the situation. IS improvements are often perceived not to be in the interest of the professional. In some cases the benefits that IS implementation may bring the entire organization may reduce resources to certain individual units that will then resist the implementation. IS development projects may need to permanently sell the project to different units in the organization. The recognition of subtle *power plays* and existing alliances between various hospital units assumes a greater role in health care systems design

and implementation than in organizations where well-defined teams have strong authority over IS development.

IS development has to set *priorities* concerning which part or aspect of the organization should receive primary support and how this decision effects or influences other types of activities. Simple issues concerning how computers could be employed without disturbing sensitive conversations or how teams will share computers deserve careful consideration and are part of the design effort.

Interdepartmental cooperation is critical in hospitals. The cooperation is highly regulated and at the same time unique to each hospital. The systems analyst must appreciate this complexity.

3.4 A Failed Design Case

The management of a local hospital in a rural community in the United States initiated the acquisition of a hospital-wide *order processing system* (Huynh and Agnihothri, 2000). This system is to communicate and process orders primarily from doctors. These orders are patient related and include tests, x-rays, and medications. At present, a paper-based order processing system is used, as in many hospitals. To start the project, the hospital organized a committee with the president, chief information officer, the manager of nursing, a resident, a laboratory system coordinator, and a radiology coordinator. The wide range of needs from various departments, the diversity of orders, and the different order handling procedures all needed to be addressed.

Given time and resource constraints, the *preliminary study* was limited to the West Wing of the hospital. The West Wing was the largest and most active of the wings of the hospital, and its requirements were perceived to be in common with those of the rest of the hospital. First the processes existing were carefully documented. The West Wing specializes in heart patients, and has 40 nurses and 35 beds. The floor manager, nurses, and unit clerks were interviewed about the order processing system, and work at the reception center was observed. Two other departments that would receive orders and return values were also studied. Those departments had various needs as regards online notification and message content. Surveys of staff were circulated.

Next, a flowchart was developed to indicate the flow of information and what happened to the information. Data was collected and manually run through the *flowchart* to confirm its validity. The hospital processed an average of 95,000 orders per month and 25% of these came from the West Wing. Interviews were again done with staff with the flowcharts in hand to register their feedback.

According to the original plan, the next step was to be a second phase of data collection and revisions to the design. At this stage, however, a *restructuring* in management took its toll on the project. Top management became involved in other projects and did not give adequate support to this effort. Senior management did not convey the re-engineering message to the staff in a continuing way.

Many of the hospital staff were not familiar with the plan to automate order entry and were not necessarily supportive of changes. The actual intended users of the system, principally physicians and nurses were little involved in the requirements and design generation process. There was poor response rate from doctors to the surveys that were circulated. In fact, only one doctor replied to the survey. The radiology department noted that it did not intend to surrender any of its control over its current radiology system which would however be otherwise expected to interface with a new ordering system.

In reflecting on the needs of the hospital, the intention of redoing order processing in one sweep throughout the hospital was naïve. The logic of ordering is complex in the working hospital and connected to numerous existing systems, which cannot be readily removed. The cost/benefit analyses need to be carefully considered in advance, and the management and staff need to share a *vision* of where they want the hospital to go.

3.5 A Success Case

The patient puts high demands on the information processing requirements and design of hospital information systems (HISs):

- A patient requires different specialists and their coordination,
- His condition changes and necessitates changes in planned actions,
- He moves from place to place, but staff need the ability to locate him, and
- The patient may need attention any moment of the night or day.

With this as general background, three generic needs of the design team can be sketched as follows (Krabbel and Wetzel, 2000):

- Designers need to understand the relationships and interdependencies among activities. Each activity concerns the individual accomplishing a task and the organization assuring that the performance of the task meets diverse organizational requirements. For instance, a patient may want to stay in the hospital another night, and the health care provider may feel this is justified based on the patient's personal situation. However, the organization may want to consider whether the insurance will cover another night. These dual concerns of the individual and the organization require the designer to continually interact with users in providing first one (the individual) view and then another (the organization) view.
- The heterogeneity of user groups requires consideration of competing interests. The designers have to fight against narrowed perspectives and, at the same time, endlessly attempt to motivate an integrated solution against possible disadvantages for the individual units -- this requires an ongoing negotiation process.
- Since health care organizations often have little professional focus on organizational development, designers may have to initiate infrastructure developments. This leads to the need for illustrating the current and future work practice.

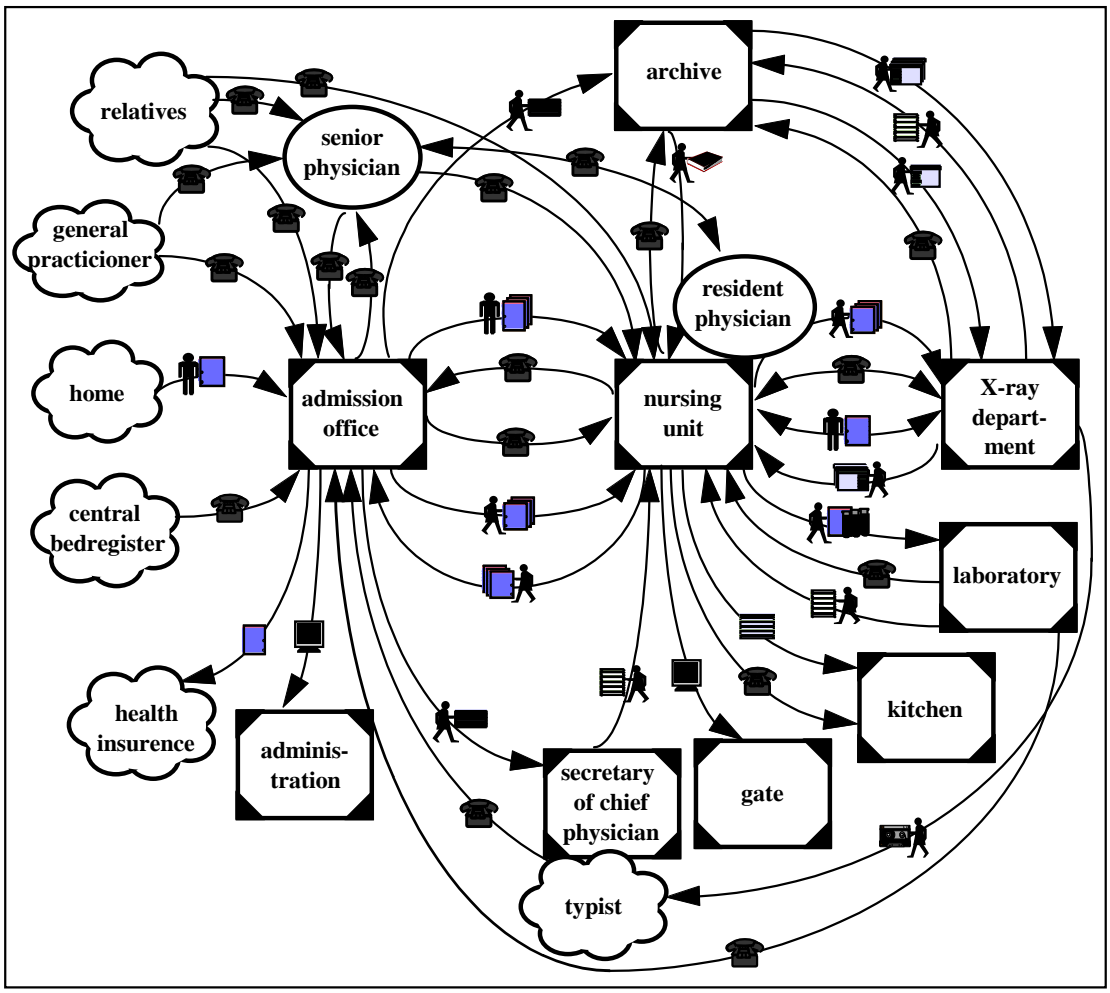


Figure "Cooperation Picture": Admission of a patient in the hospital domain. The flow of information is depicted by the arrows. The boxes represent units within the hospital. Copied with permission from Krabbel et al (1996).

An example is presented of applying these approaches to the acquisition of a *HIS* for a small acute care hospital with 230 beds and 560 employees. The project was embedded in the organizational development of the hospital and had participation from all departments: internal medicine, surgery, anesthesiology, nursing, administration, and technical. The new system was successfully acquired and then worked in several parts of the hospital beginning with patient administration.

3.5.1 Cooperation Pictures

The starting point for the analysis of current work practices is the use of qualitative interviews at workplaces. Interview partners are chosen following the concept of a functional role. The choice of actual person to be interviewed in each role should be made by the hospital. The interviews are performed in serial by small developer teams. The main focus lies on the learning and communication processes and not in the complete registering of each activity. The interviews must be held at the actual workplace to get an impression of the environment. *Scenarios* are used to represent the results of the interview. The beginning of a scenario is illustrated as follows:

- At least one nurse accompanies the physician during the daily ward round.
- The ward round takes place every morning. Each patient is visited. The nurse is responsible for carrying the patient record files.
- The physician gives orders for examinations, for changing the medicine, and the treatment and writes them down on the ward round form.
- After the ward round, the nurse transfers the examination orders to order forms, changes in medicine to the chart, …

Through these scenarios analysts quickly gain an understanding of the context and task performance in the workplaces.

Pictures promote the understanding, illustration, and feedback of the current work practices of joint ventures. The transfer of information and objects of work may be visualized. *Pictures* may represent

- places between which information and objects are exchanged,
- the kind of exchange in the shape of annotated arrows, and
- errands to be performed by staff and how patients make their way to different units.

In a picture for the admissions process there are

- six entities making phone calls to the admissions office,
- computer records sent to administration,
- paper records sent to the nursing unit,
- the patient sent to the nursing unit, and
- paper records sent to medical records and retrieved from medical records.

The picture (see Figure "Cooperation Picture") also shows other entities and activities.

The *Cooperation Picture* distinguishes between places outside and inside the hospital and certain roles, like a chief physician. Annotated arrows represent cooperation. In the hospital context the delivery of documents by the hospital staff, phone calls, data exchange via computer, and the patient making his way to the different units of the hospital are distinguished (see Figure "Symbols"). The arrows are annotated by pictograms indicating these different

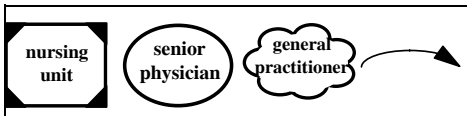
	Symbols for organizational units, functional roles, units/functional roles outside of the hospital and information transmission
	Icons for employee, patient, phone, computer
	Icons for employee with documents, tape, patient record, X-ray bag

Figure "Symbols": Selected symbols and icons for Cooperation Pictures are indicated here. A distinction is made between rooms for organizational units, roles that have no fixed room, and places or roles outside the hospital.. Patients and staff are differentiated in combination with different objects like the patient record, the X-ray bag, lists, order entry forms, cards, lab tubes, and tapes. Copied with permission from Krabbel et al (1996).

kinds of cooperation. A more detailed picture could focus on the process of an X-ray examination, where numbers are added to the arrows to indicate work sequences for a typical case. The focus in this analysis lies on the purpose of cooperation, since this is the more stable factor compared to the how of cooperation which might change.

Figure "Purpose Table"

Single Activities	Purpose
Physician writes the order on physician order form	Documents who ordered the test for what purpose and initiates the order.
Physician puts the order entry sheet in the nurse's in-basket.	Nurse is alerted that she has to act. She knows what is planned with her patient.
Nurse enters patient's name, other relevant data and the type of test on the order entry sheet	Nurse prepares the sheet in order to relieve the physician of such burdens.
Nurse enters the test on the patient's flow sheet.	Every member of the care team now is alerted to the order.
Nurse puts the order entry into the physician's mail basket.	Physician knows to validate the order.
Physician adds relevant clinical information to order and signs it.	The physician responsible for the test being done now knows who ordered the test and why.
Nurse carries the order to the radiology department.	The radiology department can initiate the scheduling of the test.
Radiology technician phones the ward to confirm a date for the patient to be brought to radiology.	The patient schedule is coordinated between the ward and radiology.

The Cooperation Pictures illustrate which errands have to be made by the hospital staff and how the patient makes his or her way to the different units of the hospital. They *objectify the cooperation* through 'places' and annotated arrows. This contrasts with the popular means of representing information systems in which merely abstract information passing is described.

In many workshop sessions, Wetzel (2001) found that Cooperation Pictures were very useful in initiating *active participation* of the heterogeneous groups in elaborating, discussing and sharing their activities. Cooperation Pictures supply an appropriate subject of discussion, which put users directly into the position to reflect together about their own organization. Users were able to elaborate on the picture and provide reasons for particular tasks. All workshop participants were surprised that within a regular admission of one patient, seventeen phone calls are made. Immediately, a discussion ensued about how to improve the process. For many users, the picture manifested for the first time that their work does not consist in caring for a patient only but that a significant portion includes tasks for cooperation and documentation purposes.

Tables supplement pictures by providing more detailed information at selected areas. They add information by naming the objects at the arrows in the picture and by describing the purpose or implications of individual activities (see Figure "Purpose Table").

3.5.2 The Kernel

Systems in the market sometimes neglect the cooperative parts of the task and only note the requirement, such as 'registration of the x-ray order'. Those systems may presume the physician performs the order entirely. Thus, the physician writes a note to himself about which patients should have x-rays, goes to the computer, and makes the required entries. The information for the nurse and others would thus be missing, and the physician would be doing more work than normal. The computer system must respect not only the accomplishment of the basic task of ordering the test but also of *coordinating* the work among the members of the health care team.

Parallel to the analysis of current work practices, a *task-oriented design* of functions needs to be ongoing. The complexity of the HIS necessitates agreement about the subdivision of tasks. For reducing complexity and supporting negotiation, a document called the Kernel System and another called Systems Stages are introduced.

For a HIS the content of the *kernel* is debatable. From the organizational point of view, the kernel should support tasks of key units that show a high cooperation profile. It must satisfy urgent needs of the organization and supply a basic and uniform infrastructure. For the case study here, the kernel

included patient administration and billing, admission/discharge/transfer, procedure codes, and communication. These were connected to non-kernel systems, including surgery, radiology, laboratory, medical records, dietetics, and administration.

Each user group has its own profession and perspective. These groups compete and are able to varying degrees to exert their will on other groups. Each group wants an optimal solution for its own work, whereas aspects of integration are less important. Additionally, each group may want to be autonomous and to be served immediately. If not enough players advocate an integrated solution, then the project will fail. The agreement on the kernel system is a key step in *integration*. A pictorial representation of workflow and of the kernel can help understanding.

The kernel will typically be too large and complex to be readily understood without further explanation and analysis. Accordingly, *system stages* are introduced in which the workflow through the kernel is divided into steps. In the case under study, the stages began with these 3 steps:

1. patient administration,
2. admission, transfer, and discharge, and
3. nursing workload.

These do not need to be done in that sequence but making steps for people to understand the exercising of the kernel facilitates understanding. As systems will be assessed for their suitability, the existence of this step-by-step walk through the kernel can make it easier for staff to test the systems and determine their suitability to the hospital.

3.5.3 Prototype

Two further steps are appropriate in this preparation of the hospital to procure a HIS:

- system visions need to be elaborated and
- prototypes for selected functions built.

The *system vision* would give users expectations of what to see in the system. Examples of systems visions for this case study are:

> The ward group workplace shows an information area and a working area. The information area provides general guidance without logging into the system. The working area is accessible only after logging into the system and then provides the user with tasks.

Prototypes are operational models of selected aspects of the future system. Prototypes are developed with regard to single tasks, the arrangement of group workplaces, or the design of cooperation tools. The prototypes make concrete the system visions. They allow users to interact with a computer screen and get a realistic sense of how the system might behave for them although the prototype is not connected to real data or the rest of the hospital activity. The prototypes would show actual screens with dummy patient names and staff names with tasks to do, proper color-coding or whatever else had been deemed important in the scenarios and visions.

3.6 Another Success Case

Another *case study* is used to illustrate the complexity of the design process for a HIS. Calgary General Hospital in Calgary, Canada designed a modularized HIS that depended heavily on a kernel containing masterfiles (Ross et all, 1991). A masterfile is an index for large amounts of information on a particular subject. The Calgary masterfile is hierarchical and includes:

- the hospital masterfiles contain information general to the hospital, such a valid financial classes,
- the department masterfiles contain information specific to a department, such as telephone number, and
- the procedure masterfiles contain the most specific information and cover each procedure, test, or diet that patients may receive.

At *Calgary General Hospital* there are 800 diagnostic imaging procedures alone. Masterfiles indicate all required entries related to a specific test or procedure. For instance, an entry may specify that ‘height, weight, and blood pressure are required for the test’.

Individuals from different departments in Calgary view the same function performed within the hospital differently. Upper management has the global view. Within departments, staff may have a clear understanding of how their area performs but may be unfamiliar with how those functions support other departments. Since all departments access the masterfiles, all departments should have input into the design of the masterfiles. Calgary also found appropriate the establishment of a *masterfile analyst role* that was filled by a nurse with broad experience of different departments. The work of this role is not finished when the system is implemented but is a permanent position, as the masterfile needs to be maintained across time.

The preparation for acquisition of a system from the marketplace is an enormous task. The hospital should not simply buy a system. The hospital should carefully analyze its own *workflow* and understand

what it wants to achieve. Such self-study will be crucial to the use of any purchased system. Even if multiple systems exist that could equally well satisfy the needs of the hospital, the ability to successfully use a system requires careful forethought, training, and planning all of which are best initiated before the system is purchased rather than afterward.

3.7 Questions

Reading Questions

1. Compare and contrast the design approaches in the sections 'A Failed Case' and 'A Success Case'.
2. How were pictures and purpose tables used in the success case and why did they help?

Doing Questions in Brief

1. Try to identify someone or find information somewhere that provides further information about an analysis and design case for a health care information system. Describe how that case was done and compare and contrast to the cases described in this chapter.
2. The analysis done that involved significant discussions with staff from the workplace and organizational views seems to have been more labor intensive and user-sensitive than the DoD vision analysis. Is this your impression and if so, what do you think would account for this difference and what do you think would be the end-result? You might study the military CHCS site and look for evidence of how the analysis and design was done and assess it relative to the experiences suggested in this chapter.

Doing Question in Detail

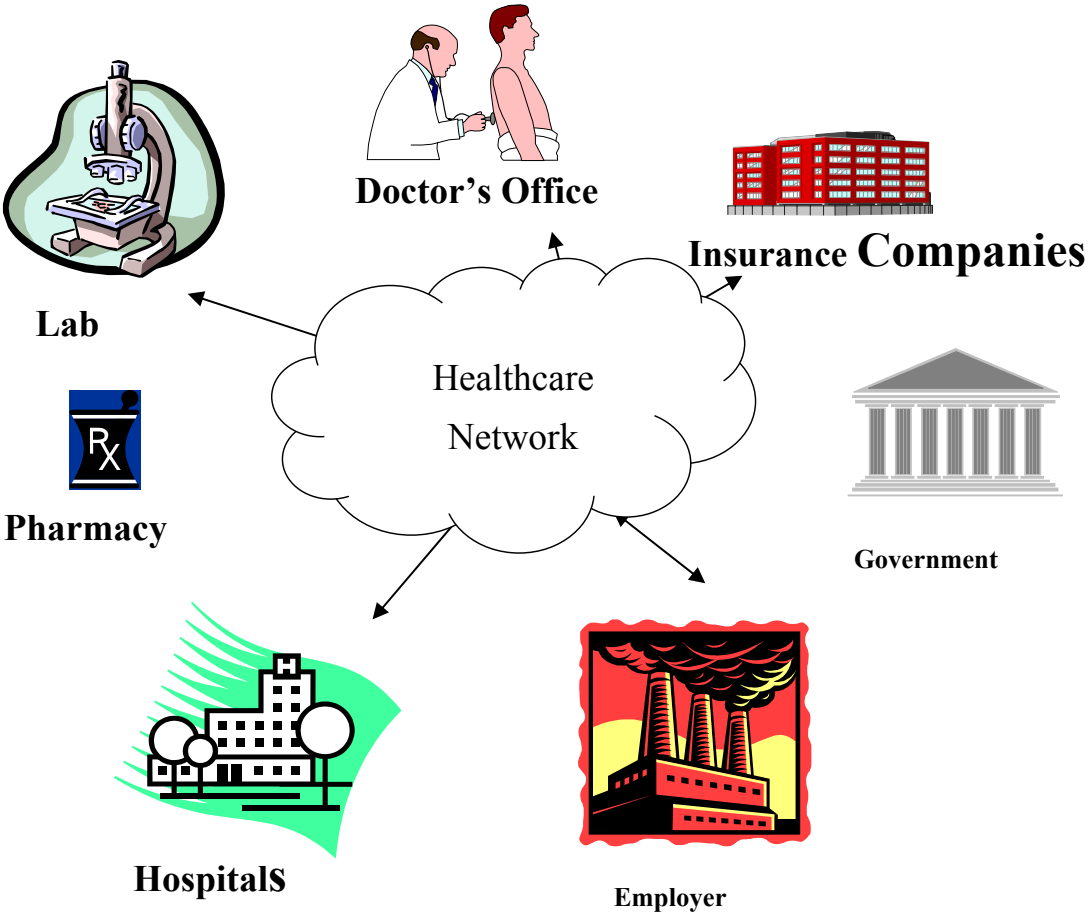
Consider that you are to design a web-enabled information system to connect you and your primary doctor's practice. This is not the design of an interface for the patient but also an information system that works with the doctor's office. Consider in your design what the people in the office need to do to maintain their side of the deal.

Enlightened by the analysis and design method of Krabbel and Wetzel (1996) you must demonstrate a

1. scenario,
2. Cooperation Picture, and
3. Purpose Table.

for your system. For the cooperation picture obtain your own symbols and provide a table explaining what symbols mean what. You can do this by choosing from clip art widely available. A handful of icons or symbols is enough for the symbol table. The Cooperation Picture does not need to depict the entire scenario but rather to indicate your understanding of the significance of a Cooperation Picture. A few icons and labeled arrows is enough. The Purpose Table needs only to describe what you put in the Cooperation Picture.

Part II: Providers and Payers



4 Providers

Learning Objectives

- Distinguish the types of health care systems serving middle-class families, poor families, and military personnel
- Diagram the major components of a hospital information system and indicate at least two subcomponents of each.
- Describe the flow of information in patient management.
- Demonstrate how characteristics of patient information peculiar to a clinical unit, such as radiology, lead to unique characteristics of the information system underlying that system.

The official definition of a *healthcare provider* is broad. It encompasses institutional providers such as hospitals, nursing facilities, home health agencies, outpatient facilities, clinical laboratories, various licensed healthcare practitioners, and durable medical equipment suppliers. Any individual or organization that is paid to provide healthcare services is a healthcare provider.

4.1 Components

The major structural components in a typical large health care information system, such as hospital information systems, are:

- administrative systems,

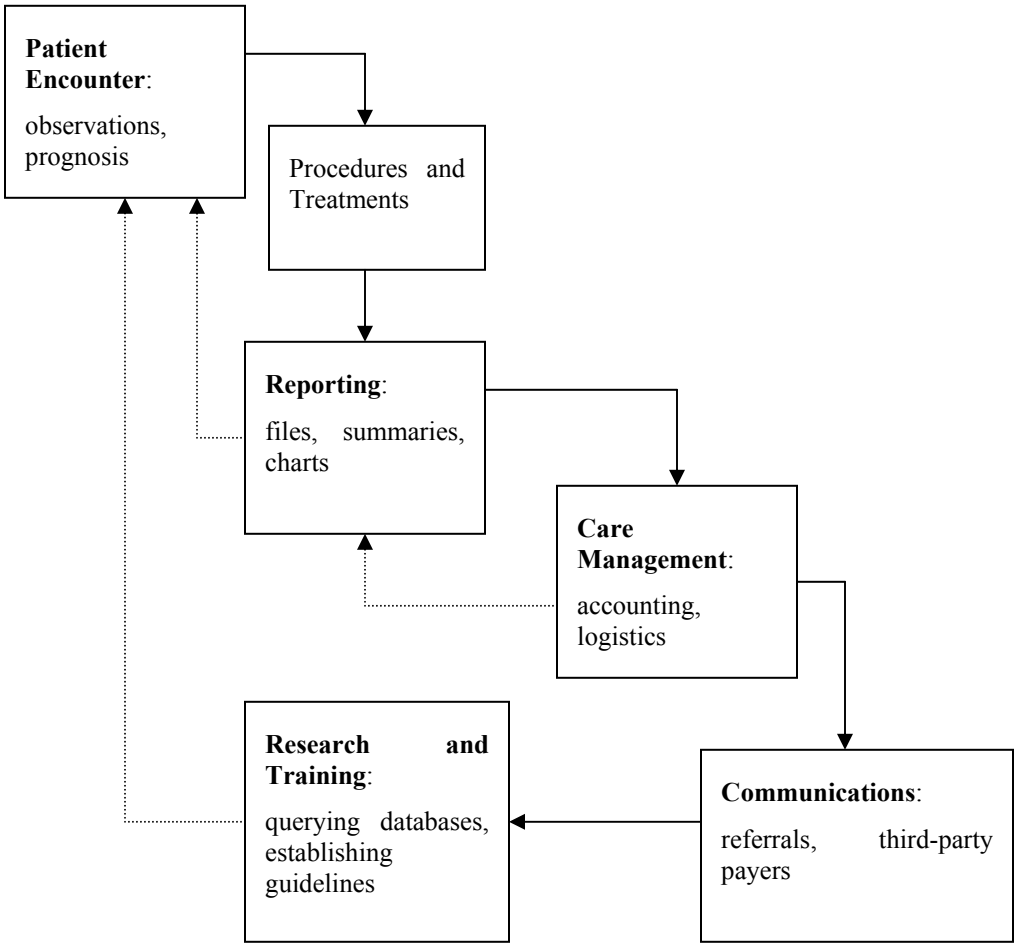


Figure "Functions of Patient Management": The waterfall of actions from patient care management to communications with external parties is matched by a feedback loop (adapted from Smith, 2000).

- clinical support systems, and
- patient management systems.

Administrative systems include accounting, finance, and strategic systems. Clinical support systems include pathology laboratory, pharmacy, and radiology. Patient Management includes admission/registration, medical records, and order entry.

Functional analysis helps to define what the information system is to do. Structures, on the other hand, are prerequisites for effective function. Functional analysis shows that the patient is first examined, then procedures are ordered or treatments initiated, followed by reporting on these efforts. Care management includes accounting and other administrative functions. Research and training may occur relative to the collected information and feed into the next round of patient management (see Figure "Functions of Patient Management").

The migration of patients from inpatient to outpatient settings necessitates new functions in the outpatient section. *Outpatient systems* assist with appointment scheduling, registration, medical records, insurance eligibility, service pricing, and billing and collections. These features are reflected in the core functions of the systems in larger provider organizations. The outpatient management system may also directly connect with a hospital information system so that access to records of a patient and various resources is most direct. Physician offices may have a miniature version of all these systems and also may be connected to hospital systems.

4.2 Administrative Systems

The *administrative systems* include patient accounting, scheduling, financial management, and strategic information systems.

4.2.1 Patient Accounting

Patient accounting systems are one of the most popular HIS applications. By the mid-1980s many different accounting systems were in use. The patient and payer accounting application performs the following major tasks (DeLuca, 1991):

- patient service pricing,
- patient billing and insurance claims,
- electronic data interchange,
- receivables management, and
- payer logs.

Patient service pricing determines the price of a service or checks the price of a service when proposed by another module in the health care information system. This pricing determination is a complex function. A wide range of services may be provided for patients in various categories, such as inpatient, outpatient, and emergency room, and the pricing varies with all these factors. Furthermore, Diagnostic Related Groups may be assigned by another module and for some payers will determine the price that can be attached to services for a patient. Additionally, various exclusions and limitations may be required for contracts with various service contractors, and this further complicates the pricing function.

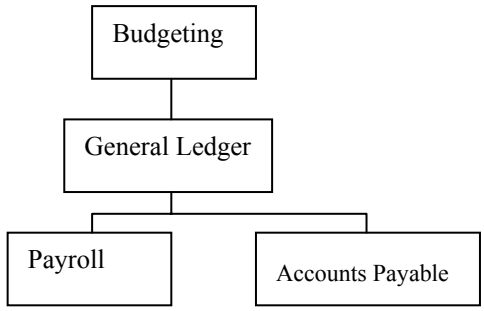


Figure "General Accounting": This diagram shows the payroll and accounts payable feeding into general ledger and then budgeting.

The charges for services must be converted into bills. Different payers have historically expected different formats for the *claims*. Historically, insurance companies, Medicare, Medicaid, intermediaries, employers, guarantors, and patient may each have expected a different format for a bill. The diversity of claims formats has changed with the implementation of the Health Insurance Portability and Accountability Act.

For a given patient, whether inpatient or outpatient, multiple bills may need to be generated to accommodate a range of payers for those services for a single patient. Increasingly claims are submitted electronically and payments also sent electronically. The accounting system would handle this *electronic data interchange*.

Receivables management keeps track of the bills that have been generated and what has not been paid is flagged for a further collection effort. Thus, if a patient is late in paying or has underpaid, then the receivables management subsystem might automatically generate a reminder bill. If a reminder bill is unsuccessful, then the receivables management subsystem may next notify the collectors of the need to pursue the patient.

Payer logs are generated, usually on an annual basis, by the accounting system to facilitate negotiations

with payers. If a provider treats many patients of one payer, then the payer may give that provider particularly favorable business conditions.

4.2.2 Scheduling

Enterprise scheduling helps bring disparate organizations together and optimizes resources (Kissinger and Borchardt, 1996). A scheduling system controls the use of services or limited-access resources, such as magnetic resonance imaging (MRI) equipment. Scheduling systems may automate various administrative tasks, such as searching for available slots, maintaining a waiting list, generating medical record pull chart instructions, scheduling recurring appointments, and scheduling multiple resources, such as room, equipment, and staff. A surgery center, for example, may require the ability to block and schedule rooms, equipment, and staff based on pre-defined requirements. As a first step, a surgery center may allocate rooms based on specialty (see Figure "Allocate Rooms"). In this case, specialists from different groups know when they may schedule their patients for procedures in the surgery center. If they do not confirm the room at least 24 hours in advance, the room may be released for rescheduling.

Scheduling systems were developed to serve *niche markets*. Systems developed originally for inpatient facilities may be strong in their ability to support resource scheduling, like an MRI, but may be weak in their ability to schedule services, like a doctor examination. Conversely, scheduling for outpatients may be strong in their ability to support services scheduling but weak in resource scheduling.

To realize the potential of scheduling to help an organization requires either connecting existing systems or replacing them with an enterprise-wide system. Several vendors now offer *enterprise-wide scheduling systems* that they created by expanding on the niche products.

A number of control and operation issues challenge the organization trying to implement a system-wide enterprise scheduling solution. First, most departments are reluctant to allow staff from other facilities to schedule appointments in their facility. This *control problem* must be resolved administratively. Second, the new system will have to offer all the functionality of the previous niche systems, otherwise the niche units will object to the new system. Third, the new system will have to link to both legacy systems and the hospital information system in order that adequate information is available to semi-automatically exploit enterprise-wide scheduling.

An example of the challenge of linking a scheduling system to the *legacy system* follows. St. Agnes Hospital in Fresno, California uses vendor X's hospital information system. St. Agnes has linked X to vendor Y's scheduling application. Requests for appointments are called into a centralized scheduling site where operators schedule the procedures on the Y system. Demographic information is then automatically retrieved from system X. Scheduling results are then routed from Y to X. Scheduling information is maintained on X to provide access to hospital-based users. Furthermore, St. Agnes uses Y's materials management module that links into Y's enterprise-wide scheduling system. With this link, materials are automatically ordered based on the scheduled procedures.

Many *linkages* are possible. Scheduling systems may be linked to transportation systems. Additionally, many tests that must be ordered when certain procedures are scheduled can be automatically put into the order-entry system by the procedure scheduling system. Further integration is possible as staff allocation systems calculate staffing based on procedure schedules. The possibilities are endless.

To facilitate the development of enterprise-wide scheduling, a standards development organization has developed messaging standards for scheduling. The basic structure involves placer, filler, and querying applications. A placer application requests the booking, modification, or cancellation of a schedule; a filler application owns a schedule for services or resources, and a querying application gathers

	OR #1	OR #2	OR #3	OR #4
Monday	General Surgery	Orthopedics	Cardiac Surgery	Pediatric Surgery
Tuesday	General Surgery	Orthopedics	Vascular Surgery	Gynecology
Wednesday	General Surgery	Plastic Surgery	Neurosurgery	Urology

Figure "Allocate Rooms": Surgery rooms allocated by specialty across weekdays. OR means Operating Room.

information about a particular schedule. The filler application connects the placer and query applications. Standardizing the format of messages among these applications helps health information systems integrate scheduling.

4.2.3 Financial Management

A *financial management system* includes general accounting and resource management:

- *General accounting* includes payroll and accounts payable that feed into general ledger, which in turn supports budgeting. The payroll module tracks hours worked, computes vacation days and tax withholdings, and so on. The module produces the paychecks. The accounts payable module converts a purchase order into a financial obligation and eventually a check to a supplier or vendor.
- *Resource management* includes human resources, maintenance management, and fixed assets management. The human resources module maintains employment history and might be used to link quality control and incident reporting to the individual employee record. The fixed-assets module lists each piece of capital equipment, its physical location, depreciation schedule, current book value, and insured value.

When integrated with the resource management system, the accounts payable system becomes more complex but can provide further services, such as allowing the receiving unit to automatically match the arrival of a purchased item with the purchase order and confirm that what has arrived is indeed what was ordered.

4.2.4 Strategic Information Systems

An organization needs a strategy for achieving its vision. Information systems can provide support in refining and implementing this strategy. Such information systems may be called *strategic information management systems*.

Strategic information management systems may have multiple sub-systems:

- A cost accounting sub-system will collect a large amount of cost data and produce a cost per procedure. From this can be computed such things as cost per case and then per case profitability.
- Case-mix analysis modules analyze the diagnosis distribution of outpatients and inpatients. Reports on utilization aid in analyzing patient trends and physician order patterns. Case-mix systems may typically be part of a patient accounting system.
- Financial modeling systems perform simulations of revenue and expense patterns based on differing assumptions. For example, changes in case mix can be the basis for different revenues and based on the results of financial modeling, the organization may decide to encourage a shift of patients from inpatient to outpatient.

At the opposite end from strategic information systems, are the bread-and-butter tools that staff use, such as *office automation tools*. Office automation provides for centralized calendaring, telephone messaging, and electronic mail. Office automation can help in many routine ways and provide a substantial productivity boost at relatively low risk. Some of the features, such as calendaring, that are supported with office automation might be incorporated in more advanced systems such as workflow management systems. The ability to compose, share, and track messages is important for many communications that occur in the management of the organization but are not directly linked to patient care.

4.3 Patient Management

Managing the patient and his record is a complex process. The patient has to be admitted or registered and associated with a unique identifier. Diagnoses should be coded into some standard nomenclature. Orders that are entered should be connected to a billing system and to the medical record system.

4.3.1 Admission

Patient admission is for admitting a patient to a hospital. Admission includes the following functions to:

- collect enough demographic, clinical, and financial information to supply the patient care, clinical, patient accounting, and medical records applications with data;
- produce forms that patients must sign, to include admitting forms, consent forms, and insurance benefit assignments; and
- notify housekeeping, security, volunteers, and other departments as room transfers and discharges occur. The midnight census is balanced through this application, and daily room and bed charges are generated.

Registration is similar to admissions but is for registering an outpatient rather than admitting an inpatient.

An admission and registration information system might be a freestanding system. Alternately, the admission and registration functionality might be provided in another package, such as a patient care system or an accounting system. These other systems need the information provided by admission and registration and need to know the structure of that information. If a health care organization gets different systems from different vendors, the health care organization then needs to decide which admission and registration system to use. Whatever the choice, the health care organization then faces the difficult task of *integrating* the systems that may make contrary assumptions about the admitting and registration data.

A vignette of a registration system is presented for a *remote laboratory system*. The patient goes to the laboratory to have testing done.

> The patient first provides either a paper order or a pointer to an electronic order. The order from the physician details the patient demographics, insurance information, tests to be performed, and diagnosis. The nurse or phlebotomist inputs the order or retrieves the electronic data, if the physician placed the order electronically. After the patient name is entered into the registration system, the information is passed to the medical records management system. The medical records management system determines if the patient has a record on file. If so, it compares the data on file to previous records and asks the nurse/phlebotomist to verify anything that may have changed. If this is a new encounter, a medical record number is assigned to the patient and the data is passed back to the registration program. If the patient was found to have previous records, the registration system then passes the patient medical record to the patient account system which verifies that there are no outstanding balances due to rejected claims. If there are outstanding claims, the nurse/phlebotomist is asked to verify the patient's insurance information. At the same time, the patient account system also checks the patient's insurance guidelines to verify that all required information to submit a claim has been provided and to determine if the insurance may deny the claim due to limited coverage or limited frequency. (An insurance company may deny a claim because the diagnosis provided by the ordering physician, according to the insurance company, does not warrant the test or procedure. An insurance company may also deny a claim because the test or procedure may only be performed once over a certain period. For example, Medicare will only pay for a PAP Smear once every three years). After resolving any patient account issues, the registration system generates a requisition with accompanying forms, if needed. Finally, the data collected through registration passes to the laboratory system. Regardless of how the order was placed, some state laws require a paper requisition be submitted. (So much for the paperless office!)

The admission or registration process is one of the most crucial in patient management because the identity of the patient is first determined here.

4.3.2 Medical Record

The *medical record* may be seen as a set of attribute-value pairs for a given patient at a given time. For example, an attribute might be heart rate and the value might be 60. The basic medical datum has four elements:

- the patient identifier,
- an attribute (for example, heart beat),
- a value of the attribute (for example, 60 beats per minute), and
- the time the value of the attribute was collected.

Depending on the attribute, the value could be narrative (for example, history of illness), numerical (for example, heart rate), signals (for example, electrocardiogram), or images (for example, chest x-ray). Before the era of instrumented tests, a record did not necessarily contain many test results, but now the record typically includes numerous test values.

The earliest medical records were *time-oriented*. Hippocrates said the medical record should accurately reflect the course of the disease. A record would thus be a list of attribute-value pairs sorted according to when the value was recorded -- in other words, chronologically sorted.

Lawrence Weed proposed in the 1960s an alternate structuring of the medical record that focuses on identifying the problems of the patient and the plans to resolve the problems. This is called the *problem-oriented medical record* structure. In the problem-oriented medical record, the notes are recorded for each problem assigned to the patient. Each problem is described according to the patient's complaints, physician's findings, interpretations, and plan. The modern day American medical record is a mixture of

the problem-oriented medical record and the time-oriented medical record.

Originally, medical records were *physician-centered* in that a physician knew only the records that he or she maintained. The Mayo Clinic in 1907 began the movement to patient-centered records in which different Mayo Clinic doctors taking care of the same patient would share the medical record. Generally, in the United States the hospital or clinic that cares for a patient retains the record. The physician tends to consider him or her self to be the owner of the record because he or she created it and only allows the patient to see it under special circumstances. The HIPAA Privacy Rule basically requires health care providers to give a patient a copy of his or her medical record anytime the patient requests it.

Electronic medical records offer numerous benefits. Multiple users from remote sites can simultaneously access the same medical record. Different views of a given record can be dynamically generated. For instance, the physician may want to see all the blood glucose values from a half-year period sorted chronologically or might want to see all the laboratory values of a particular day. Decision-support tools can be readily integrated into an electronic medical record. Summary data across patient records can be readily generated.

Historically, managing patient information (collecting information accurately, storing it, retrieving it, and properly sharing it) has been handled poorly. A quote from *Florence Nightengale* published in 1863 sounds like it could be said today (see Figure "Nightengale"). Collecting accurate data consistently is a problem of the doctors and nurses. Managing the medical record in a hospital is in part the responsibility of the medical records department.

The medical record is a guide to, and continuous record of, treatment while the patient is in the hospital. After discharge it becomes an archival record available for retrieval if the patient is re-admitted or requires further treatment as an outpatient. Medical records also support medical audits. Finally, they support research. To accomplish this myriad of functions, sound *records management* is needed.

Medical records management assigns a medical record number to a patient who is being seen for the first time by this provider. When the patient is admitted or registered, the communication between the admitting/registration system and the medical records management system must determine whether a patient has already a record in the system or is a first-time patient. To facilitate these determinations

> an urgent appeal for adopting … some uniform system for … records of hospitals. There is a growing conviction that in all hospitals, even in those which are best conducted, there is a great and unnecessary waste of life … In attempting to arrive at the truth, I have applied everywhere for information, but in scarcely an instance have I been able to obtain hospital records fit for any purposes of comparison.

Figure "Nightengale": This quote from Florence Nightengale (1863), the mother of nursing, reflects the disorder of patient records in the 19th century but might be said today too.

the medical record management unit maintains a *Master Patient Index* that contains enough of a record for each patient to allow accurate determination of whether an arriving person already has a record in the system or not. Unfortunately, this Master Patient Index combined with the information that some patients bring to the provider prove inadequate too often, as a patient is either matched with the record of someone else or is given a new, empty record when in fact the patient already has a record in the system.

The medical records department is responsible for *transcription processing*. Doctors may orally dictate reports that need to be rendered into textual form or they may hand-write information on one form that needs to be transcribed into another form. In addition to transcription, the medical records department is responsible for tracking the location of charts and for assuring that charts are complete. If, for instance, some document needs a signature but has been put in the chart without a signature, then the medical records department should detect this omission and obtain the correct signature for the document.

To avoid some transcription costs and to facilitate access to records stored digitally rather than in paper, a popular approach in medical records departments has been to scan and digitize medical records and store then as images. The high-capacity physical media for storage of digital information, the increasing computer power for processing of images, and the advances in imaging and workflow technology have underpinned the growth of *document imaging systems*. When the Jewish Hospital Healthcare Services adopted a document imagining system, delays in getting old charts were

reduced and records became available to more than one person at a time (Odorisio, 1999).

Since all medically oriented systems contain some portion of the patient's medical record, the point at which a system qualifies as a *record system* requires clarification. An admission system, though it contains demographic data, is not a patient record. A radiology system that contains an x-ray is not a patient record. The key factor in the design of the computerized record system is that it should be a physically distributed system with logical central control of the entire record. The central system should provide integrated and coordinated use of the data (Smith, 2000).

In the future within either patient care systems or medical records systems, certification modules may be included. A *certification module* will help providers assess whether a patient's symptoms meet the criteria for treatment and whether this intervention should have in-patient or outpatient status. This kind of assessment is particularly important where the provider is accepting capitated payments.

4.3.3 Order Entry

The most basic capability of patient care management is *order entry*. A physician might write an order onto a patient chart, and then a nurse or unit secretary enters that order into the nursing station terminal. Alternately, the physician might enter the order directly into the computer. Such direct order by the physician facilitates pre-emptive quality control feedback by allowing the doctor to receive warning about potential drug-drug interactions incurred by a new drug prescription or other such warning.

The order entry data will also be connected with the *service pricing system*. Thus orders that generate charges are automatically and immediately added to the patient's bill. This electronic capture of charges is one of the immediate, financial incentives for order entry within the health care organization.

The patient care management system should not only send the orders from the originating department to the department that might fulfill the order but should also permit the flow of information in the other direction. Thus an order of a x-ray to the radiology department might go directly to the radiology department from the ward, lead to the scheduling of the patient for the x-ray, and be followed by an electronically submitted radiologist's report being associated with the patient record online as soon as the *radiologist's report* is completed. The same flow of information and service would apply to pathology laboratory orders.

The concept of 'computerized order entry' is commonplace in enterprise-wide information systems. If someone in a factory needs to order more screws, then placing that order via the computer makes sense. In health care the concept has been slow to be accepted in practice, but new forces may accelerate the adoption of computerized order entry. In particular, the interest is in computerized physician order entry (CPOE) that includes decision support and is specific to prescriptions. In this context, CPOE refers to computer-based systems of ordering medications, which automate the medication ordering process and include Computerized Decision Support Systems of varying sophistication.

CPOE ensures standardized, legible, complete orders by only accepting typed orders in a standard and complete format (Kaushal and Bates, 2001). Basic clinical decision support may include suggestions or default values for drug doses, routes, and frequencies. More sophisticated decision-support systems can perform drug allergy checks, drug-laboratory value checks, drug-drug interaction checks, in addition to providing reminders about corollary orders (such as prompting the user to order glucose checks after ordering insulin) or drug guidelines to the physician at the time of drug ordering.

Adverse drug events (ADEs) are injuries that result from the use of drugs. An example of a preventable ADE is the development of rash after the administration of ampicillin to a known penicillin-allergic patient. *Medication errors* refer to errors in the processes of ordering, transcribing, dispensing, administering, or monitoring medications, irrespective of the health of the patient. One example is an order written for amoxicillin without a route of administration. Studies show that CPOE can substantially decrease medication errors. One study demonstrated that CPOE reduced medication error rates by 55%-- from 10.7 to 4.9 per 1000 patient days (Bates et al, 1999). Another study demonstrated a 70% reduction in ADEs after implementation of a CPOE system (Evans et al, 1997).

The cost of purchasing and implementing large commercial CPOE systems varies substantially, but may be on the order of tens of millions of dollars. Healthcare systems must garner both financial and organizational support before introducing CPOE. CPOE requires a large up-front investment. In addition, CPOE impacts clinicians and workflow substantially. Its complexity requires close integration with multiple systems, such as the laboratory and pharmacy systems.

The Leapfrog Group is a consortium of more than 100 large companies that provide health benefits to

over 30 million Americans (www.leapfroggroup.org). The Leapfrog Group's mission is to

- make the American public aware of a small number of highly compelling and easily understood advances in patient safety; and
- specify a simple set of purchasing principles designed to promote these safety advances.

Leapfrog Group member companies agree to adhere to a common set of purchasing principles in buying health care for their enrollees, including:

- Rating and comparing major healthcare providers' safety efforts and
- Holding health plans accountable for implementing the Leapfrog purchasing principles

The Leapfrog Group has developed a CPOE standard. In order to meet Leapfrog's CPOE standard, hospitals must:

- Require physicians to enter medication orders via computer linked to prescribing error prevention software;
- Demonstrate that their CPOE system intercepted at least 50% of common serious prescribing errors; and
- Require documented acknowledgment that the physician read the directives to any override.

The Leapfrog Group will invite hospitals with CPOE systems to warrant that their systems meet these three CPOE standards.

Other organizations support CPOE. A Medicare Payment Advisory Commission suggested instituting financial incentives for CPOE implementation. California enacted legislation stipulating that acute care hospitals implement information technology, such as CPOE to reduce medication-related errors.

4.3.4 Military Health System

An example of an integrated system on a large scale is the Department of Defense Military Health System (MHS). The *Composite Health Care System* (CHCS) integrates data from multiple sources and displays the data at the point of care in the form of a life-long Computer-based Patient Record (CPR). This CPR is

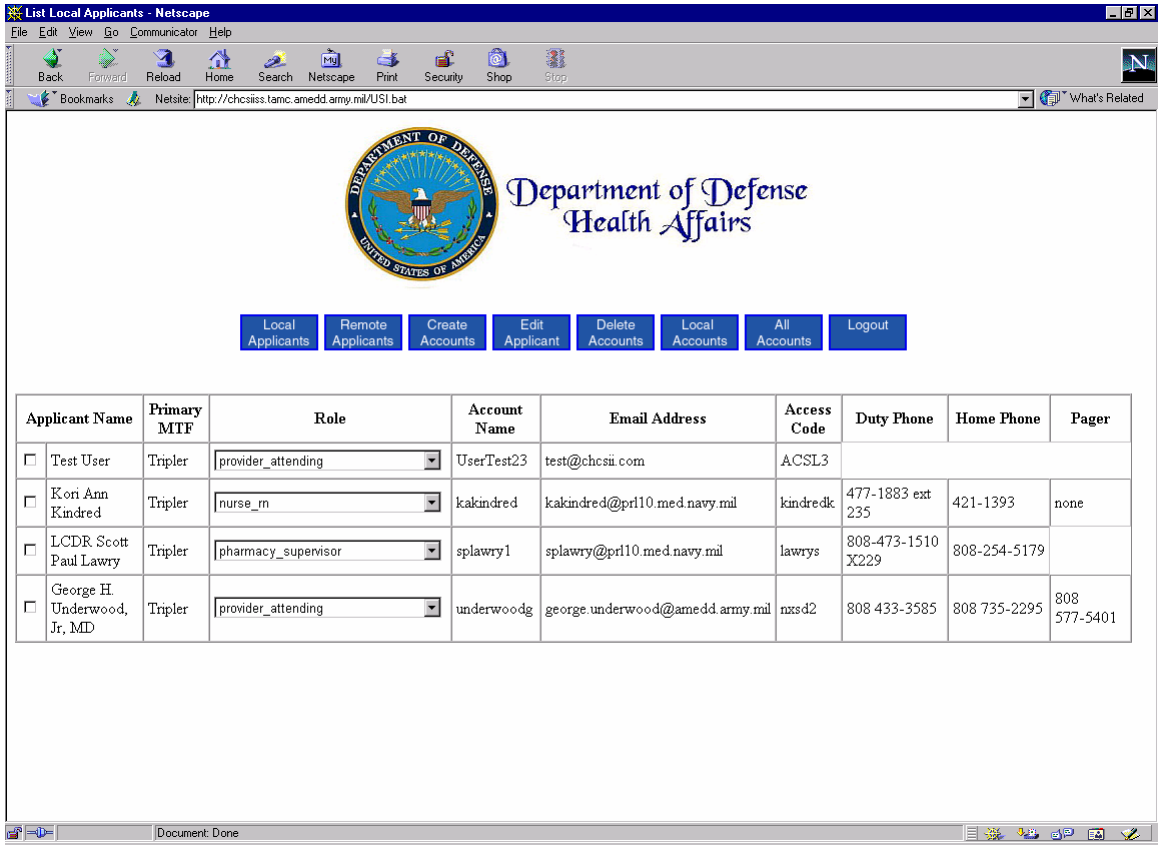


Figure "Account Administrator": This screen from the CHCS system shows how the roles of individuals can be selected readily.

available for viewing whenever and wherever needed to support medical readiness and quality healthcare. The CHCS provides a seamless, merged, enterprise-wide repository of health data that will facilitate the worldwide delivery of healthcare, assist clinicians in making healthcare decisions, and support leaders in making operational and resource allocation decisions (CITPO, 2005). The CHCS is a compendium of commercial and government-developed software using an open system architecture.

The CPR will capture, maintain, and provide patient-focused information for health service delivery at any time and at any location over the beneficiary's period of eligibility. CHCS connects *Medical Treatment Facilities* (MTFs) within a given geographic region. It consolidates individual MTFs into regions using the capabilities of a Health Data Dictionary, Master Patient Index, and Clinical Data Repository. The Health Data Dictionary enables communication among unlike information sources and the Clinical Data Repository provides a virtual infrastructure for interoperability.

CHCS provides real-time availability to eligible medical and dental patient records, access to critical patient-based medical and dental information, and access to population data for automated queries. CHCS supports *Clinical Practice Guidelines* and enhances the information workflow of MHS health care providers. All data is documented electronically, from the patient check-in to the completion of the health care encounter. An electronically accessible medical and dental record is generated and maintained by CHCS, allowing for quality measurement and utilization management within a facility and regionally. The system generates custom reports allowing for patient and provider-specific inquiries, as well as population health studies. As a by-product of the encounter, coding is accomplished.

The CHCS operational *architecture* consists of a common presentation layer (at the user workstation)**,** a database layer, and an applications layer comprised of a variety of health care software packages. System elements are interconnected via interface devices, local area networks (LANs), and wide area networks (WANs) that support heterogeneous distributed hardware platforms and operating systems.

The Tri-Service Infrastructure Management Program Office is responsible for providing a common *communications infrastructure* to support CHCS. This communications infrastructure includes, but is not limited to, a LAN of sufficient size to accommodate all CHCS users, including medical and dental clinics outside the main MTF, and a WAN sized to facilitate data exchange from internal and external sources.

The *CHCS database* resides on a regional server suite located at the Defense Information System Agency computer support facilities. The CHCS Project Office requires six regional server sites to support CHCS worldwide. Each regional server site supports numerous, geographically dispersed CHCS host sites. The CHCS host sites are assigned to regional server sites based on availability and quality of communications links, and other technical and programmatic factors.

CHCS allows users to customize how they interact with the system. The *user interface* includes prompts and context-sensitive, on-line help. Functional Capabilities support Results Retrieval, Consult Tracking, Order Entry, Problem List, Patient Encounter, Summary of Care, Alerts, and Procedural Coding.

The CHCS *enterprise security solution* is designed to provide each site flexibility in configuration while also enforcing standard role-based access across MTFs. The security product is installed at each MTF with a standard set of roles, which have been constructed by the CHCS Functional User Workgroup. Each role has been granted access to CHCS functions based on the work that the role performs. These functions can be altered at each MTF to suit the nuances between sites.

The set of *roles* is large, allowing a very granular set of functions to be assigned. This is intended to limit the amount of user-level granting that must be done. Granting specific functions on a user basis is labor intensive. The CHCS security solution utilizes a web-based interface to allow CHCS Account Administrators to perform the basic functions needed for granting access to the CHCS system (see Figure "Account Administrator").

4.4 Clinical Support

Various departments support patient care in specialist ways. These departments have such *specialized needs* that they typically have special information systems. The clinical departments in this support category include operating rooms, pathology, pharmacy, and radiology.

4.4.1 Overview

Historically, the information systems for specialist departments were provided by vendors distinct from those who provide the core functions, such as admissions and patient records. Thus problems of *integration* have been notorious. However, more

recently, individual vendors provide both the core modules and the support modules, and the integration issues are addressed through standardization of messages.

Pathology, pharmacy, and radiology are particularly likely to be extensively *computerized*. They often obtain or generate data in digital form. For instance, the test machines employed by pathology and radiology often have computers in them and generate digital output. These departments also do not tend to directly treat patients, and thus have greater flexibility in determining how specimens, information, or patients will reach the department. For instance, tubes with blood are collected from patients and conveyed to the pathology laboratory where they are assembled into long queues and fed into the blood analyzer. The pathology and radiology departments may be responsible for providing interpretations of test values, and this task is readily supported by computerization.

Operating room systems and intensive care systems emphasize the *scheduling* of various health care professionals in interaction with the patient. The schedule may go room-by-room and identify the various professionals that are needed in each room at each moment. For example, in surgery the anesthesiologist's schedule along with the surgeon's schedule needs to be precisely known for a given patient's procedure in a given operating room.

Every unit of the health care system that provides clinical support can benefit from computerization. Consider for instance the *food service*. The following functions can be performed with information systems: food inventory control, institutional menu standardization and planning, nutrient analysis, patient selective menu operation, and menu item forecasting.

4.4.2 Pathology

The *pathology laboratory* includes hematology, chemistry, anatomic pathology, microbiology, and blood bank. Particularly for hematology and chemistry the machines in the laboratory may be directly connected to the patient care management system so that results are automatically sent from the laboratory to the patient record without human intervention. The order for these tests may typically require the scheduling of work by a technician to collect the necessary specimen, such as a blood sample, the affixing of an appropriately generated label to the container of the specimen, and the feeding of this specimen into the machine that analyzes the specimen.

By storing values of many tests across time for a given patient, the laboratory system can provide for the physician interactively various summaries of the data across time. Rules in the system can flag abnormalities and give *guidance* to the physician as to what the values might mean diagnostically.

4.4.3 Pharmacy

Medication orders are entered into the pharmacy *system*. The pharmacist may then use various computer-generated documents to guide the delivery of the medications to the patients. Some contemporary hospital systems have special pharmacy machines on the wards that operate somewhat like robots and supply various drugs to the caregiver from the robot based on the drug orders the robot received from the caregiver.

Some pharmacy tasks can be readily automated, such as analysis of appropriateness of drug dosage with respect to patient age and usual dosage level. More generally, the pharmacy system may develop a drug profile of a patient and a prescription history of the doctors and from these two sources support various decisions.

4.4.4 Radiology

Radiology systems typically deal with images that are very large in terms of bits stored. Special image processing and transmission systems have been devised to support *radiology departments* and the circulation of radiological images in the health care network. The radiology system will support the scheduling of patients for radiological exams and the managing of the patient through the radiology department. Since the radiologist's report is typically a natural language report, radiology systems might capture the radiologist's report orally and immediately convert it into textual form.

Traditionally radiology images were stored on film that was cumbersome. Of course, only one copy of the image typically existed. Thus when one caregiver had the image, no other caregiver could have it at the same time. Finding and transporting images was a major task. *Digital radiology systems* permit the images to be stored, transmitted, viewed, and annotated digitally.

All radiological images can be captured digitally. X-rays can be captured by *non-film detectors*. All other modalities already involve electronic data capture, including ultrasound, nuclear medicine, computerized tomography scanning, and magnetic resonance imagining. Systems dedicated to digital radiological image management are called *Picture Archiving and*

Communications Systems (PACS). However, PACS are expensive and require:

- high-resolution acquisition,
- high-capacity storage,
- high-bandwidth network, and
- high-resolution displays.

Many radiology centers still store images on film. Conventional x-rays are taken on celluloid film. Digital studies (computerized tomograms, magnetic resonance images, ultrasounds, and nuclear medicine images) are usually optimized for viewing and stored on film.

Physicians in clinics could make diagnostic and therapeutic decisions more quickly, if the radiologist's interpretation of the image was quickly available *online*. However, most radiology departments do not interpret images in real time but rather on an elective basis in which a radiologist schedules some fixed time to view images collected at an earlier time. Thus the benefit of digital speed of image transmission is reduced.

Image processing experts working with radiologists have not been able to develop robust systems that automatically interpret all radiological images. Intelligent systems to assist the radiologist in interpreting images do exist, and these require the image to be in digital form.

4.5 Physician Group

The description in this chapter of the information systems of providers has focused on the activities of hospitals. The small group physician practice is, however, also very important and very different from the hospital in its information systems support.

The major professions, medicine, law, and the church, emerged in the 19th century from the trades and crafts. In those early days, patronage and a liberal education were all that were required. By 1860 the elements of professional standing were tolerably clear (Reader, 1966):

> You needed a professional association to focus opinion, work up a body of knowledge, and insist upon a decent standard of conduct. If possible, and as soon as possible, it should have a Royal Charter as a mark of recognition. The final step, if you could manage it -- it was very difficult -- was to persuade Parliament to pass an Act conferring something like monopoly powers on duly qualified practitioners, which meant practitioners who had followed a recognized course of training and passed recognized examinations.

The professional has assumed authority in the specific sphere of his expertise.

Traditionally physicians were solo practitioners charging a fee for service. The solo practitioner was the norm till the 1960s. Physicians now typically, formally band together in partnerships or groups.

The bureaucratic nature of group practice may be expected to impose certain rules and regulations. For example in group practice there may be more

- detailed protocols to be followed in a given situation than in solo practice, and
- systematic methods of storing, annotating, and reviewing patient records.

Another organizational attribute of physician practices worth noting is that of general practice or specialist (see Figure "Referral System"). The general practice is dependent on patients. The

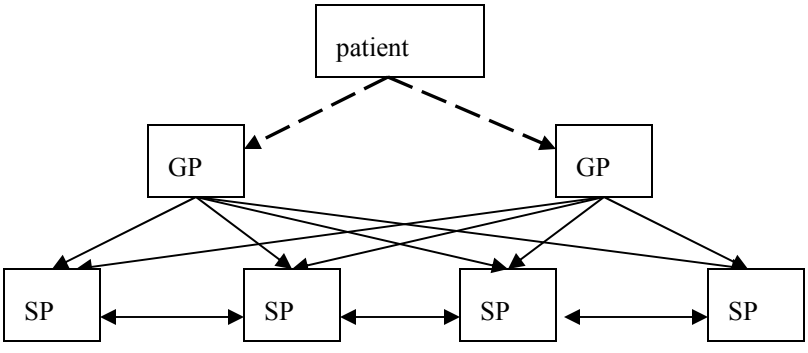


Figure "Referral System": GP is general practitioner. SP is specialists. Dashed line is private patient flow. Solid line is referred patient flow.

specialist is dependent on referrals from general practitioners (or other specialists). The specialist becomes subject to some peer review by the general practitioner who will get the results of the specialist's work. However, the specialist will also be in an indirect position to do some quality review of the work of the general practitioner.

The typical, physician, group practice is supported by three medical assistants per physician. Medical assistant refers to a broad category to include receptionist, transcriptionist, appointment schedulers, billing clerks, and examination assistants. The workflow for a medical assistant might look as follows:

- when doctor arrives ask about hospital visits and emergency room calls in order to post charges for those services,
- when patient arrives, set-up chart for assistant, and write name on day sheet,
- new patients fill-out registration form,
- after patient seen, post charges, ask for payment, make next appointment,
- post check to patient account
- attach lab reports to front of patient's record and place on doctor's desk,
- file lab and other reports in chart,
- make phone calls for forms and payments,
- copy charts for forwarding to new doctors and insurance companies,
- distribute materials brought from doctor's hospital box, and
- check office supplies.

Most of the work of the group practice is done on paper. In particular, the medical record is typically in paper form. Most offices keep records in manila folders. Each patient will have a folder. Sometimes doctors dictate their patient notes, and their secretary transcribes the material into typewritten form for the record. The medical record in the group or solo practice is expected to have these features (Reschke, 1980):

- patient name on all pages
- all pages secured with fasteners
- forms organized with tabs for easy access
- organized chronologically
- missed appointments documented
- telephone message documented
- dictation proofread and initialed
- allergies documented
- diagnostic reports initialed prior to filing
- reason for visit documented
- clinical findings documented
- treatment plan documented
- patient instructions documented
- patient education documented
- prescriptions list
- allergies list
- informed consent on chart
- referral letters on chart
- consultation reports on chart
- problem list kept current

The part of the group practice that is most often automated is billing. This quote from a 1980's textbook remains largely applicable (Lindsey, 1980):

> Since the advent of medical and hospitalization insurance, the medical assistant has found a great deal of his or her

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.

> time now spent billing various insurance companies so that the doctor's fees can be collected.

However, in the past 20 years what has changed is the introduction of software to support the billing. An example of one such product to support billing follows, called Business1 (www.per-se.com). *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 Business1 Accounting Viewer provides a summary of receivables for the patient and guarantor. The *Accounting 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.

4.6 Future

The progress with digital information in health care has been slower than some wanted or predicted. However, progress is continuing. Pushes from employers for computerized physician order entry systems will increase the use of computers in health care. New hospitals are being built with extensive electronic infrastructure, as the following two examples illustrate.

HealthSouth (www.healthsouth.com) spent $100 million to build the HealthSouth Medical Center. The project was a partnership among HealthSouth, 15 medical equipment manufacturers, healthcare specialty firms, and Oracle Corporation. HealthSouth's goal was to improve patient care by bringing together technological advances in healthcare that, due to incompatible computer systems, lack of integration among equipment manufacturers and other obstacles, have had limited impact to date in the hospital industry .

The Indiana Heart Hospital eliminates paper and film-based medical records. The hospital functions with fully electronic patient records that clinicians can view from inside or outside the hospital. The design eliminates medical record storage rooms, paper charting areas and central nursing stations. It focuses on providing information that helps doctors and nurses deliver higher-quality care at the patient bedside. David Veillette, CEO of The Indiana Heart Hospital said (HCPro, 2002):

> We have to make certain that we allow our caregivers to be at the bedside with the patient. Being paperless and filmless will help us accomplish that.

The all-digital workflow features an electronic patient medical record technology that integrates patient information – including images, waveforms and medical history – from every care area of the hospital into a single electronic record that can span a patient's entire lifetime.

4.7 Questions

Reading Questions

1. What are the interactions among the four top-level components (administrative systems, clinical support systems, medical applications, and patient management) of a health information system?
2. What is the relationship between patient accounting and financial management?
3. What are the responsibilities of the medical records department?
4. What are functions of a pharmacy information system?

Doing Questions in Brief

1. Visit a hospital or clinic and observe the admission or registration process. Document the extent to which information systems are utilized.
2. Describe how a master patient index might be developed and maintained and what problems might be encountered during routine use in terms of entering the same person with two different identities in the system.

Doing Question in Detail

A Clinical Documentation System is the portion of a Computerized Patient Record that allows patient data entry at the point of service. Compare and contrast the Clinical Documentation system available from 3 vendors. Note the prominent connections of each vendor product to other components of the health

information system as described in the chapter. Predict what you would see and hear in terms of the health care professionals (all levels) in their use of the Clinical Documentation system in a hospital.

5 Payers


Learning Objectives

- Diagram the basic operations of a health plan.
- Identify salient characteristics of information systems applications in health plans based on case studies.

Most of what has been discussed in this book focuses on the provider and its relation to the patient as regards information systems. However, the connection between the provider and payer is critical to the smooth functioning of the system (Starr, 1997). This chapter focuses on the *payer* (or health plan).

5.1 Definitions

The American healthcare system shows complex relationships among

- patients,
- employers who typically subsidize their employees' health insurance,
- health insurance companies that collect premiums from enrollees (patients) and pay providers for care delivered to patients, and
- providers who care for patients but are paid by insurance companies.

An example of the variety of players in the health system is provided by the *Wisconsin Health Information Network* that links 16 hospitals, 8 clinics, 3 nursing homes, 1,300 physicians, 7 health plans, and 4 clearinghouses. Definitions of health plan and clearinghouse are provided next.

5.1.1 Health Plans

A *health plan* is an individual or group health plan that provides, or pays the cost of, medical care. On the other hand, plans, such as property and casualty insurance plans and workers compensation plans, which may pay healthcare costs in the course of administering non-healthcare benefits, are not considered health plans.

Health plans often perform their business functions through *agents*, such as plan administrators (including third party administrators), entities that are under 'administrative services only' contracts, claims processors, and fiscal agents. These agents may or may not be health plans in their own right; for example, a health plan may act as another health plan's agent as another line of business. The three most prominent kinds of health plans in the United States are indemnity, health maintenance, and government plans (DHHS, 2001).

Traditional *indemnity plans* offer the widest range of choice to consumers. Blue Cross & Blue Shield organizations offer well known indemnity plans. The consumer obtains medical services from the physician or hospital of his choice. He submits his bill to the insurance company and the insurance company makes whatever payments it has pre-agreed it would make for such services. The *consumer* typically pays a percentage of the bill till some threshold is reached.

For the indemnity (indemnity means security against damage, loss, or injury) plans, the patient typically pays 20% and insurance pays 80%. However, this is 80% of what insurance deems is 'usual and customary reimbursement' (UCR). Often this UCR is less than the physician charges so the patient pays more than 20% of the charge. Say the physician charges $1,000 for repair of inguinal hernia, but the insurance company says the UCR is $800. Insurance then pays 80% of $800. The patient is then responsible to pay $360 and not $200.

Health Maintenance Organizations (HMOs) are designed to provide medical care at a pre-arranged monthly fee. Instead of paying a 'premium' to an insurance company, the consumer pays a *membership fee* to an HMO. In return, the consumer receives all medical care from the HMO. Instead of treating patients and then trying to collect money from either the patient or the insurance company for the cost of the treatment, HMOs bypass the insurance company completely and make their 'deal' with the consumer.

Managed care is often reimbursed on a capitation scheme. The physician agrees to provide a specified list of services to each patient assigned to him or her for a set dollar amount each month. The insurer pays the specified amount regardless of what this patient does. Typically, this fee is between $3 per patient per month to $15 per patient per month. Obviously these risk-sharing agreements can lead to very different results for the physician depending on circumstances. If the physician has 100 patients in the plan and the capitated fee is $15 per member per month, then if the physician sees 20 of these patients at a cost to the physician of $1,800, then the physician has lost $300. If the physician sees only 5 of the 100 patients and their total services are $200, then the physician has a gross profit of $1,300.

The government is involved in one form or another in various health plans to include:

- The Medicare and Medicaid programs.
- The healthcare program for active military personnel.
- The veterans healthcare program.
- The Civilian Health and Medical Program of the Uniformed Services.

Smaller government programs exist, such as the Indian Health Service program.

The health insurance market may also be viewed as consisting of three distinct segments: *large group*, *small group*, and *individual*. These are not simply points on a continuum; they constitute entirely different product lines, often sold by different sales forces and serviced by different insurers or corporate divisions (Hall, 2000).

The large group market accounts for two-thirds of private health insurance. The large group market consists of employer-based insurance for groups of more than fifty workers. Regulation of these groups is determined by whether they are self-insured (the employer bears the financial risk for most claims) or not. More than half of groups of more than 500 workers are self-insured. For these groups, the *Employee Retirement Income Security Act (ERISA)* preempts the core of state-law insurance regulation. *Preemption* includes regulation of solvency and other financial matters, consumer protection regulation, and regulation of the content of health insurance. For large groups that are not self-insured, these matters are subject to state regulation.

Because the employer selects and pays for employees' insurance, there is little tendency for insurance to be selected with the health condition of particular subscribers in mind (adverse selection). This allows the market to function well with little or no medical underwriting (that is, screening and evaluation of individual health risks), since underwriting is focused on group averages. Another advantage to *employer-based insurance* is the subsidy it confers to subscribers, because the employer pays a large portion of the premium and because this premium contribution is not taxed as income to the employee. Finally, larger groups typically offer employees a choice of plans.

At the other extreme, the *individual market* consists of insurance purchased outside the workplace, such as by self-employed or unemployed people, or people with jobs that do not provide health insurance. The individual market segment accounts for less than 10 percent of private health insurance. Its regulation is almost entirely the province of the states. States typically regulate solvency and other financial matters, the content and wording of policies, and managed care activities.

Because the purchase of individual insurance is determined entirely by purchasers' *health needs*, adverse-selection concerns are great. Thus, medical underwriting is very prominent, in the form of premium variations, coverage limitations or exclusions, and outright denials of coverage. On the positive side, purchasers in the *individual market* can choose from the full array of product types and variations in coverage.

5.1.2 Clearinghouses

The network of connections among American health care entities for the purposes of *money transfer* reflects a complex diversification of specializations. Between the provider and payer lies another network of entities that might be generically called clearinghouses. A *healthcare 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 healthcare transactions from healthcare 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 healthcare clearinghouses, as necessary, for further action.

The clearinghouse provides more than simple connectivity (see Figure “Clearinghouse”). Additional *functions* include:

- reformatting transactions into standard data formats,
- error checking,
- editing, aggregating, distributing and routing transactions, and

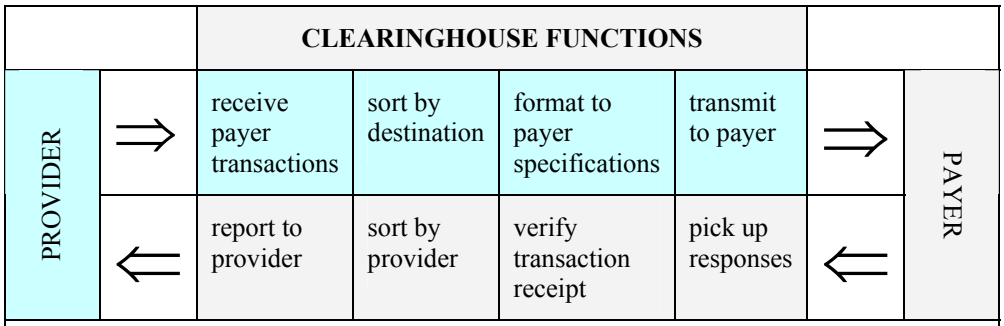


Figure "Clearinghouse": The functions of the clearinghouse are indicated on the internal cells. The arrows indicate the flow of information to and from the clearinghouse.

- producing management and analysis reports.

To perform these functions, the clearinghouses 'open the transaction envelope' for routing and switching purposes yet ensure security and integrity of the data through administrative procedures, technical tools, and contractual agreements.

A prominent form of intermediary organization (or clearinghouse) is called a *third-party billing agent*. Third-party billing agents help providers generate claims. These third-party billing agents or the providers directly contact with health plans or other 'clearinghouses'. Hospital information system vendors, telecommunication companies, consortia of provider organizations, and others may support other intermediary activities.

5.2 Basic Operations

What are the basic operations of a typical health plan? First it *enrolls* members. Either members or their sponsor pay premiums to the health plan. What is the main service provided by a health plan? It pays providers for health care delivered to enrollees. The plan agrees with certain providers to *reimburse* them for certain expenses that they incur in treating enrollees of the plan. The plan might also directly reimburse the member for expenses the member paid directly to the provider, though this is increasingly uncommon.

A typical provider function relative to a payer begins with the first encounter between the provider and patient. The provider wants to confirm that the patient is eligible for health care services from the provider and checks this *eligibility* with the health plan. If eligibility holds and care is delivered, then the next major communication between the provider and the payer is the submission of a claim for reimbursement from the provider to the plan.

In 1958, the Health Insurance Association of America and the American Medical Association (AMA) attempted to standardize the insurance claim form. However, payers did not universally accept this form, and as the types of coverage became more variable, new claims forms, requiring more information, were developed. In 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. Prior to HIPAA, all services for Medicare patients from physicians and suppliers (except for ambulance services) had to be billed on the HCFA-1500 form.

The HCFA-1500 form is divided into two sections (see Figure "HCFA-1500" at end of chapter):

- 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.

Having received a claim, the health plan needs to *adjudicate* the claim. This requires determining whether the services were appropriately rendered and whether the costs are justified. If the health plan feels that inadequate information has been provided to judge the fairness of the claim, the plan will ask the provider to send additional information to the plan. Sometimes the plan will ask the provider to send a copy of the entire medical record of the patient to the plan. Eventually, the health plan must issue a response that includes its payment and an explanation of the relationship between its payment and the claim.

These operations can be elaborated in many ways. The health plan employs many roles for helping assure its smooth operation. In addition to the obvious roles of soliciting enrollees and paying

claims, the plan has a layer of operations that includes underwriters and profilers. *Underwriters* are involved in the determination of what health care costs a potential enrollee is likely to incur and what premiums would be required to cover the risks of insuring this enrollee. Profilers analyze providers and recommend providers that are likely to reduce the costs to the plan.

The health plans also work with outside entities other than providers, employers, and enrollees. Clearinghouses are one prominent example, but equally important to the viability of a plan are brokers. Brokers and agents give advice to people about available health plans and get paid a commission by a health plan for each enrollee that the broker or agent brings into the plan.

For a payer to perform its functions efficiently, Information Systems are vital. Time and personnel resources to perform these functions manually are too high. Consider the following examples of how manual processes might work for enrollment, claims adjudication, and claims payment.

For enrollment, the payer would receive an application for enrollment of a beneficiary and would:

- Visually inspect the form for missing fields or invalid information,
- Look-up the rules for enrolling that beneficiary in a printed reference to determine eligibility. The printed references might vary by employer, or in the case of individual plans, by characteristic of the beneficiary. For example, the printed reference might state that employees of a particular company must be employed for at least 90 days before being eligible for insurance. The payer would then need to check the enrollment application to see that this condition had been met. This process of manual verification of enrollment eligibility would be time consuming and error-prone.
- If the application is valid, then the payer adds the beneficiary to the list of individuals currently enrolled in the plan.

For claims adjudication, suppose a pharmacy is filling a prescription for a patient and wants to determine the patient's co-payment, the pharmacy would phone the payer, who then might need to do the following:

1. Verify whether the patient was enrolled in the prescription drug program by looking up the patient's name in a printed enrollment log.
2. Check the printed benefits history for that patient to ensure the patient had not exceeded the maximum annual prescription benefit already.
3. Find the pharmacy in a printed provider log.
4. Find the medication name in the printed formulary, since there is a higher co-payment for medications not on the formulary.
5. Report the co-payment back to the pharmacy.

Now suppose the pharmacy filled the prescription and submitted a paper claim to the insurance company. The payer might then need to do the following:

- Go through steps 1 through 4 above again.
- Check to see if the pharmacy's charges were usual and customary (UCR) and determine the payment amount based on this and the co-payment. If the payer determined the charges exceeded the UCR, they would need to reflect how much of the charge exceeded the UCR on the claim payment statement.
- Issue a check and a statement to the pharmacy.

The above manual processes are time-consuming and inefficient. Currently, for many payers and pharmacies, filling the prescription is tied to electronically submitting the claim--the two occur at the same time. Claims adjudication and payment may occur in a matter of seconds.

5.3 CMS

The Centers for Medicare & Medicaid Services (CMS) is a federal agency within the U.S. Department of Health and Human Services. CMS was known prior to 2001 as the Health Care Financing Administration and is a component of the Department of Health and Human Services of the U.S. Government. CMS runs the Medicare and Medicaid programs - two national health care programs that benefit about 75 million Americans. CMS also runs the State Children's Health Insurance Program (SCHIP), a program that is expected to cover many of the approximately 10 million uninsured children in the United States. CMS also regulates all laboratory testing (except research) performed on humans in the United States. CMS spent over $360 billion in 2000 buying health care services for beneficiaries of Medicare, Medicaid and SCHIP (www.cms.hhs.gov).

The Information Technology Objectives of CMS include:

- Meaningful information is readily accessible to CMS's beneficiaries, partners, and stakeholders, and

- IT is effectively applied to support program integrity.

The functional view of CMS divides the organization into eleven Functional Areas as follows:

1. CMS Management
2. Program Development
3. Program Operations Management
4. Medicare Financial Management
5. Program Integrity Organization
6. Medicaid and Child Health Insurance Program Administration
7. External Communication
8. Administrative Services
9. Outreach and Education
10. Health Industry Standards
11. Program Quality Organization

The Information Systems that support this host of functions and organizational areas at CMS are:

- Beneficiary Data Management System
- Provider Data Management System
- Insurer Data Management System
- Health Care Plan Data Management System
- Utilization Data Management System
- Survey Data Management System
- General Ledger Data Management System
- Business Management Information System
- Health Care Finance Information System
- Health Care Stakeholder Information System
- Health Care Assessment Information System
- Health Care Services Information System
- Geographic Locations Information System
- Document Information System
- Human Resources

The Information Systems are, in turn, decomposed into numerous subsystems of which a listing of those whose acronyms begin with the letter 'A' or 'B' indicates the complexity:

- AAPCC Adjusted Average Per Capita Cost System
- APPSGHP Automated Plan Payment System
- ARKA Arkansas Part A System
- ASPEN Automated Survey Processing Environment
- ATARS Audits Tracking and Reporting System
- BAAADS Budget's Apportions Allotments Allowances Database System
- BESS Part B Medicare Extract and Summary System
- BEST Carrier Beneficiary Alpha/State System
- BUCS Budget Under Control System

Each of these systems is complex enough to contain multiple other subsystems.

5.4 BCBS

The *Blue Cross and Blue Shield System*:

- consists of approximately 45 member plans that are independent, locally operated companies under the coordination of the Blue Cross and Blue Shield Association,
- provides health care coverage for approximately 80 million people in the US,
- contracts with 80 percent of hospitals and 90 percent of physicians in the US, amd
- employs 150,000 people.

Administrative costs average 12 percent of health care payments and gross revenue was approximately $1 trillion for the year 2000.

5.4.1 Operations

A large Blue Cross & Blue Shield Plan is a complex of entities typically and not purely a health insurance company. In one example, the 'plan' includes a health maintenance organization, a disease management group, and a plan services group in addition to the traditional BC&BS Group (Paramore, 2001). Information is exchanged among these components. For instance, the Plan Services Group sends health information covering

- Eligibility Information,
- Membership Lists, and
- Claims Information

to the Disease Management Group.

In its connection to providers and members, the BCBS plans shows another complex of relations (see Figure "Plan, Members, and Providers"). In the provider direction, the Plan is connected to clearinghouses, pharmacies, and other providers. Other providers include hospitals, individual physicians, clinics, long-term care facilities, and skilled nursing facilities. In the members' direction, the BCBS Plan is linked to groups, enrollees, and brokers. From the BCBS Plan to the hospitals and physicians the following information goes:

- Eligibility Rosters,
- Capitation Reports,
- Membership Lists,
- Pre-authorizations and Certification Communications,
- Claims Information,
- Daily Error Reports,
- Paid Claims Information,

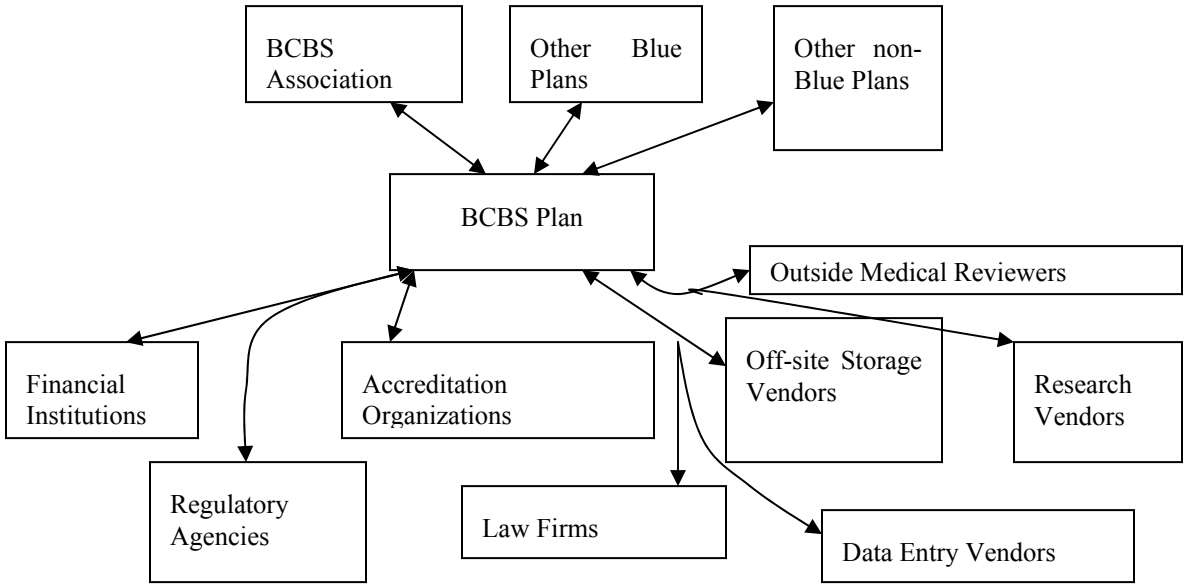


Figure "BCBS and Others": The Plan connects to other plans in the upper half of the diagram. In the lower half, the Plan connects to a variety of organizations that regulate, support, and review activity.

- Case Management Negotiations, and
- Utilization Data.

To the pharmacy, a subset of this information is exchanged to include:

- Eligibility Approval,
- Drug Claim Information, and
- Paid Claim Information.

From the BCBS plan to the Member or Applicant goes

- Eligibility Information or Changes,
- Quote Information,
- Enrollee Reject Notice,
- Member Communication Letters,
- Pre-Authorization and Certification Communications,
- Paid Claim Information,
- Dependent Benefits Information,
- Record Request Communications,
- Disease Management Information,
- Case Management Information, and
- Release Coordination.

From the BCBS to the Groups goes some of the preceding plus 'High Dollar or Stop Loss' information.

The BCBS Plans have natural connections to other plans and to vendors, regulatory agencies, and financial institutions (see Figure "BCBS and Others"). To the BCBS Association the Plan sends

- appeals and complaints,
- transplant network information, and
- fraud and abuse case information.

To other Blue Plans, the Blue Plan sends

- secondary cross-over information,
- eligibilities, and
- claims information for fraud investigation.

To non-Blue Plans, the Blue Plan may send:

- subrojation information,
- coordination of benefits information, and
- claims information for fraud investigation.

In the other direction, the Blue Plan will send to financial institutions 'verification of benefits' data. To regulatory and accreditation organizations the Plan will send auditable and accreditation information and medical information to support medical audits. To off-site storage vendors, the Plan sends paper applications and underwriting and claims information.

This complex set of relationships of the BCBS Plan is not unique to BCBS Plans but is typical of the health plan situation in the US. The health plan is not only collecting enrollee premiums and paying providers but is engaged in a complex set of financial, quality

control, and medical activities with numerous other entities.

5.4.2 One Case

One of the regional Blue Cross and Blue Shield Plans is *Blue Cross and Blue Shield of North Carolina* (BCBSNC). BCBSNC has about 1.8 million members and performs 14 million transactions annually. To improve its connectivity with its various stakeholders, BCBSNC extended its legacy systems to make them more accessible to external stakeholders. BCBSNC implemented an Internet-based solution that offers its employer groups and healthcare providers easy access and control over routine but important business functions (AMS, 2001).

BCBSNC converted the current legacy application, running over an SNA network, to a *Web-based application* communicating over a TCP/IP Intranet. This Internet-based solution streamlines millions of *transactions* between BCBSNC and its healthcare providers and employer groups. The new system gives more than 9,000 hospitals, doctors, other healthcare providers, and employers access to membership, eligibility, benefits, and claim status information. The new system also lets providers and employer groups submit health care claims, request pre-authorizations, and submit enrollments.

5.5 CMS versus BCBS

The most salient difference between CMS and BCBS is that BCBS has more control over who is enrolled and who can provide services. This control allows them to be more accountable to their stakeholders in terms of ensuring an acceptable quality of care at a reasonable cost.

BCBS has a high degree of control over who can enroll in individual plans. Based on the applicant's age, sex, and health status, BCBS can gauge the amount of services the individual is likely to require. If it determines that the individual is likely to be a high cost, frequent user, it can

- refuse to cover the applicant;
- cover the applicant, except for his/her pre-existing conditions; or
- cover the applicant but charge a very high premium.

BCBS will typically have less direct control initially over who is enrolled in its small and large group plans. It may or may not enforce pre-existing condition limitations on beneficiaries of these plans. Still, it can mitigate excessive costs and exert indirect control by raising premiums. If a particular group uses a large amount of resources, BCBS could raise premiums the next year to an amount that the employer might no longer be able to afford. Increasing premiums would benefit BCBS by either mitigating the financial risk of providing coverage for a high cost group (if that group decided to pay the premiums) or forcing an undesirable, high cost/liability group to drop the coverage.

On the provider side, BCBS exerts control by deciding which providers can participate in the plan. It carefully monitors claims in order to track provider's utilization and habits. A provider who orders many expensive treatments or medications, or who often refers patients to specialists could be dropped from the plan. BCBS may also exert control over existing providers by giving them feedback on their performance. It may send them 'report cards' of their performance as compared with their peers, particularly with regard to utilization (e.g., number of tests ordered, referrals to specialists, and number of times they have ordered non-formulary medications).

Without sophisticated information systems (IS), BCBS would be unable to exert this kind of control over enrollment and providers. IS are essential for BCBS to be able to determine patient and provider utilization rates, and to determine how much it costs to insure a particular demographic group, patients with various medical conditions, and specific employer groups. Without detailed cost and utilization data, BCBS might take on excessive risk by not charging sufficient premiums to cover the costs of high-utilization individuals and employer groups. Or, it might undertake excessive risk by allowing a high-utilization/high-cost provider to continue to participate in the plan. Finally, using IS to track utilization data would enable BCBS to provide performance information to its stakeholders.

About 90% of BCBS's business is derived from insured groups. Insurance brokers advise the insured groups to enroll in BCBS. The obvious implication is that BCBS should make its IS as helpful to brokers and groups as possible. One way to do this would be a web site that enables groups and brokers easily and quickly to find premium quotes and benefit and plan information and to enroll new employees or groups. Since CMS does not address groups or brokers, CMS has little need for these functions.

CMS has little control over who is enrolled in Medicare, Medicaid, or SCHIP. Eligibility is not based on health status but on age, disability criteria, and/or income. CMS has no way to mitigate the cost of insuring patients who frequently use significant amounts of health care resources. Also, CMS is not able to exert control over high-cost, high-utilization

providers unless these providers also happen to commit some gross act of misconduct or fraud. CMS has several approaches to handle skyrocketing costs:

- reduce benefits to existing beneficiaries;
- change eligibility requirements so fewer people will be eligible;
- increase government financial support;
- reduce payment to providers; and
- reduce costs by improving the efficiency of existing programs/services.

The first four options are politically unattractive and most would require an act of Congress to implement. The fifth option is attractive because the majority of CMS's stakeholders (beneficiaries, providers, taxpayers, and government) want that option, and CMS can implement that option with the help of IS. CMS has undertaken initiatives using IS to attempt to improve efficiency and effectiveness.

5.6 Accountability

Some take a jaundiced view of the impact of the American system on the ability of the patient to influence change, as witnessed in this excerpt (Fogoros, 2001):

> Very few patients go out and buy their own health insurance. Most receive their health insurance through their employers, the government, or not at all. Thus, patients don't really have the power to shop around and choose among health plans (except within very strict limits), nor do they have any true power to walk away from the health plans presented to them. Their lack of the ability to choose a plan, and the ability to exit a plan, essentially destroys any claim they may have to the title 'customer'. Indeed, their economic position in the health care system is more akin to that of 'commodity'. (They are, in fact, called by the industry 'covered lives', and are traded back and forth like pork bellies.) Thus, health plans see relatively little reason to afford patients the same respect that businesses traditionally afford their customers.

What are the balances among the stakeholders that lead to accountability?

Organizations are accountable to their stakeholders, and health care organizations typically have more stakeholders than other businesses (Goddard and D'Andrea, 1999). 'Accountability' is 'the process by which one party is required to justify its actions and policies to another party'. In the case of a health plan, the stakeholders include:

- Individual patients;
- Purchasers (private and public);
- Health care providers (physicians and non-physicians);
- Government entities (federal and state);
- Other health plans; and
- Investors (for publicly-held organizations).

In many cases, health plans are involved in reciprocally accountable relationships with their stakeholders. For example, while a health plan has extensive obligations to its health care providers (e.g., prompt payment of clean claims, due process in disciplinary proceedings), the providers have a responsibility to the health plan (e.g., a duty to maintain licensure and privileges, a duty to not discriminate against health plan members).

Accountabilities to particular stakeholders may vary with *circumstances*. For instance, a health plan has obligations to each enrollee to provide accurate information about accessing benefits. Those obligations change when an enrollee becomes a patient. The health plan must then ensure that claims are paid on a timely basis and that medically needed care is available.

Behaviors for which health plans are accountable include:

- Financial reliability and performance;
- The provision of reasonable access to qualified health care providers;
- The provision of information to promote member health;
- Legal and ethical conduct;
- The continuous improvement of the quality of health care provided through the health plan; and
- Competent administration.

Within a particular *behavioral domain*, a health plan often has several sets of standards against which its performance is measured. For example, a multi-state health plan may have its performance in a single behavioral domain – continuous quality improvement, for example – measured against *standards* imposed by

- multiple state insurance regulators,
- multiple state health regulators,
- the U.S. Department of Health and Human Services,
- the American Accreditation HealthCare Commission, and
- large employer benefit administrators.

The web of accountabilities in which each health plan is embedded imposes complex administrative and operational responsibilities on the health plan.

Technology supports the exchange of information between employers and health plans. This includes enrollment information from *employers* and outcomes information from the health plan. Some employers and payers exchange enrollment information online.

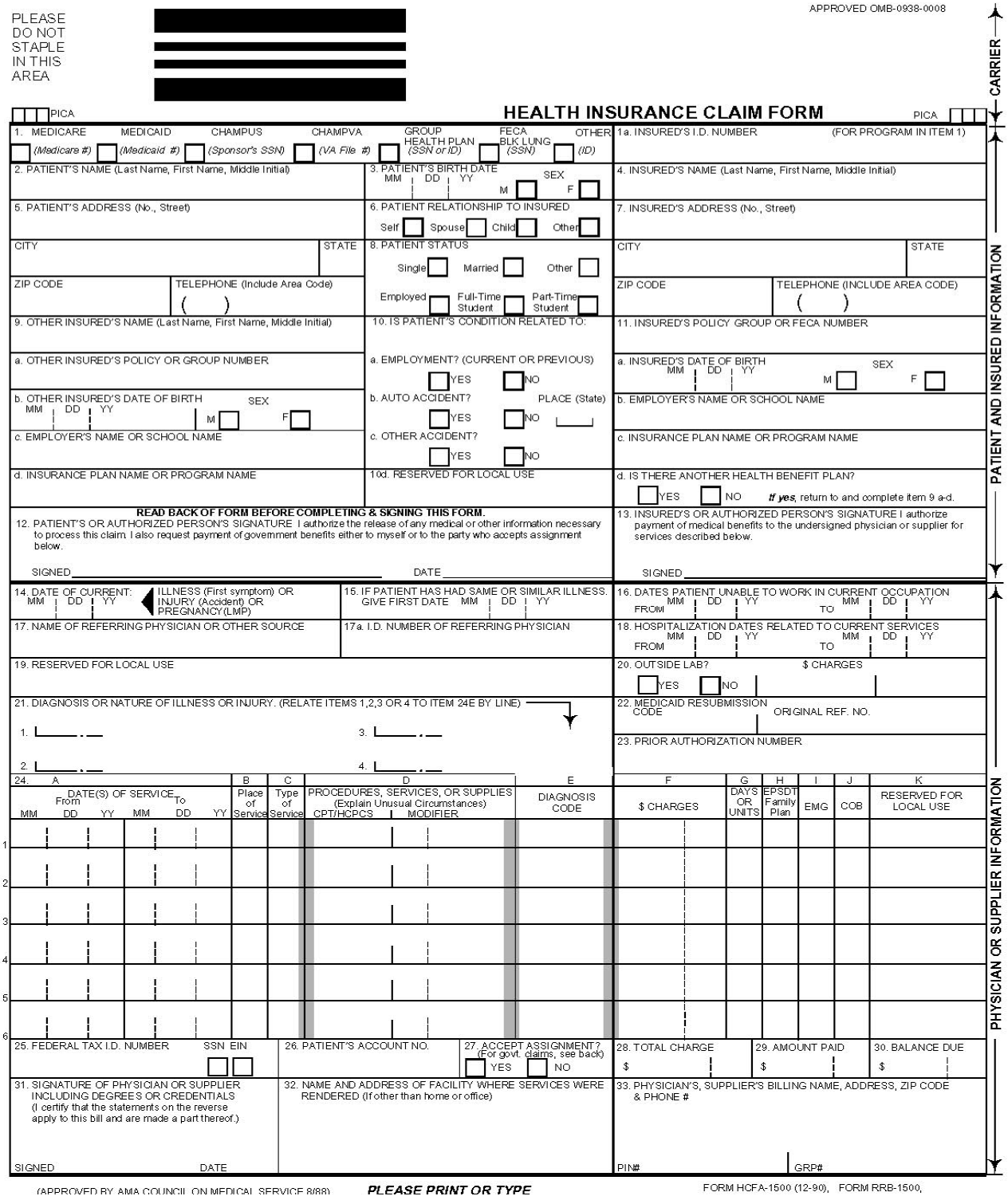
The *Health Plan and Employer Data Information Set* (HEDIS) is a set of performance measures designed to standardize the way health plans report data to employers. HEDIS focuses on four major performance areas:

- quality,
- access and patient satisfaction,
- membership and utilization, and
- finance.

Quality indicators include childhood immunization rates and mammography rates. Patient satisfaction measures reflect the members' satisfaction within their plans. Membership and utilization data includes enrollment and dis-enrollment statistics by age and sex. Finance includes per-member revenues and rate trends. HEDIS is increasingly important for health plans as buyers of health care pay more attention to HEDIS data in deciding what plans to use. Technology is required for accurate and timely extraction of HEDIS data from the various transactions to which payers have access (Kissinger and Borchardt, 1996).

5.7 Questions

1. What is the definition of a health plan?
2. What are the basic operations of a health plan?
3. What characteristics do the Blue Cross and Blue Shield case and the Medicare case have in common?
4. What kinds of companies become clearinghouses?



PLEASE DO NOT STAPLE IN THIS AREA

[redacted]

APPROVED OMB-0938-0008

PICA

HEALTH INSURANCE CLAIM FORM

PICA

CARRIER

PATIENT AND INSURED INFORMATION

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

CITY STATE

ZIP CODE TELEPHONE (Include Area Code) ( )

Employed Full-Time Student Part-Time Student

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

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 MM DD YY FROM 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 MM DD YY FROM 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. 3.

2. 4.

22. MEDICAID RESUBMISSION CODE ORIGINAL REF. NO.

23. PRIOR AUTHORIZATION NUMBER

PHYSICIAN OR SUPPLIER INFORMATION

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

(APPROVED BY AMA COUNCIL ON MEDICAL SERVICE 8/88) ***PLEASE PRINT OR TYPE*** FORM HCFA-1500 (12-90), FORM RRB-1500,

Figure "HCFA 1500": This is the claims form widely used throughout the 1990s.

Part III: Regulations

6 Compliance

Learning Objectives

- Predict the trends in government regulation of business in the U.S.
- Design a corporate compliance program that balances the various forces that work for and against compliance.

The use of innovative applications of technology in the highly regulated world of medicine continues to require resolution of numerous legal issues (Goldberg and Gordon, 1999).

6.1 History

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.

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. The *Industrial Revolution* shook the foundations of American society. Purposive control of business in the name of the public good slowly became the American response to big business. The *Sherman Anti-trust Act* of 1890 made illegal every contract that restrained free trade. The Act symbolizes 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 an equal threat.

Since the late 1960's, regulations have appeared that effect 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 1980 election brought *Ronald Reagan* to the White House and a different approach to regulation. 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 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's 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.

6.2 Role of Business

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, and
- 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 that 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.

6.3 Insurance

In the twentieth century, the federal government passed several major pieces of legislation with implications for health care insurance. A US Supreme Court decision first applied federal scrutiny to insurance markets in 1944. An *antitrust* dispute led the court to rule that insurance transactions were indeed interstate commerce and thus subject to federal antitrust laws. Largely at the behest of insurers who feared federal oversight, the next year (1945) Congress passed the McCarran-Ferguson Act. McCarran-Ferguson exempted health insurance markets from federal antitrust prosecution as long as those markets were regulated by the states.

Workers in the early part of the twentieth century opposed employers' picking their doctors for them. These arguments were refined over time to support prohibitions against *employers* hiring *doctors* to whom employees were expected to go in the case of medical need. The employees preferred the employer to provide indemnity insurance whereby the employee can go to any healthcare provider and have the insurance pay for expenses engendered. The states supported this opposition to employer-selected healthcare by stifling or prohibiting it. Pre-paid group practices to which an employee is expected to go were not allowed by the states.

The *HMO Act of 1973* was the first major federal effort to promote alternatives to indemnity insurance. The act fostered the development of qualifying HMOs by overriding state statutory and *common law*

prohibitions on the operation of prepaid group practices and the corporate practice of medicine. The HMO Act required employers with more than twenty-five employees that offered at least one health insurance plan to also offer an HMO, if requested by a local HMO.

6.4 HIPAA

Congress determined in 1996 that small-group and individual health insurance market performance could and should be enhanced with the explicit articulation of new federal goals and placed these in the Health Insurance Portability and Accountability Act (HIPAA) of 1996. In effect, HIPAA establishes a federal floor for a degree of assurance that health status will render neither individuals nor their dependents *uninsurable* .

HIPAA was put into law by the American Congress in 1996. 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 best known 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.

The Administrative Simplification component of HIPAA:

- 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.

Administrative simplification should improve the information systems infrastructure of healthcare.

6.5 Associations

An *association* is an organization of persons having a common interest. Numerous associations are relevant to regulation and compliance. 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 use of information systems in health care. JCAHO and NCQA tend to incorporate requirements from federal regulations into their standards and practices for evaluating healthcare organizations.

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.

6.6 Corporate Compliance

Each corporation has its culture. A compliance program good for one corporate culture might not be good for a different corporate culture.

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.

A typical *compliance program* may be viewed as involving four steps:

- management commitment,
- education,
- implementation, and
- 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.

Tracking and documenting progress may be a crucial part of 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. Some regulations require such internal vigilance, 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. Groups responsible for internal reviews tend to become clearly established as a compliance constituency.

Any internal review group can find things that should be corrected. Furthermore, the group can be expected to want to bring attention to its successes by highlighting irregularities. 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.

6.7 Questions

Reading Questions

- Describe the history of government regulation of business in the U.S.A.
- Illustrate how different corporations have different cultures as regards compliance with federal regulations.

Doing Questions

- What lesson do you draw from the history preceding the Pure Food and Drug Act (see Introduction Chapter) as regards the role of business in supporting the finalization of federal regulation of business? Imagine a piece of health care information systems legislation that you see having a challenging battle in congress and for which you can anticipate some businesses supporting it and some opposing it. Describe briefly the intent of the legislation and the opposing and supporting forces.
- Make an analogy between the insight that some business needs to support a successful legislation and the observations about the nature of corporate compliance. If you were CEO of a large firm, what would you want to do and why regarding the distribution of authority between the corporate compliance unit and those units responsible for profit generation?

7 Fraud

Learning Objectives

- Differentiate whistleblowers from fraud investigators.
- Construct relationships between software to support coding and software to support fraud detection.
- Demonstrate that shared information among payers can increase the ability of fraud investigators to successfully, semi-automatically detect fraud.

The number one *white-collar* crime in the United States is healthcare fraud. Fraud is an intentional deception or a misrepresentation that the individual or entity makes knowing that the misrepresentation could result in some unauthorized benefit to the individual, or the entity or to some other party. The most common kind of healthcare fraud involves a false statement, misrepresentation or deliberate omission that is critical to the determination of health benefits payment.

The variety of fraudulent reimbursement and billing practices in the healthcare area is potentially infinite. The most common healthcare fraudulent acts include, but are not limited to (NHCAA, 2005):

- Billing for services, procedures, or supplies that were not provided.
- The intentional *misrepresentation* of any of the following for purposes of manipulating the benefits payable:
    - The nature of services, procedures, or supplies provided;
    - The medical record of service or treatment provided;
    - The condition treated or diagnosis made;
    - The charges or reimbursement for services, procedures, or supplies provided.
- The deliberate performance of unwarranted services for the purpose of financial gain.

Fraud by *billing* for services not provided is easier to detect than fraud by misrepresentation of the patient condition. The following is an example of flagrant fraud (Thornton, 1999):

> A physician previously convicted of fraud in another state begins a new life in Pennsylvania. He opens a clinical office using a corporate name not easily tied back to his prior life. He recruits patients who provide him with their insurance coverage information in return for a one-third share of the proceeds of his billings. Most patients appear at his office only to sign forms and pick up their share. Investigators retained by the local Blue Shield discover his history and obtain admissions from two patients about their arrangement. They refer the matter, together with signed witness statements, to the FBI and U.S. Attorney.

The ensuing investigation will take an average of eighteen months before return of an indictment. Bank subpoena returns show that in the meantime the doctor is netting $250,000 per month.

Imagine that a patient goes to the *dentist* for a routine examination. The dentist detects that a small cavity has appeared near a filling in a molar that already has one small filling. The proper treatment is another small filling for which the dentist would get paid about $200 by the insurance. However, if the dentist says that the cavity is large and convinces the patient to accept a crown on the tooth, then the dentist may earn $1,000 for doing the crown. How are the patient or the insurance company to know whether the cavity warranted a crown or not? Determining whether fraud has occurred in this case would require another dentist to see x-rays of the patient's tooth and perhaps re-examine the patient. Another dentist may hesitate to dispute the practice of a peer. The cost of such an investigation might exceed the difference in cost between the small filling and the crown and might breed ill-will for the insurance company among the providers so an *insurance company* or other payer may hesitate to pursue this type of fraud.

7.1 False Claims Act

The False Claims Act dates back to the Civil War. Passed during the Civil War, the False Claims Act was intended to protect the Union army from fraudulent suppliers who sold faulty war material to the government. In support of the False Claims Act, *Abraham Lincoln* wrote:

> Worse than traitors in arms are the men who pretend loyalty to the flag, feast and fatten on the misfortunes of the nation while patriotic blood is crimsoning the plains of the south and their countrymen are moldering in the dust.

During the *Civil War* the government was so busy with the war that it did not have time to investigate fraud in bills sent to the government for the purchase of supplies. The False Claims Act asks citizens to report to the government any evidence of fraud. It allows a private individual with knowledge of fraud (a *whistleblowe*r) on the federal government to sue for the government to recover compensatory damages, stiff civil penalties, and triple damages.

If the false claim suit is successful, it not only stops the dishonest conduct, but also deters similar conduct by others. The whistleblower may receive a substantial share of the government's ultimate recovery–as much as 30 percent of the total.

Retaliation by the employer is prohibited. The False Claims Act punishes an employer for retaliating against an employee for attempting to uncover or report fraud on the federal government. If retaliation does occur, the whistleblower may also be awarded:

> all relief necessary to make the employee whole,

including reinstatement, two times the amount of back pay, litigation costs, and attorney fees.

7.2 Trends

In 1992, only seventeen healthcare fraud suits were filed. In 1992, *National Health Laboratories* settled a case with the Government for $110 million. In 1998, almost three hundred such suits were filed. The settlements made it apparent that recoveries in fraud cases had the potential to be of budgetary significance. That got the attention of Congress.

In the 1990s several state legislatures required joint efforts between state law enforcement agencies and private insurers to address healthcare fraud. In 1994, Pennsylvania established its Insurance Fraud Prevention Authority to serve as a conduit for insurers to fund specific investigators and prosecutors who work only on insurance fraud. For certain information-sharing activity Massachusetts, Florida, Ohio and New Jersey have similar legislation. These laws are often quite specific in imposing obligations upon insurance companies to

- establish anti-fraud units with specified dollar budgets and
- deliver the results of their investigations to specific state law enforcement agencies.

The state law enforcement agencies in turn provide immunity for the authors of such reports when they form the basis of state civil and criminal action.

The late 1990s witnessed a dramatic increase in federal funding to control fraud in the healthcare industry. As a direct result, the numbers of successful *prosecutions* rose dramatically. Many providers have reacted to the enforcement effort by devoting significant resources to compliance. In other words, the providers are making accurate billings. The Medicare program is benefiting by this trend, the 'sentinel effect' of enforcement.

Threats of looming insolvency for *Medicare*, combined with protests from a public convinced of rampant fraud, spurred *Congress* into action. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 contains tough, concrete provisions aimed directly at fraudulent practices. HIPAA significantly expands the False Claims Act. It lowers the bar for the definition of *fraud* itself (Thornton, 1999). HIPAA removes the concept of intentional from civil fraud, preserving it only for criminal acts. HIPAA increased

- the percent of the award that could be paid to whistleblowers,
- returned the fines collected back into the Fraud and Abuse Control Program, which funds the investigations, and
- created the *Medicare Integrity Program*, which contracts out the investigative work to the private sector.

Billions of dollars are now annually paid in settlements on healthcare fraud.

7.3 Coding

In the course of treatment, physicians or other healthcare professionals insert diagnostic and treatment information into the medical record. This information is then classified or coded. Insurers and the government will then relate these *codes* to categorical *reimbursements*.

Pressure exists to recover the greatest reimbursement for an episode of care. If a healthcare provider says that patient with condition x was treated, then a lesser reimbursement may be possible than when a patient with condition y was treated, even when the treatments are the same in each case. The difference between x and y may be subtle and knowledgeable people might even argue whether the proper diagnosis is x or y. So the healthcare provider is motivated to say that the diagnosis is y. Of course, if the provider says this knowing that it is false, then the provider is guilty of fraud.

Reimbursement consultants and software packages can help providers increase reimbursement through

Correct Claim		
Procedure Code	Description of Procedure	Reimbursement
ID1234	Incision and Drainage of Abscess	$250

Fraudulent Unbundling of Claim		
Procedure Code	Description of Procedure	Reimbursement
ABC7890	Local Anesthesia	$100
GHI0011	Surgical Procedure on Skin or Soft Tissue, Not Otherwise Specified	$200
XYZ5555	Wound suturing	$150

Figure "Fraudulently Unbundling".

up-coding or coding that is intended to earn the maximum revenue based on the available evidence. Some up-coding is accomplished by a few consultants who review charts and try to apply all available codes. If proper coding guidelines are not followed, then some simple checks of certain properties of the codes might betray those facilities that inappropriately utilize this strategy for maximizing revenue.

Given the practices followed by insurance companies and the government to combat up-coding, providers may also engage in 'down-coding' or 'under-coding':

- 'Down-coding' occurs when the proper code is known and a deliberate decision is made to submit a claim for a lesser service in the belief that the proper code would subject the case to strenuous scrutiny. This scrutiny may require considerable effort by the provider to create copies of the medical record for the payer to study, and the payer may delay payment to the provider. Providers fear that their submitted code will be diverted for manual review and result in cash-flow problems.
- 'Under-coding' occurs when physicians systematically report less work than they do, believing they can avoid a confrontation by not getting near the line. When physicians do not fully understand the coding rules and the anti-fraud regulations, 'under-coding' may seem the safest route. The cynics believe the government does not investigate these cases because more accurate reporting would result in greater payments.

Those that systematically 'under-code' might receive greater reimbursement when technology assists them in coding.

One insidious form of fraud is known as unbundling of services. A fictitious example follows. Suppose a patient has a soft tissue abscess. She goes to her physician, and he drains the abscess. The proper way to bill for the service according to Medicare guidelines is as a single procedure 'Incision and Drainage of Abscess' costing $250 (see Figure "Fraudulent Unbundling"). Instead, the physician decides to unbundle the bill into three procedures to get a higher reimbursement:

- Local Anesthesia costing $100,
- Surgical Procedure on Skin or Soft Tissue, Not Otherwise Specified costing $200, and
- Wound Suturing costing $150.

Medicare is starting to use software to attempt to identify unbundling of services. Procedure and diagnosis codes are vital for this effort, as Medicare would be hard pressed to detect unbundling in narrative claims rather than in coded claims.

7.4 Coding Software

Tools are available to facilitate coding. Physicians can turn to vest pocket cards, paper templates, and computers for help in anticipating how much reimbursement might be received for a particular diagnosis or treatment. Functionality ranges from table lookups of published requirements to logic-based, real-time background monitoring and analysis of clinical documentation.

3M Corporation (www.3m.com) is a leader in healthcare coding for billing software. The *3M Coding and Reimbursement System* includes several standard references. There are many cross-references, which can make coding, and reimbursements more accurate and consistent. The system is designed to optimize revenue:

- special prompts highlight explanations that can influence code choice,
- edits are incorporated into the software to help the coder arrive at the correct code, and

- a review process analyzes the record and highlights information that can be used to further enhance the code assignment.

Analytic software that is contained in the 3M Coding and Reimbursement System:

- manages the complex rules and terminology of coding.
- helps determine the standard code for procedures and services provided for outpatients.
- calculates reimbursement based on formulas that implement the appropriate national and hospital-specific variables. It utilizes Medicare inpatient and outpatient formulas and a variety of other reimbursement formulas.
- helps coders uncover additional, often overlooked, secondary diagnoses or treatments.

3M's coding compliance tool audits and records each critical step in coding. The resulting 'snapshots' allow the healthcare financial services unit to document exactly what coding problems have been found. The software has two interface options -- it can work with a batch interface or can review coding concurrent with the coding session. The software provides edit messages that specify the nature of the compliance problem. The healthcare provider will have the information needed to influence individual coders and clinicians that caused the errors in the first place to take corrective action. For example:

- Resource Edits: Evaluate length of stay and charges to determine if they are consistent with clinical data.
- Clinical Edits: Evaluate the clinical consistency of the coded data.
- Code Edits: Evaluate the coding sequence and compliance with established coding rules.

In order to cover the spectrum of compliance issues, Audit Expert Software incorporates the coding rules and guidelines of many organizations -- the same guidelines the government inspectors use in their audits. As the software supports variations in coding to achieve different reimbursements, it legally and ethically toes a fine line between supporting the most accurate conclusions and those that are financially most beneficial.

7.5 Fraud Detection Software

Software can help detect fraud. For instance, Texas has the *Texas Medicaid Fraud and Abuse Detection System* (Cupito, 1998). The system produces a profile and a numerical score for each provider's risk of Medicaid fraud. The system provides lists of people whose behavior is different. Lists of suspects are given to fraud analysts and investigators for follow-up. The Texas fraud detection system uses statistical methods and logical rules. The system gathers information from many sources, and combines and analyzes it. One of the most important initial tasks is defining *features* to extract from raw claims data.

Typical fraud patrolling is done reactively. A deviant pattern of claims is detected, and an investigation is done as to whether that past pattern represented fraud. A proactive mechanism predicts future events. It might anticipate possible fraud and then investigate whether it was occurring. Or a proactive mechanism might alert investigators to anticipated deviations in data and let the investigators know that those deviations would not be expected to be fraudulent in nature and thus would not merit further attention. For instance, if a major, new, high-risk construction project begins near a small town that will lead to a higher rate of accidents in the short term, and then those patrolling the health reimbursement claims could be notified of this and could anticipate the change in claims patterns. With this proactive approach, the *fraud patrol* could focus its attention where problems were most likely to be.

The costs of fraud to the American healthcare system are enormous. The government has mounted various campaigns to try to stop fraud. Information systems can play an important role in supporting the fight against fraud.

7.6 Questions

Reading Questions

1. Why is fraud based on misrepresentation of the reasons for a treatment harder to detect and prosecute than fraud for failing to provide a service?
2. What motivates a whistleblower? Why did the False Claims Act encourage whistleblowing?
3. Summarize key attributes of the 3Com coding software.

Doing Questions

- Suggest new ways in which the whistleblower concept could be applied to encourage the spread of information systems in health care.
- What is the fragile relationship between coding software that helps a provider assign codes that will earn fair compensation and fraud detection software that looks for incorrect assignments of codes? Compare and contrast the coding software used by health care providers and the fraud detection software used by the government in terms of the rules employed, the scale at

which applied, and the extent to which the algorithms inside one system would be used inside the other system. If you can find any supporting information about either coding software or fraud detection software related to coding, please provide that evidence.

- The large scale data collection and analysis as done in the state of Texas anti-fraud example would seem to be one way forward for the use of information systems in fraud detection. Look for other examples of such systems in use and describe the results of your search.
- Consider the issue of reactive versus proactive detection and suggest additional ways to proactively detect fraud.

Part IV: Ecommerce

8 Networks


Main Points

- Standardized clinical data and the computerized patient record are critical to integration and to quality health care.
- Community health information networks support public health. An example is provided of a network to help in the management of substance abuse patients.
- Electronic Data Interchange is necessary in modern business to facilitate the management of transactions.
- The use of the Web has empowered patients to assume more direct responsibility and control over their health care.
- A National Health Information Network is invisioned.

The connection of components of the health care system is a major step in improvement of the health care system. Through networking different portions of one entity can better coordinate their efforts and separate entities can be linked and support one another.

8.1 Community Health Networks

Community health care encompasses all the services for the prevention of illness in the community. A comprehensive range of community health care services is seldom to be found in any single location. Maintenance of accurate birth and death records, protection of food and water supply, control of communicable diseases, abuses of alcohol and drugs, and occupational health safety are examples of community health care activities (Smith, 2000).

Community Health Information Networks (CHINs) include a computer-based information system and focus on community health. Some people use the term 'community health information network' to refer loosely to any information network connecting different entities in a community involved in health care and would thus consider an information network connecting a hospital and a health plan in one community to be a CHIN. However, this book prefers the more focused definition of CHIN that includes an emphasis on 'community health'. Information networks that are primarily supporting hospital-based treatment of disease would thus not be

CHINs. Examples of Community Health Information Networks (CHINs) appeared already decades ago, but their prevalence and importance have grown.

A CHIN has three essential technical services:

- linkage,
- information access, and
- data exchange.

CHINs may link local clinics, state and federal health agencies, hospitals, and other entities. A CHIN should address community health concerns and eliminate geographic and bureaucratic barriers to communication and information exchange for community health purposes.

To understand better the complexity of the community or public health sector one can consider the organizations responsible for it in the United States. The *Center for Disease Control* (CDC) is a federal agency charged with surveillance and control of diseases. State and regional health departments possess responsibilities in the promotion, protection, and maintenance of the health and welfare of citizens and often connect local health authorities with national agenda. The local health authorities are often under the jurisdiction of municipalities and implement such services as restaurant inspections and the collection of birth and death data. Various non-governmental organizations, such as the Heart Foundation or the Rotary Club, assume various voluntary responsibilities as regards fund raising, education, and various services for community health care.

The CDC initiated the *Information Network for Public Health Officials* (INPHO) in 1992. The ultimate goal of INPHO is to improve the health of Americans through more effective public health practice. The INPHO initiative addresses the serious national problem that public health professionals have lacked ready access to the authoritative, technical information they need to identify health dangers, implement prevention and health promotion strategies, and evaluate health program effectiveness. Among other services, INPHO helps public health practitioners have electronic access to health publications, reports, databases, directories, and other information. Dozens of states have participated in INPHO projects since 1993 under funding from CDC.

INPHO uses CDC WONDER (*Wide-Ranging Online Data for Epidemiological Research*) as an online, multi-way public information system. WONDER provides a single point of access to a wide variety of CDC reports, guidelines, and numeric public health data. WONDER simplifies access to public health information for state and local health departments, the Public Health Service, the academic public health community, and the public at large. WONDER supports public health research, decision-making, priority setting, program evaluation, and resource allocation (wonder.cdc.gov).

INPHO is only one of many examples of CHINs. Another set of CHINs was created through U.S. federal funding under the banner of the Target Cities Program of the 1990s (Smith, 2000). The *Target Cities Program* provided Federal aid to enhance substance abuse treatment systems. Target Cities established in each of 20 major cities a Central Intake Unit to be the single point of access for clients who experience substance dependency or abuse problems. Central Intake Units provided standardized assessment and care management to the clients, referring them to providers of treatment, recovery, support and other services.

Despite the significant technological investments in some CHINs, the successes have not always met the expectations. The primary challenges are *people-related* rather than technically-related. A CHIN is primarily about knowledge management, and knowledge management efforts depend fundamentally on organizational management. Successful CHIN projects thus typically require, among other things, extensive training of the people in the participating organizations (Ross, 1998).

8.2 EDI

A business transaction is an interaction between two parties where one party agrees to do something for the other party in return for some kind of compensation. The goal of business-to-business ecommerce is to enable companies to perform business transactions electronically. Thus activities of human actors need to be transferred to the computer. When human actors are directly involved in a business transaction they have an understanding (often implicit) about the context of the transaction. Ecommerce captures the context of the transaction from the real world and brings it to the system level in a structured way (Williams and Whalley, 2000). Standards for business transactions strive for electronic *interoperability* between organizations (Stegwee, 2001). Business Transaction Standards are a set of definitions, specifications, and guidelines that enable the interoperability of independent systems with respect to the joint execution of a specific class of business transactions.

Standardizing commerce is as old as culture. The invention of money was to abstract goods. For the use of electronic communication, history might go to

1910 when fifteen florists in Belgium banded together to exchange out-of-town orders for flower arrangements via telegraph. Their Florists' Telegraph Delivery group, now FTD Inc., was an example of standardizing commerce with electronic communication. A larger example of the use of telegraph in commerce occurred in 1948, when the Soviet Union cut off road, rail and barge access between Western Germany and the parts of Berlin that were controlled by the U.S., England and France after World War II. Western powers intervened to supply Berlin's inhabitants with the necessities of life by air. With aircraft landings at the rate of one every three minutes, cargo had to be loaded and off-loaded faster than accompanying paperwork could be completed and verified. Because of this, inventory lists were rarely up-to-date and ordering and expediting lists became of little consequence. Recognizing the need to standardize the paper manifests from different countries (and in different languages) and the need to communicate this information independently from delivery, a standard manifest system was developed that could be communicated via telex. From this standard manifest system, electronic data interchange (EDI) evolved.

By 1968, so many railroads, airlines, truckers and ocean shipping companies were using electronic manifests that they formed the Transportation Data Coordinating Committee to create cross-industry standards. In 1975, that Committee published its first EDI specifications. In 1978 this became the Accredited Standards Committee X12 (ASC X12). Tasked with the development of EDI standards that would be acceptable across industries, X12 created standards for purchase orders, invoices, and requests for quotation.

Both users and vendors input their requirements to create a set of standard data formats that:

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

The EDI developers did not use then-current words and phrases, and instead what others were calling an electronic document, they termed a Transaction Set. That which might have been deemed a record, was named a Data Segment, and what seemed to others to be a field, was called a Data Element (Bass et al, 2002).

8.3 Health Ecommerce Networks

Another common use of the term Community Health Information Network is for a network that supports ecommerce among providers and payers. This book prefers to call those networks Health Ecommerce Networks (HENs). HENs are particularly compelling when providers and plans seek to standardize transaction requirements and reduce the cost of creating a common platform. Representative collaborations include (Noss and Zall, 2002):

- Wisconsin Health Information Network (WHIN),
- New England Healthcare EDI Network (NEHEN), and
- HealthBridge of Cincinnati.

WHIN subscribers pay on a per transaction basis. Among the functionalities provided by WHIN are:

- Eligibility and Benefits Verification,
- Referral Status and Submission,
- Claims Status and Submission,
- Hospital Administrative and Clinical Data,
- Lab and Radiology Results, and
- Access to Educational Resources.

WHIN provides access to eligibility information for over 100 payers and provides access to information at 15 Wisconsin hospitals. WHIN demonstrated cost reductions between $17,000 and $68,000 per physician practice through making electronic requests for information to hospital departments.

NEHEN was formed by six provider organizations, eight health insurers, and the Massachusetts medical society. NEHEN focuses on HIPAA-compliant transactions. The cost per transaction for NEHEN is reported to be less than 5 cents, compared to the typical 35 to 50 cents for nonstandard electronic transactions. NEHEN has been able to achieve significant provider adoption and at least 70 percent of each hospital's eligibility transactions can be done online.

HealthBridge of Cincinnati started in 1997 as an independent not-for-profit organization between major payers and hospital systems in Cincinnati, Ohio. Access to HealthBridge is free to physicians. The project provides:

- Eligibility Inquiry,
- Secure Messaging, and
- Clinical Results from Hospitals.

The hospital sponsors of HealthBridge have provided significant clinical information to physicians, including laboratory and radiology reports. Access to payer information and systems is limited.

Table "Health Care on Internet"	
Stage	Consumer Capability
1) Information Access	Medline, Disease Specific, Product Centric
2) Community	Support Communities, Treatment Alternatives, Quality Comparison
3) Personalization	Personalized News, Risk Profiling, Online Records
4) Transactions	Coverage Selection, Lifestyle Programs, Drug Authorizations
5) Services	Disease Management, Scheduling, Compliance Programs

What factors determine the success of a HEN? Hospitals tend to have more access to capital and technology resources than individual physicians and also have important clinical information. Payers are critical to providing administrative and financial transactions. Achieving a critical mass of payers in a market is important. WHIN and NEHEN have had significant payer participation from the outset.

To obtain initial participation in a HEN, it is critical that it have credible sponsorship within its local community. In the cases of HealthBridge and NEHEN, neutral entities were created by a broad base of sponsors within the local healthcare community.

Unless the architecture for the HEN is going to be built in-house, a reliable technology partner is critical to the success of the HEN. NEHEN has had a successful partnership with one of the largest healthcare IT vendors. WHIN has been less reliant on a single technology partner and has different vendors for different functionalities. HealthBridge has relied primarily on internal architecture development.

8.4 Supply Chain Management

Through group purchasing, companies may achieve cost containment, improve the quality of goods

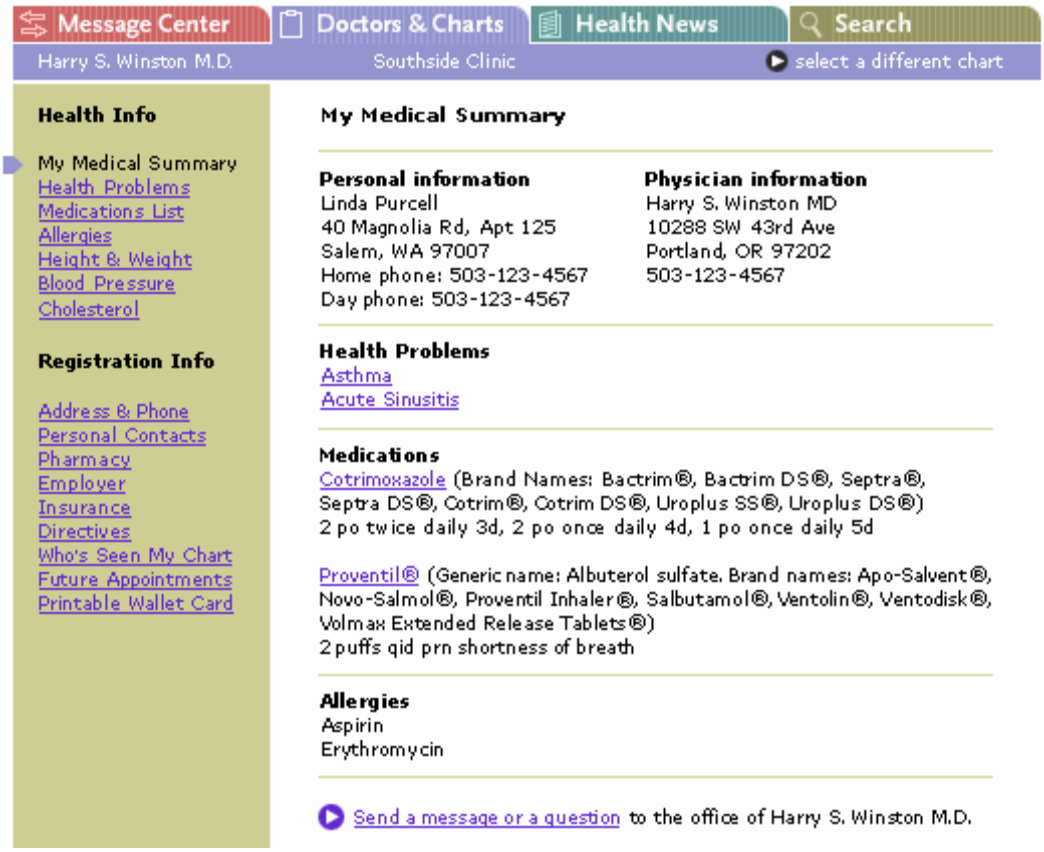


Figure "Doctors and Charts": In this web window of the consumer medical record system, the patient sees details of her medications and allergies.

purchased, and allow staff to focus their efforts on other activities. Goods and purchased services accounted for the second-largest dollar expenditure in the hospital setting. About 80% of every acute care supply dollar is acquired through group purchasing. However, the state of supply chain management is primitive in health care as contrasted with the consumer goods or industrial manufacturing (Langabeer, 2005).

Purchasing for health care organizations must meet the needs of management, key business stakeholders, clinician partner preferences, and patients. The enormous push to achieve standardization has achieved only modest success. Purchasing in the typical hospital is an antiquated process in which multiple customers independently access suppliers, distributors, and hospitals (Rundle, 2000).

The biggest potential benefit of e-commerce for providers involves eliminating overpayments and reducing rework and manual processes. The benefit for suppliers lies in freeing sales representatives from administrative tasks, enabling them more time to sell, providing access to real-time sales information, allowing for better management of fill-rates and operational processes and reducing the level of effort for labor-intensive administrative processes including contracts, rebates and eligibility.

8.5 Consumers

Health care in the US has been provider-centered. This means

- authoritative decision-making from the doctor,
- the provider is the source of all information,
- care is provided at the doctor's office or hospital, and
- the emphasis is on treatment.

The Internet supports *consumer-centered* care. This means the provider and patient collaborate in decision-making, the consumer finds information from the Internet, care is provided at home, and the emphasis is on prevention.

8.5.1 Web Trends

Health is one of the top three categories of Internet users' interests. While health information for many is an episodic need, this could not be further from the truth for the 100 million individuals in the U.S. with

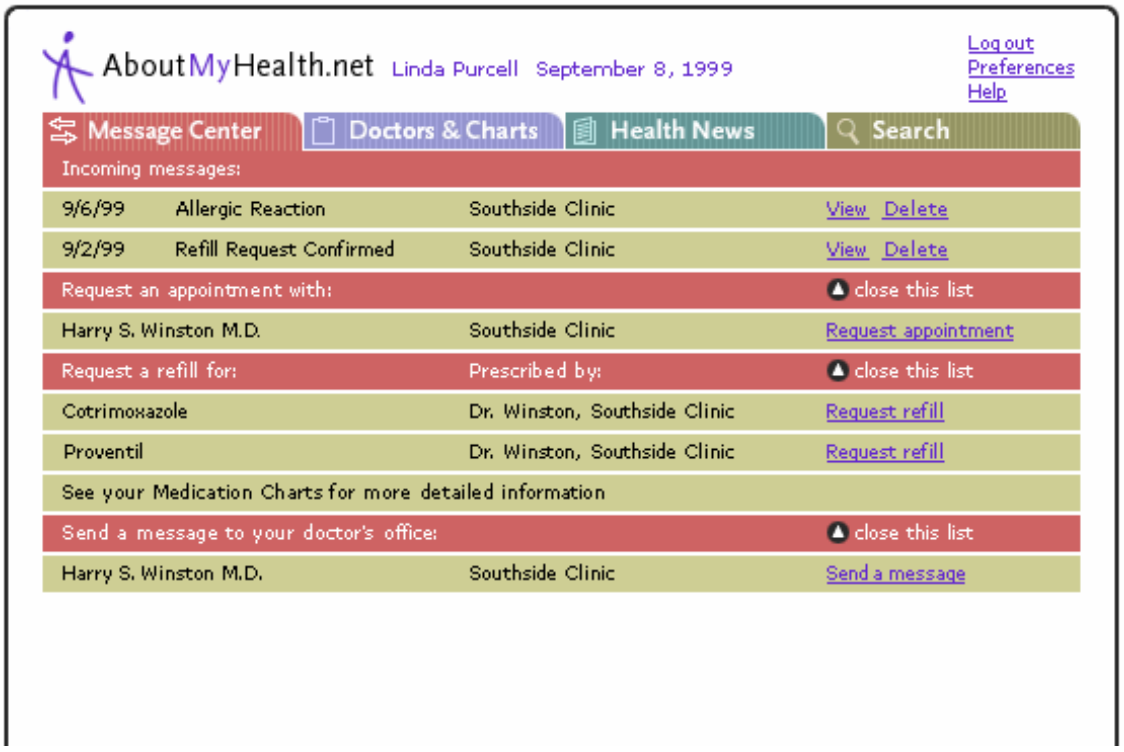


Figure "Messages": In this web window onto the consumer medical record, the patient sees her incoming messages from the medical practice and specifics about refills.

chronic illnesses (as well as their families).

Grove (1996) says the *strategic inflection point* of industries is the critical juncture where old models of conducting business are rapidly displaced by a new model, as a critical mass of cultural, regulatory, and technological change comes together. This may be happening now in medicine and has happened already in the financial markets.

The *financial industry* was at first skeptical of the individual investors' ability to manage their own portfolios. But the advents of the PC and the Internet have rapidly and dramatically changed the face of investing. Will the health care industry enter an analogous transformation, as the confluence of the Internet and health care creates its own 'strategic inflection point' for the industry (see Table "Health Care on Internet")?

The Web allows *mass customization*. For example, information about specific health conditions can be provided at appropriate levels of understanding. Risk appraisal can also be done online. For example, personal health plans can be tailored to risks for heart disease. The Web can simplify routine transactions, such as prescription refills, scheduling office visits, and certain authorizations. For routine follow-up of specific problems, the Web sites that generate targeted email might be helpful (Payne and Kiel, 2005).

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 and responsibility of 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 large amounts of 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.

8.5.2 Examples

Aboutmyhealth.net allows patients to online

- gather, view, and share physician medical records,
- communicate with physicians,
- order prescriptions and other healthcare products,
- manage diseases such as diabetes,
- assess wellness, and
- receive context-specific health news and information.

In one project with The Sisters of Providence Health System in Portland, Oregon, the patient initially sees a screen introducing the family medicine clinic. An example of the use of aboutmyhealth.net is provided based on a demonstration for a fictitious patient provided at aboutmyhealth.net.

The *fictitious patient*, 'Linda Purcell', has asthma and acute sinusitis. When Linda logs on, the first screen she sees asks her to enter a user ID and PIN number. Then she sees a screen that offers her a choice of message center, doctors and charts, health news, and search. In the 'Message Center' (see Figure "Messages") she can view communications from her physician, request an appointment, ask for a prescription refill, or send a message to the doctor.

When Linda moves on to the *Doctors and Charts* section (see Figure "Doctors and Charts"), she can view a medical summary, a description of health problems, a medications list, allergies, weight data, blood pressure, and cholesterol data. She can also view and update registration information that includes contact information, pharmacy, employer, insurance, directives, who has seen her chart, future appointments and a printable wallet card. She can click on the health problems listed and get a summary of the problem, its diagnosis, and treatment. If she clicks on any of the medications she can receive instructions on taking the drug and contraindications. At any time, she can send a message to the physician's office.

There is a counterpart application that allows physicians to create their own version of the medical record. With this *web-based patient record program*, patients can receive prescriptions directly from their physicians over the Internet. Or patients can send their physicians a message, which the physician can respond to and then forward prescriptions to an online pharmacy. The patient can receive the medication in the mail, or pick it up at a nearby physical pharmacy.

A 'personal medical record' system that can be used either on a stand-alone computer or across the Internet is called CapMed (www.capmed.com). The CapMed system was developed by a neurosurgeon who used it with his patients. Denton (2001) provided 330 patients a copy of CapMed and their medical records as Denton had them in his office. One year later, he conducted a mail-in survey that posed a series of relevant yes-and-no questions regarding usage and invited narrative comment and anonymous responses. Patients

- intended to begin or continue keeping records,
- used CapMed on medical visits,
- would rather not store health information on the Internet,
- wished to use e-mail with the doctor's office,
- believed doctors do not keep full records, and
- strongly believed individuals should keep their own records.

In addition to gaining new information from informed patients, Denton established the technical feasibility of transferring information between doctor's office and personal health records.

8.6 National Network

Evidence of the importance of information networks is reflected in the US government creation in 2004 of the Office of the National Coordinator for Health Information Technology (ONCHIT). ONCHIT is to implement a vision for widespread adoption of interoperable electronic health records by 2015. Presidential Executive Order #13335 issued in 2004 created ONCHIT and charged it with 4 primary responsibilities:

- Serve as the senior advisor to the Secretary of DHHS and the President of the US on all health information technology programs and initiatives;
- Develop and maintain a strategic plan to guide the nationwide implementation of interoperable EHRs in both the public and private healthcare sectors;
- Coordinate the spending of approximately $4 billion for health information technology programs and initiatives across the federal enterprise;
- Coordinate all outreach activities to private industry and serve as the catalyst for healthcare industry change

Essentially, ONCHIT is to support the development of a nationwide health information network (NHIN). A NHIN is an Internet-based architecture that links disparate health care information systems together to allow patients, physicians, hospitals, community health centers and public health agencies across the country to share clinical information securely.

To gain broad input on the best mechanisms to achieve nationwide interoperability, DHHS requested input from anyone. The request specifically asked for feedback on how a NHIN could be governed, financed, operated, and supported. Among the many opinions expressed, significant support emerged for the following concepts (DHHS, 2005):

- A NHIN should be a decentralized architecture built using the Internet, linked by uniform communications and a software framework of open standards and policies.
- A NHIN should reflect the interests of all stakeholders and be a joint public/private effort.
- A governance entity composed of public and private stakeholders should oversee the determination of standards and policies.
- A NHIN should be patient-centric with sufficient safeguards to protect the privacy of personal health information.
- Incentives will be needed to accelerate the deployment and adoption of a NHIN.
- Existing technologies, federal leadership, prototype regional exchange efforts, and certification of EHRs will be the critical enablers of a NHIN.
- Key challenges to developing and adopting a NHIN were listed as: the need for additional and better refined standards; addressing privacy concerns; paying for the development and operation of, and access to the NHIN; accurately matching patients' identity; and addressing discordant inter- and intra-state laws regarding health information exchange.

Other overarching concepts that were espoused by many of the respondents included:

- There is a need for some form of implementation and harmonization at a regional level.
- Cooperation between the public and private sectors is essential for successful realization of a NHIN.
- The NHIN should evolve incrementally and include appropriate incentives, coordination, and accountability to succeed.
- The federal government plays a role in advancing a NHIN.

The fiscal year 2006 budget for ONCHIT was $75 million, which will not be enough to finance a small part of a NHIN, but may help focus attention.

Clinton (Aug. 11, 2000): With today's release of new national standards for electronic claims for health care transactions, we are taking a major step.

9 Provider-Payer Transactions

Learning Objectives

- Assess costs of transactions.
- Delineate the different parts of transaction and code sets standardization.
- Construct a sketch of an X12 message based on Implementation Guide details and certain data content.

9.1 Cost Savings

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.

The cost of paper versus electronic transactions can be readily computed. Ten minutes on the phone to check eligibility compared to six seconds electronically adds up. An electronic remittance advice can be posted in a fifth the time required for manual posting. While the savings in labor is significant, the biggest savings could come from reduced bad debt. 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.

If one considers a small group physician practice, then one can illustrate simply enough the benefits to electronic transactions. 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.

The labor savings from automation is about $14k. The savings from bad debt reduction is about $105k. An illustrative spreadsheet is provided in the Table “Cost Savings”.

A different perspective on costs considers the challenge of different formats which have historically plagued the management of provider-payer transactions in the US. To understand the costs of multiple formats, an analysis of the number of translations is presented. Assume there are formats A and B and messages have to be shared that might be in either format. A *translator* is needed from format A to format B and conversely. If there are 4 formats A, B, C, and D, then 12 translators 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, and D to C. The 12 can be computed from 4 times (4-1). In general, for n formats, n times (n-1) translators are needed. Thus, for 400 standards there would be needed 400 times 399 or approximately 160,000 translators.

9.2 History

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

Table "Cost Savings"

General Practice Information		Your Information	Automated Process
Number of Visits Per Week		260	x
Average Claim Value	($)	$191	x
Number of Visits with Insurance per week		215	x
Staff Cost per hour	($/hr)	$14	x
Average number of eligibility checks in a week		33	x
Average number of claim follow-ups in a week		44	x
Average number of referrals in a week		25	x
Amount of time spent to (minutes)			
Obtain eligibility on a patient		11	0.5
Prepare a claim		6	0.5
Post a Payment		11	0.5
Obtain status of a claim		18	0.5
Referral check		13	2
Yearly Cost Estimates			
Eligibility Verification		$4,404.40	$ 200.20
Claims Preparation		$15,652.00	$1,304.33
Account Posting		$28,695.33	$1,304.33
Claim Status Follow-up		$9,609.60	$ 266.93
Referral Prepared		$3,943.33	$ 606.67
Total Estimated Yearly Costs		**$62,304.66**	**$3,075.79**
POTENTIAL YEARLY SAVINGS			**$59,228.87**

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
Increase in Potential Profits – Yearly	($)	$129,116.00

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.

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.

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)*. The government asked WEDI to evaluate electronic claims standardized billing issues for the purpose of advancing electronic data interchange. However, 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."

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.

In 1993 the Clinton administration included standardized transactions in its blueprint for healthcare reform. The legislation known as HIPAA was finally passed in 1996. The legislation calls for the Department of Health and Human Services to create a Transaction Rule and that Rule was finished in 2000. The Rule specifies the format of transactions and the codes that will fill the fields in the forms.

9.3 Transactions

Electronic Data Interchange (EDI) has been important for decades. The prominent American standards development organization for EDI is the 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 the federal government has mandated as the standard for healthcare. These Implementation Guides include:

- 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 transactions in the appropriate form. For systems that generate transactions in other than compliant forms, other software might translate the information from the one format to the other.

PROVIDERS	routing	PAYERS	routing	SPONSORS
Eligibility Verification	270 eligibility inquiry ⟶ ⟵271 eligibility information	Enrollment	⟵834	Enrollment
Claim	837 claim submission⟶	Claims Acceptance & Adjudication		
Accounts Receivable	⟵ 835 payment advice	Accounts Payable		

Figure "Transactions among Provider, Payer, Sponsor":

9.4 X12 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 transaction is in the transaction set that followed. 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.

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:

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

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"		

where ITA is the data segment initiator. The subsequent two 1's are data elements separated by '*'. The segment is terminated with a ';'. 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 first overviews the transactions and then summarizes the '270/271 Eligibility Request and Response Transaction' Implementation Guides. The 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.

For situations where an "Implementation Guide" is not comprehensive, an entity can provide its own requirements and publish those in a "Compendium Guide".

9.5 Eligibility Details

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:

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' 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

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 a sample value 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*123456789
0~

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.

9.6 Further Detail

One can appreciate further details of the character of a transaction standard by elaborating other characteristics of the data segment guidelines and illustrating them with the 'information source' field of the eligibility inquiry (the '270') transaction.

The data element is the smallest named unit of information in the X12 standard. Data elements are assigned a unique reference number. Each data element has a name, description, type, minimum length, and maximum length. The data element types in the 270 Transaction are given in Table 'Element Types'.

Table "Data Elements of Information Source Name". CD is Condition Designator.

Name	Reference Designator	CD	Element Type	Length
Entity ID Code	NM101	M	ID	2/3
Entity Type Qualifier	NM102	M	ID	1/1
Name Last	NM103	O	AN	1/35
Name First	NM104	O	AN	1/25
Name Middle	NM105	O	AN	1/25
Name Prefix	NM106	O	AN	1/10
Name Suffix	NM107	O	AN	1/10
ID Code Qualifier	NM108	X	ID	1/2
ID Code	NM109	X	AN	2/80
Entity Relat Code	NM110	X	ID	2/2
Entity ID Code	NM111	O	ID	2/3

Table "Element Types"

SYMBOL	TYPE
Nn	Numeric
R	Decimal
ID	Identifier
AN	String
DT	Date
TM	Time
B	Binary

For ID type data elements, the manual or guide provides the applicable X12 code values and their descriptions or references where the valid code list can be obtained. Each data element is assigned a minimum and maximum length.

X12 has standard conditions designators. Data element conditions are of three types: mandatory, optional, and relational, as follows:

- M – Mandatory. The designation of mandatory is absolute as there is no dependency on other data elements.
- O – Optional. The designation of optional means that there is no requirement for a data element to be present in the segment. The presence of a value for a simple data element is at the option of the sender.
- X – Relational. Relational conditions may exist among two or more simple data elements within the same data segment based on the presence or absence of one of those data elements (presence means a data element must not be empty). Relational conditions are specified by a condition code and the reference designators of the affected data elements. A data element may be subject to more than one relational condition.

These define the circumstances under which a data element may be required to be present or not present in a particular segment.

Each data element in a segment is provided a structured code that indicates the segment in which it is used and the sequential position within the segment. The code is composed of the segment identifier followed by a two-digit number that defines the position of the data element in that segment.

Part of the 'Information Source Name' data segment of the 270 transaction is illustrated here. The data

segment identifier is NM1 and has the data segments condition designators, data type, length, and name as shown in the Table "Data Elements of Information Source Name".

9.7 Codes and Identifiers

Key components for the values of 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. 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).

Problems with the existing code sets are acknowledged (Chute et al., 1996).

Some of the fields in the transactions are filled with values from identifiers. In January 2004, DHHS published the Final Rule that adopts the National Provider Identifier (the NPI) as the standard unique health identifier for health care providers. Covered entities will use the NPI to identify providers in all standard transactions. The NPI is all numeric. It is 10 positions in length (9 plus a check-digit in the last position).

The Employer Identifier Final Rule was published in 2002. The 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.

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.

9.8 Testing

Each organization should test that it is 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.

Table "Partial Test Results"	
Line No	**Description**
8	*PRV*BI*ZZ*203BA0200N*
8	"203BA0200N" specified at Provider Taxonomy Code (PRV03) is not a valid Health Care Provider Taxonomy Code
13	Value "LU" does not look like a valid Reference Identification Qualifier (REF01). If Identification Code Qualifier (NM108) has a value of "XX", then REF01 must be either EI or SY.
16	*SBR*T********C*I
16	Insured Group Name (SBR04) is required when Insured Group or Policy Number (SBR03) is not present.

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:

- Level 1: Integrity testing – validation of X12 syntax.
- Level 2: Requirement testing – Testing for implementation of guide-specific syntax requirements.
- Level 3: Balance testing – 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.

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.

Reviewing a 'transaction testing' result, one gains insight about transaction processing and about testing. The HIPAA auditor (www.applabs.com) gives error reports that pinpoint the location and nature of errors in EDI files. First the user selects input file(s). One file chosen as input is an 837I which is a Claim from an Institution (see Figure "Actual Complete Transaction"). The partial results of the transaction test on this transaction show several errors (see Table "Partial Test Results").

9.9 Problems

Achieving compliance with the intent of the Transactions Rule has proven more difficult than initially envisioned. The intent was to reduce costs by standardizing the transactions. However, transaction variability has proven problematic. The sources of this problem are two-fold:

- The standards fail to cover some situations that need to be addressed, and thus entities are left in a quandary as to what to do. For instance, the standards do not adequately address the mode of the transaction or the acknowledgement of a claim.
- Entities are promulgating too many entity-specific requirements within a Companion Guide. They use situational and optional data elements in non-standard ways. In fact, some required data elements that have mandatory rules of use are used in non-standard ways. For example, some trading partners require the 837 to be submitted with the provider identification information (usually in the NM or REF segments) at the provider level (Loop 2000), the claim level (Loop 2300), and at the service level (Loop 2400), even though the provider has never changed. Standard use would only require the provider identification at Loop 2000 and any provider identification at Loops 2300 or 2400 as situational, if the provider is different at those levels.

This propagation of additional requirements that have not been outlined in the HIPAA-mandated Implementation Guides has caused abrasion among payers, providers, and the vendors that serve each (WEDI, 2005). This non-standard use of the transaction can play havoc with standard translators, testing systems, and other systems downstream.

The health transactions enterprise has a long history of introducing requirements in the transactions to accommodate particular work flow processes of each trading partner. In general, if a transaction exchange is not working and the transaction standard is in question by one of the trading partners, the use of the standard has been perverted and the non-standard work process has continued. To change this approach will require breaking old-style, well-working, well-rewarded habits in the industry. As of 2005, the cost savings envisioned through standardized transactions had only been partially achieved.

9.10 Epilogue

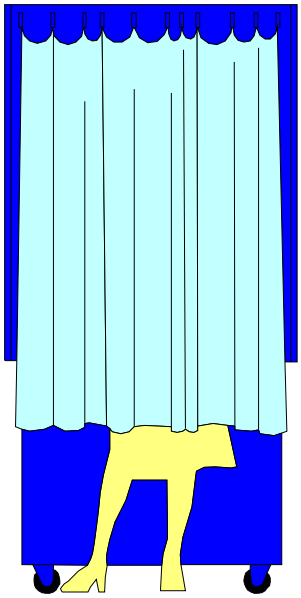
Initially, only a handful of transactions were standardized, and they emphasized claims and payments. However, the transactions that were initially standardized are the tip of the iceberg. For the payer-provider relation more transactions will progressively cover other aspects of the communication between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

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 major step towards such *standardization*.

```
ST*837*987655~
BHT*0019*00*12345*19980202*2121*CH~
REF*87*004010X096~
NM1*41*1*HEALTHCARE PPO*NAME1*NAME2***46*1234~
PER*IC*JANE DOE*TE*123456789~
NM1*40*2*INSURANCE COMPANY*****46*962TT8R~
HL*1**20*1~
PRV*BI*ZZ*203BA0200N~
CUR*85*AFA~
NM1*85*2*GENERAL HOSPITAL*****XX*32322~
N3*125 VIRGINIA AVE~
N4*CALIFORNIA*CA*90210*US~
REF*LU*420456789~
PER*IC*NAME1*TE*123456~
HL*2*1*22*1~
SBR*T********CI~
NM1*IL*1*BOZARTH*LANCE*D***ZZ*123456~
N3*5707 FERN FLOWER DR~
N4*COLUMBIA*MO*65202~
DMG*D8*19980201*M~
REF*SY*123456789~
NM1*PR*2*KEY INSURANCE COMPANY*****PI*66783JJT~
HL*3*2*23*0~
PAT*01~
NM1*QC*1*BOZARTH*MAGGIE*B~
N3*5707 FERN FLOWER DR~
N4*COLUMBIA*MO*65202~
DMG*D8*19691125*F~
CLM*72255589*2593.69***11:A:1*Y*A*Y*Y*********Y~
DTP*434*RD8*19961222-19961224~
DTP*435*DT*199612220930~
DTP*096*TM*1630~
QTY*CA*2*DA~
REF*9A*6003E0332701~
HI*BK:643.03~
HCP*06*2040*553.69*252665599~
NM1*71*2*NORDSTRUM*HAROLD****XX*572999543~
PRV*AT*ZZ*363LP0200N~
LX*1~
SV2*11**949.68*UN*1~
SV4*12345~
NM1*71*2*ABCD CORP*****34*123456789~
PRV*AT*ZZ*203BA0200N~
SVD*CD*1123*HC:111*123*123*123~
SE*45*987655~
```

Figure "Actual Complete Transaction": This figure is a complete transaction – it is just a sequence of lines of codes following a pre-agreed format – in this case an X12 837I format – such that two communicating partners know how to decipher the message. The transaction is from Applabs (www.applabs.com).

Part V: Privacy and Security



10 Privacy


Main Points

- Privacy is about power.
- 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, 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 flexibility in how they implement the privacy regulations, but they are expected to have a privacy officer, train staff, and document policies.

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.

10.1 Political Struggle

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 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.

10.1.1 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.

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.

10.1.2 Balance

The social philosophy of *communitarianism* holds that a good society crafts a careful balance between individual rights and the common good (Etzioni, 1999). 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.

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.

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.

10.2 HIPAA's Privacy Rule

HIPAA's 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. This chapter presents the *principles and related information of the Privacy Rule*.

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
- 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*.

10.3 Applicable

The Privacy Rule only applies to health plans, health care clearinghouses, and health care providers that transmit health information in electronic form in connection with a HIPAA standard transaction. Thus, an entity needs to answer three questions:

1. Is it a health plan, clearinghouse, or care provider,
2. Does it transmit health information in electronic form, and
3. Does it submit such health information in HIPAA transactions?

If the response to any of these questions is 'no', then the entity does not need to comply with its requirements. If the response to all the questions is 'yes', then the entity must comply with the Privacy Rule.

In the Privacy Rule, *health information* is any information, whether oral or recorded in any form or medium, that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Individually identifiable health information is a subset of health information, including demographic information collected from an individual, with respect to which there is a reasonable basis to believe the information can be used to identify the individual. Protected health information means individually identifiable health information in a covered entity.

10.4 Notice of Privacy Practices

The Privacy Rule extensively describes a Notice of Privacy Practices. Health plans must provide the Notice to all health plan 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. Health care providers must offer the Notice to patients on their first encounter.

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. Failure by this provider to obtain an individual's acknowledgment, assuming it otherwise documented its good faith effort, is not a violation of the Rule. Other covered entities, such as health plans, are not required to obtain this acknowledgment from individuals, but may do so if they choose.

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.

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 that entities must include in the Notice.

10.5 Authorization

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.

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:

- a statement that the individual may revoke the authorization in writing and
- a statement that treatment, payment, enrollment, or eligibility for benefits may not be conditioned on obtaining the authorization.

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.

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. An authorization may expire upon a certain event or date. An authorization that the covered entity knows has been revoked is not valid.

10.6 Uses and Disclosures

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 'disclosure' occurs outside an entity.

10.6.1 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.

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.

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

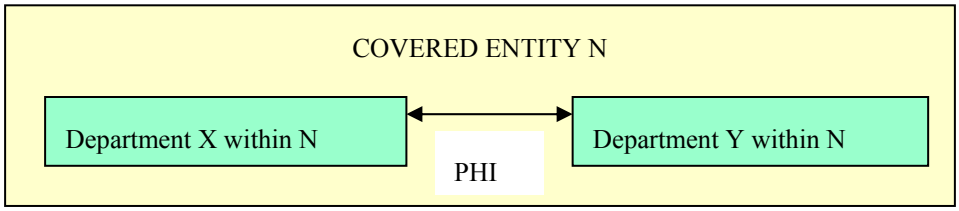


Figure "Use": Department X within the covered entity N is sharing protected health information (PHI) with another Department Y inside the same covered entity -- this is 'use'.

Figure "Disclosure": Covered entity N sends PHI to entity M -- that is 'disclosure'.

- 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*.

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.

An entity should have an organizational manual that indicates the functions of the entity. People perform certain functions. This mapping of people to functions is integral to implementing the minimum necessary standard.

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.

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*.

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.

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.

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.

10.6.2 Business Associate

Under normal circumstances, an authorization is required to share protected health information (PHI) with non-covered entities. However, under two conditions, PHI can be sent to a non-covered entity without an authorization from the patient -- those two conditions are:

- 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 entity 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. Examples of relationships that should include a business associate contract are a consultant that performs utilization reviews for a hospital and an independent transcriptionist that transcribes for a physician.

A covered entity is not required to enter into a business associate contract with an entity 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 affects the transfer of funds for compensation for healthcare.

10.6.3 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.

The de-identification method can use a statistically sound technique or the Safe Harbor specifications. In further detail:

- The *statistically-sound technique* 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 involves a minimum of burden and conveys a maximum of certainty that the rules have been met with an easily followed, cookbook approach.

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 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.

10.6.4 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.

10.7 Privacy Surrendered

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, such as for research purposes or for certain marketing purposes.

10.7.1 Research

The Privacy 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). 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.

Obtaining IRB approval in some institutions is difficult.

10.7.2 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.

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. 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.

10.8 Access to Information

A person has a right to his or her medical record.

10.8.1 Right of Access

The definition of the right of access is linked to the definition of 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. Despite the requirement to provide access, physicians maybe reluctant to share records, as they see less benefit in this sharing than the patients do (Ross et al, 2005).

10.8.2 Denial of Access

An entity may deny access to protected health information when the *physical safety* of an individual is endangered. 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.

10.8.3 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 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.

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 should normally be provided within 30 days of receiving the request, if the information is accessible on-site,

10.9 Confidential Communication

Entities must permit an individual to request a confidential communication channel. 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.

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.

10.10 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. *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 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).

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 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.

10.11 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.

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 entity must act on the individual's request for an accounting no later than 60 days after receipt of such a request. *The entity must provide the first accounting to an individual in any 12-month period without charge*.

10.12 Administration

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.

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.

10.12.1 Staff and Training

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. 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.

DHHS requires covered *entities to develop and document their policies* and procedures for implementing the requirements of the Privacy Rule. 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. 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.

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.

10.12.2 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*.

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*. 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.

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

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.

10.12.3 Enforcement

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 can file such *complaints*.

The DHHS *procedures are modeled on those used by DHHS's Office for Civil Rights*. DHHS requires 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.

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.

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 and Melamed, 2001).

10.13 Example Implementation

Achieving compliance with the Privacy Rule has been taxing of covered entities. Entities have tried where possible to build on existing efforts. An example follows for Carilion Health Systems. 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. Executive level awareness occurred first. In 2000 a Privacy Team was formed. The membership of the team was chosen to represent those areas of the entity most impacted by and whose participation in compliance was particularly critical (Rada et al, 2002).

Carilion next reformatted and reorganized the Privacy Rule. For example, one listing of rule components shows where documentation is required. Another early undertaking 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 data collection sheets were shared among like units, so that only differences needed to be recorded.

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 recorded anywhere. To avoid a completely new set of policies and procedures just for HIPAA, the practice folded 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 was also created and called 'Minimum Necessary Standard and Level of Access for Patient Information'. While the Privacy Team proceeded 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.

10.14 Conclusion

DHHS published a draft version of the Rule in 1999, and between 1999 and 2003 enormous debate occurred about the pros and cons of the Privacy Rule. Compliance with the Privacy Rule was mandatory as of April 2003. Healthcare entities invested massive resources in achieving compliance which included such time consuming steps as training all employees

and giving all patients a Notice of Privacy Practices. Maintaining compliance is also costly.

The hope by some had been that the Privacy Rule would usher a new era of electronic medical records and health care communication because people would now feel that privacy was assured. However, the impact of the Privacy Rule seems in many ways to have been otherwise. Health care professionals have been taught that the Privacy Rule makes severe restrictions in what can be done with patient information. Patients seem to have relatively little interest in exercising their right to access. The net impact seems to be largely that of another regulation taxing the health care system. For instance, the medical research community fears that important research is being compromised by well-meaning IRBs that are overly strict in their interpretation of the Privacy Rule (Feld, 2005). The challenge is to have the benefits of compliance exceed the costs.

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. *What about the fifth principle of 'consumer control'*? The principle of 'consumer control' is not part of the tradition of American healthcare.

11 Security

Main Points

- Electronic protected health information is covered by the Security Rule.
- The Security Rule is specific about risk analysis, a security officer, and training.
- Administrative Safeguards include management, workforce, access, and contingency plans.
- Technical Safeguards address encryption but focus on audit and access.
- Physical Safeguards include facility access and media controls.

The Security Rule 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. The implementation of reasonable and appropriate security measures supports compliance with the Privacy Rule.

11.1 Addressable

The Security Rule was published in the Federal Register in February 2003 and compliance was mandatory as of April 2005. Many consultants have found work as HIPAA security experts, and much new equipment has been purchased in an attempt to be Security Rule compliant.

The covered entities of the Security Rule are the same as those of the Privacy Rule. Within covered entities, HIPAA's security provisions apply to electronic protected health information. Electronically protected health information (EPHI) is PHI that is transmitted by electronic media or maintained in electronic media.

In general, DHHS is required to adopt standards developed by *American National Standards Institute* (ANSI) accredited Standards Development Organizations when such standards exist. However, the previously existing security standards developed by ANSI-recognized organizations are targeted to specific technologies or activities. No existing security standard, or group of standards, is technology-neutral and scaleable to the extent required by HIPAA. Therefore, DHHS developed a new standard in the Security Rule.

The Security Rule has administrative, technical, and physical standards. A standard is typically elaborated through several Implementation Specifications. The Security Rule establishes two types of Implementation Specifications:

- *Required*: The entity is required to implement exactly the specification.
- *Addressable:* The entity may assess whether the specification is reasonable and appropriate in the context of the entity's environment.

If an entity determines that any addressable safeguard is reasonable and appropriate, it must implement that specification. If the entity determines that an addressable implementation specification is not a reasonable and appropriate answer to its security needs, then the entity must document why. At this stage, the entity could implement any equivalent alternative security measure. If an entity determines that it can meet the standard by doing nothing, the entity may do so. The Security Rule simply requires that the entity document its rationale for its decision. To repeat, the covered entity may choose one of three options:

- *implement the specification*;
- *implement an alternative* security measure to accomplish the purposes of the standard; or
- *not implement anything* if the specification is not reasonable and appropriate and the standard can still be met.

In keeping with its results-based approach, the rule has heightened emphasis on internal risk analysis and risk management as the core elements of the security management process. Cost of security measures is a significant factor to be considered in security decisions. The decision about the *reasonable and appropriate* nature of an addressable specification rests on the covered entity and is based on its overall technical environment and security framework. This decision may rely on a variety of factors, including the results of a risk analysis, measures already in place, and the cost of implementing new measures.

11.2 Life Cycle

The life cycle of compliance begins with awareness. 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. Implementation and training must be followed by quality control.

11.2.1 Gap Analysis

The entity must determine the current status of its security protection – the baseline. Then this *baseline* must be compared to the requirements to determine the gap. 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 tailored to the HIPAA Security Rule, the baseline assessment design can be driven by the regulatory framework.

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.

A *Security Configuration Management Inventory* includes documentation of hardware and software assets. An organization wants to understand this inventory in order to know its potential vulnerabilities and determine what existing security capabilities reside in the assets.

The measurement criteria suggested as part of the gap analysis could include rankings of current readiness weighed against 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.

Gap details should 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 appropriate, 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*.

11.2.2 Risk Analysis

Risk analysis follows gap analysis. No matter how well a system is designed, *vulnerabilities remain*. Users, whether normal or hostile, may trigger or exploit these vulnerabilities. Such vulnerabilities become risks, and organization must determine how much effort to invest in preventing what *risks*.

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):

1. looking at the type of data an organization has,
2. determining who the likely candidates are for intercepting that data, and
3. determining the level of capital resources to target the problem.

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 annual, monetary loss expectancy. 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, 2000):

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.
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.

The Security Rule requires risk analysis. A thorough and accurate risk analysis would consider 'all relevant losses' that would be expected if the security measures were not in place (NIST, 2002). *Relevant losses* would include losses caused by unauthorized uses and disclosures and loss of data integrity that would be expected to occur absent the security measures.

Smaller entities, which deal with smaller amounts of information would have smaller physical facilities, smaller work forces, and therefore, would assume less risk. The smaller amount of risk involved means that the response to that risk can be developed on a smaller scale than that for larger organizations.

11.2.3 Risk Analysis Example

An example of risk analysis is presented for *Georgetown University Medical Center's kidney dialysis unit*. 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. 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.

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

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)

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 new operating system. Cost: 6 (cost of upgrading, 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").

Table "Severity of Threats"

	Frequency		
Expected Loss	Low	Medium	High
Low	1	2	3
Medium	2	4	6
High	3	6	9

Computations assign a cost/benefit value to each countermeasure. The Table "Analysis of Countermeasures" shows 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

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 countermeasure		3	2	2	2	3	1	1	1	6
cost/benefit		0.27	1.00	0.67	0.36	0.65	0.11	0.71	0.56	0.59
Y/N		Y	N	Y	Y	Y	Y	Y	Y	Y

Table "Analysis of Countermeasures": The row labeled Y/N shows a decision of whether or not each countermeasure should be recommended based on the cost/benefit ratio.

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.

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.

11.2.4 Information Security Officer

The Security Rule says that responsibility for security should be assigned to a *specific individual* to provide an organizational focus and importance to security. The assignment should be documented and responsibilities would include

- the management and supervision of the use of security measures to protect data, and
- the conduct of personnel in relation to the protection of data.

The following material about information security officers is not from the HIPAA Security Rule but is general guidance. 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.
- Knowledge 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.
- Knowledge 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*.

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.

11.2.5 Training

The Security Rule requires training of the workforce as reasonable and appropriate to perform their functions in the facility. Security training would typically become part of an entity's overall *training program*. Covered entities must have discretion in how they implement the requirement, so they can incorporate this training in other existing activities. One approach would be to require this training as part of *employee orientation*. The amount and type of training needed will be dependent upon an entity's configuration and security risks.

The Security Rule requires *security updates*. Security advisories or reminders should be periodically distributed to affected users, including contractors. Convenient delivery methods include e-mail, flyers and an intranet site. Security reminders might include warnings on current risks such as latest viruses, social engineering, new technical vulnerabilities, and risks and countermeasures specific to the covered entity. The definition of periodic is left to each covered entity, but one reasonable frequency might be twice per year.

11.2.6 Quality Control

The gap analysis and risk analysis are steps in an organization confirming its *objectives* and assessing its compliance with its objectives. The Security Rule asks 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 the security standards, plan how to achieve its objectives, work to the plan, and document its work. Again the documentation must conform to the standard and the behavior of the people must conform to 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.

The Rule requires that the policies and procedures be documented in written form, which may be in *electronic form*. The Rule also provides that a covered entity may change its policies and procedures at any time, provided that it documents and implements the changes in accordance with the applicable requirements.

11.3 Administrative Safeguards

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.

11.3.1 Management and Awareness

The HIPAA Security Rule provides guidance in its section called *Administration* that applies both to the life cycle of compliance and to security policies. The Security Rule's *Security Management Process* standard has four implementation requirements:

- risk analysis,
- risk management,

- sanction policy, and
- information system activity review.

Risk analysis and management were described in the preceding 'Life Cycle' Chapter. Sanction policy and information system activity review are described next.

Sanction policies are recognized as a usual and necessary component of an adequate security program. The type and severity of sanctions imposed, and for what causes, must be determined by each covered entity based upon its security policy and the relative severity of the violation.

The *information system activity review* should promote the periodic review of an entity's internal security controls, for example, logs, access reports, and incident tracking. The extent, frequency, and nature of the reviews would be determined by the covered entity's security environment. Formal internal audits could prove burdensome to some covered entities due to the cost and effort involved.

The Security Rule has a standard for *awareness* with four addressable implementation specifications:

- Security reminders. Periodic security updates.
- Protection from malicious software. Procedures for guarding against, detecting, and reporting malicious software.
- Log-in monitoring. Procedures for monitoring log-in attempts and reporting discrepancies.
- Password management. Procedures for creating, changing, and safeguarding passwords.

Security reminders were covered in this book under 'training' in the life cycle of compliance. The other specifications are described next.

Procedures for guarding against, detecting, and reporting *malicious software* (including most notably viruses) should be known by all members of the workforce. Guidelines to the workforce might include

- Contact the help desk if there is an unidentified or strange file received through email.
- Upon identification of a virus, quarantine systems for proper remediation.

System administrators should *monitor log-in* attempts from unauthorized users through the examination of audit and log files. Users should be made aware of steps to be taken in the event of suspicious scenarios, such as when a user leaves his desk and returns to find that he cannot login.

All users should be aware of the importance of selecting strong *passwords*. Passwords should:

- be at least 8 characters long,
- contain a varied set of characters, such as lowercase and uppercase letters and numerals, and
- not use palindromes (like abba) or sequences (like 12345).

Users should be aware of the covered entity's policy for safeguarding passwords. That policy might say that passwords should not be shared but should be changed periodically.

11.3.2 Workforce Security

The entity should implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI and to prevent those workforce members who do not have access from obtaining access to EPHI. This workforce security standard expects:

- Authorization or supervision (Addressable). Implement procedures for the authorization or supervision of workforce members who work with EPHI or in locations where it might be accessed.
- Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to EPHI is appropriate.
- Termination procedures (Addressable). Implement procedures for terminating access to EPHI when the employment of a workforce member ends.

The goal is to assure that all personnel with access to EPHI have the required access authority as well as appropriate clearances. Some of the implementation specifications may not be appropriate to a given entity. For example, a clearance may not be reasonable or appropriate for a small provider whose only assistant is his or her spouse. The implementation specifications are addressable.

Authorization or supervision requires that workforce members, for example, operations and maintenance personnel, must either be *supervised* or have *authorization* when working with EPHI or in locations where it resides. Entities can decide on the feasibility of meeting this specification based on their risk analysis -- this implementation specification is 'addressable'. For instance, the supervision of maintenance personnel by an authorized, technically knowledgeable person might not be feasible in smaller settings.

Termination procedures are relevant because of the risks associated with the potential for unauthorized acts by former employees, such as acts of retribution

or use of proprietary information for personal gain. Yet, termination procedures have been made an addressable implementation specification because formal procedures may not be necessary. For example, a solo physician practice whose staff consists only of the physician's spouse would not invoke formal termination procedures. No specific termination activities, for example, changing locks, are expected by the Rule, because, although the activities may be considered appropriate for some covered entities, they may not be reasonable for others.

11.3.3 Information Access

Confidentiality means controlling who gets access to information. DHHS requires that patient information remains confidential. An organization is required to establish and maintain documented policies and procedures for granting different levels of access to healthcare information. This involves policies for establishing access, authorizing access, and modifying access.

For *information access management*, entities should implement policies and procedures for authorizing access to EPHI. Specifications include:

- Access authorization (Addressable). Implement policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, process, or other mechanism.
- Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

Restricting access to those persons and entities with a need for access is a basic tenet of security. By this mechanism, the risk of inappropriate disclosure, alteration, or destruction of information is reduced.

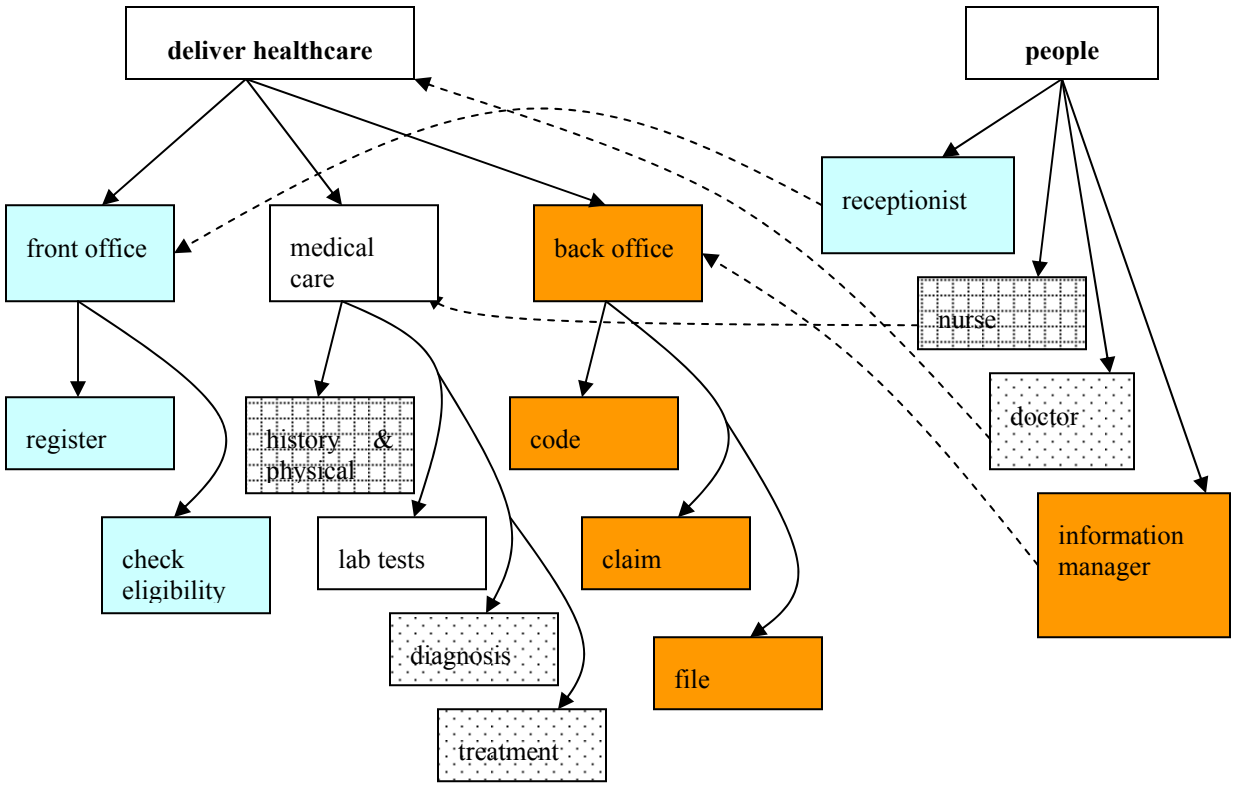


Figure "Roles to Information": The functions of the medical clinic are depicted in the left-hand tree -- three major functions of 'front office', 'medical care', and 'back office' are shown. The roles of the people are shown in the right-hand of the diagram. Each person in a role is expected to use certain types of information.

DHHS cannot, however, specifically identify roles and privileges. These will vary depending upon the entity, the needs within the user community, the system in which the data resides, and the specific data being accessed. This standard is consistent with the Privacy Rule (minimum necessary requirements for use and disclosure of protected health information).

In the next example a policy is based on who is in a renal dialysis unit. A more elaborate policy for Partners HealthCare System is then presented and followed by an example from long-term care.

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.

Partners HealthCare System 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' information access management 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 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.
- 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.

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.

Another example of access models comes from the long-term care industry. The roles in a typical long-term care facility include:

- A facility's certified nursing assistants provide the basic care.
- The dietary director oversees meal preparation. Cooks and dietary aides provide the hands-on meal preparation and delivery.
- The director of activities develops and organizes a monthly calendar of events. Most nursing homes have maintenance personnel and a small laundry and housekeeping staff. The business office generally includes an office manager, receptionist and several clerical personnel.

The diagram of roles to information (see Figure "Roles to Information") indicates how the facility might organize the assignment of people to the information they are allowed to access.

11.3.4 Incidents and Contingencies

Documenting and reporting incidents, as well as responding to incidents are an integral part of a security program. The Security Rule has a standard for *Security Incident Procedures*, which requires entities to implement policies and procedures to address security incidents. A *security incident* is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

A contingency plan protects the availability, integrity, and security of data during unexpected negative events. Data may be exposed in these events, since the usual security measures may be

disabled, ignored, or not observed. Each entity needs to determine its own risk in the event of an emergency that would result in a loss of operations. A contingency plan may involve highly complex processes in one site, or simple manual processes in another. For instance, *data backups* should be stored in a secure location with controlled access. The appropriate secure location and access control will vary, based upon the security needs of the covered entity. For example, a procedure as simple as locking backup diskettes in a safe place and restricting access to the key may be suitable for one entity, whereas another may need to store backed-up information off-site in a secure computer facility. While regularly scheduled back-ups are good business practice, under the Security Rule they must also be documented and updated on a routine basis.

11.3.5 Business Associate

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. Next, the definition of a business associate and scalability are addressed.

Since the Security Rule is intended to support the *Privacy Rule*, the Security Rule incorporates organizational requirements that parallel those of the Privacy Rule. This approach minimizes the burden of complying with both Rules. The Security Rule refers to the Privacy Rule for the definition of a Business Associate. The Privacy Rule allows the covered entity to send for certain 'healthcare-serving' purposes 'protected health information' to a non-covered entity without patient authorization. However, the two entities must have a 'business associate contract' to protect the information.

The Security Rule requires, of course, different provisions in the business associate agreement from what was prepared for the Privacy Rule. The agreement is designed to confirm the business associate's commitment to provide security for EPHI. A covered entity is not in compliance with the Security Rule, if the covered entity knew of a practice of the business associate that constituted a *violation* of the business associate's obligation under the contract, unless the covered entity took reasonable steps to end the violation.

11.4 Technical Safeguards

The Security Rule has 5 standards under the heading of 'Technical Safeguards', and the majority of the implementation specifications are 'addressable' (meaning not required). The Security Rule technical specifics cover access control, audit, integrity, authentication, and transmission.

11.4.1 Access Control

Compliance with the *access control* standard means access to EPHI is only for those persons or software programs that have been granted access rights. The standard's 'implementation specifications' are

- Unique user identification (Required). Assign a unique name or number for identifying and tracking user identity.
- Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary EPHI during an emergency.
- Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
- Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt EPHI.

Each specification is explained next.

If a computer workstation is on the hospital ward and anyone who comes to the keyboard and screen can enter the system without identifying himself or herself, then unique user identification is missing. Unique user identification is typically obtained by giving each user an identifier, such as their last name, and requiring the user to login with that identifier.

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. Various forms of inactivity lockout other than automatic logoff are permissible.

The use of file encryption is an acceptable method of denying access to information in that file. The use of encryption, for the purpose of access control of data at rest, should be based upon an entity's risk analysis.

Access controls will still be necessary under emergency conditions, although they may be very different from those used in normal operational circumstances. In a situation when normal environmental systems, such as electrical power, have been severely damaged or rendered inoperative due to a natural or man-made disaster, procedures should be established beforehand to provide guidance on possible ways to gain access to needed EPHI. For example, in a doctor's office, the computer has

crashed and the doctor cannot access the laboratory values on the doctor's computer. A procedure is in place to contact the laboratory and have the values faxed or communicated verbally.

11.4.2 Audit

Audit controls entail hardware, software, or procedural mechanisms that record and examine activity in information systems that contain or use EPHI. The Security Rule points to two publications of the National Institute of Standards and Technology for further information about audit (NIST, 1996 and NIST, 2001).

In the extreme case, an entity would record each operation that is invoked along with the identity of the subject and object. For *medical records*, audit policies could be elaborate, though the Security Rule does not require it. For example, the computer system on which a patient record is maintained might

- Record the date and time of each entry to a record.
- Record the identity of each person who makes an entry.
- When an error is corrected in a patient record, the system might preserve both the original entry and the correction.
- The identity of the person making each correction and the date and time of correction might be recorded by the computer in the same manner as this information is recorded for original record entries.

The sophisticated auditing mechanisms described in the immediate foregoing are *not required* by the Security Rule. The rule does not require the entity to be able to produce an audit trail of views or changes to a specific data record within its information systems. The entity does not need, for example, to be able to identify all the users who viewed a given patient's lab results.

For further insight on the Rule's auditing requirement, one might look to the NIST standards that the Rule cites. NIST says that a system's audit trail is a collection of audit records containing data about attempted violations of the security policy or changes to the security state of the system. When required, applications should be able to generate these audit records. This notion of *auditing security violations* or changes to the security state of the system is far more limited than auditing of each user action.

Modern operating systems often have *built-in facilities* to log security relevant events. However, tools for such auditing are also available as separate packages from third parties, sometimes as freeware. If some systems do not have auditing tools, the entity might consider acquiring and using such tools for those systems.

11.4.3 Integrity

Integrity entails policies, procedures, and tools to protect EPHI from improper alteration or destruction. The integrity standard has exactly one implementation specification and that specification is addressable – the data authentication specification. *Data authentication* means that an organization can corroborate that data in its possession has not been altered or destroyed in an unauthorized manner.

The Security Rule states that very little is required to achieve integrity. Storing information on magnetic disk, which is a common way to store information on computers, is considered adequate data authentication. The Rule specifically says:

> Error-correcting memory and magnetic disc storage are examples of the *built-in data authentication mechanisms* that are ubiquitous in hardware and operating systems today.

Other examples of how data corroboration may be assured include the use of a check sum, a message authentication code, or a digital signature. The risk analysis process will address what data must be authenticated and how.

11.4.4 User Authentication

Person or entity authentication means implementing procedures to verify that a person or entity seeking access to EPHI is the one claimed. 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.

Authentication mechanisms include:

- A password system,
- A biometric identification system,
- A personal identification number (PIN), and
- Telephone callback.

The prevalent means of entity or user authentication in healthcare systems is the entry of passwords.

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.

11.4.5 Transmission

Transmission security means that when EPHI is transmitted from one point to another, it must be protected in a manner commensurate with the associated risk. The Security 'transmission security' standard has two implementation specifications:

- Integrity controls (Addressable). Security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed.
- Encryption (Addressable). A mechanism to encrypt transmitted EPHI when appropriate.

Integrity of transmission can be achieved with check sums. With a check sum, a string of transmitted digits is followed by another digit that indicates some attribute of the preceding digits. If the initial string is modified, then the check sum digit may no longer properly characterize the initial string and the transmitters can signal that a corruption in the data has occurred. Transmitting with check sums is routine in modern digital telecommunications. Another approach to data integrity in transmissions is electronic signatures.

Another type of protection of transmitted data is encryption. For the Security Rule, encryption is optional based on individual entity risk analysis. Non-judicious use of encryption can adversely affect processing times and become both financially and technically burdensome. Covered entities are encouraged, however, to consider use of encryption technology for transmitting EPHI, particularly over the Internet.

- If entity e1 sends something encrypted with method m1 to entity e2 but e2 uses method m2 to try to decrypt the message, then miscommunication occurs. Without an agreed encryption method among entities, encryption is not practical.

DHHS is committed to the principle of technology neutrality, as rapidly changing technology makes it impractical and inappropriate to name a specific technology. Specification of an algorithm or specific products would be inappropriate. No specific (or minimum) cryptographic algorithm strength is recommended. For instance, the Centers for Medicare and Medicaid Services (CMS) has an Internet Security Policy, which requires certain encryptions. However, the *CMS Internet Security Policy* is the policy of a single organization and applies only to information sent to CMS, and not between all covered entities.

11.5 Physical Safeguards

The Security Rule includes standards for physical safeguards for facility access controls, proper workstation use and physical security of workstations that access EPHI, and device and media controls.

A 'facility' is the physical premises and interior and exterior of a building. The *facilities access control standard* requires covered entities to implement policies and procedures that limit access to facilities that contain EPHI. These specifications could be very costly to implement, since they affect the *day-to-day flow* of people and information. In public buildings, provider locations, and in areas of heavy pedestrian traffic, sign-in procedures might be implemented for visitors, and escorts might be provided where appropriate. However, one should weigh the cost of such procedures against the expected benefit.

Access control to physical resources is in some way more cumbersome than access to software resources. The software is capable of semi-automating the access decisions based on data and rules. For physical access, this can be partially accomplished by providing people with identity cards that can be read by sensors at locked doors. The doors unlock, if the person has been categorized as authorized to enter the door.

The Rule requires a covered entity to implement policies and procedures specifying the proper functions and the manner in which they are performed at *workstations* that contain EPHI. The *workstation use* policies and procedures should also address the physical location and surroundings of workstations. For instance, a policy may say that only patient care staff are to access the workstations on the hospital ward.

In the extreme case, a security advocate might request that every workstation be in a locked room to which only carefully screened, authorized users have access. However, in the health care environment this is not practical. Workstation physical security may rely more on *social conventions* than on physical mechanisms. A social convention would be that staff are alert to the presence of any stranger 'behind the counter' and promptly check whether the stranger has

appropriate authorization. Success with this kind of social security is a function of training and management.

11.6 Example Implementation

The size and organizational structure of the entities that are required to implement the Security Rule 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.

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 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.

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,
- 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 or oral reminders in meetings.

The small or rural provider office would normally evaluate 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, by a consultant, or by the vendor of the practice management system as a service to its customers.

11.7 Conclusion

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 might be done in a profit-making way* (Rada, 2001).

Maintenance costs for security compliance are high. In the case of privacy compliance, the costs for one year of maintenance are a small fraction of the costs of implementation. However, for security the maintenance costs in one year are higher than the implementation costs. The reason is that security takes time of every employee – procedures like security checks at doors – but for privacy most employees do nothing in maintenance mode.

The reaction to the Security Rule was much less than the reaction to the Privacy Rule in the years 2000 to 2005. For starters, the Privacy Rule compliance deadline was two years earlier than the Security Rule deadline. Then, the health care industry realized that enforcement of the Privacy Rule was largely supportive rather than punitive and expected the same for the Security Rule. Finally, while the Privacy Rule tends to require absolutes, such as every patient must

see a Notice of Privacy Practices, the Security Rule emphasizes addressable standards for which an entity can do whatever it can reasonably argue is appropriate. However, the Security Rule provides the framework.

Part VI: Personnel and Vendors

12 Personnel

Main Points

- Patterns of health care personnel employment in the U.S. show a growth in absolute number from half a million to eight million in the past hundred years. The greatest relative growth has occurred in the allied health category, which has risen from representing 1 percent of the total health work force to representing over half.
- The health care system has a complex personnel structure that indicates the hierarchical relations between administrators and some staff but the dotted-line relation to physicians.
- Physicians have much independence but their cooperation with information systems developments is crucial to the computer-based patient record.
- Nurses are the largest segment of the health care workforce and also those most likely to routinely use computers in updating patient records.
- Medical records staff have their own professional societies and certifications.
- The Chief Information Officer directs the information systems functions of his or her health care organization and has staff for working with users and maintaining operations.

Successful information systems depend more on people than on technology. What are the roles that are filled in a health care organization? The major roles are that of nurse and physician. Within the organizational hierarchy the Chief Information Officer is particularly important to information systems.

12.1 Patterns

The last one hundred years witnessed a dramatic growth in the number and types of *personnel* employed in the health care sector. The numbers rose from about 0.5 million in 1910 to about 7.5 million in 1990. This growth outstripped the American population growth and showed an increasing ratio of health personnel to the general population (see Table “Health Personnel over Time”).

More extraordinary than the increased supply of health personnel has been the increasing number of categories of personnel. The US 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 fell 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 rose 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 in 1910 and over half the health workforce in 1990. These figures should not mask the fact that all groups have increased in absolute number from year to year (Mick and Moscovice, 1993).

The health services industry provided more than 11 million wage and salary jobs in 2000 (Labor, 2004). Almost one-half of all salaried health services jobs were in hospitals; another one-third were in either nursing and personal care facilities or offices of physicians including osteopaths.

Workers in health services tend to be older than workers in other industries. They are also more likely to remain employed in the same occupation due, in part, to the high level of education and training required for many health occupations.

Health services firms employ large numbers of workers in professional and service occupations. Together, these two occupational groups cover 75 percent of the jobs in the industry. The next largest share of jobs is in office and administrative support. Management, business, and financial operations occupations account for only 5 percent of employment (Table "Employment Statistics").

Average earnings of non-supervisory workers in health services are slightly higher than the average for all private industry, with hospital workers earning considerably more than the average, and those in nursing and personal care facilities and home healthcare services earning less. Average earnings often are higher in hospitals because the percentage of jobs requiring higher levels of education and

Table "Health Personnel over Time": categories leftmost versus years across the top

	1910	1990	2000
Employed in health sector	500,000	7,500,000	11,000,000
Total US population	93,000,000	250,000,000	280,000,000
1 health person per how many people	1 health person per 186 people	1 health person per 33 people	1 health person per 25 people

Table "Employment Statistics": Employment of wage and salary workers in health services by occupation in the year 2000. Will not add to totals due to omission of occupations with small employment. (Employment in thousands)

Occupation	Employment, 2000	
	Number	Percent
All occupations	11,065	100.0
Management, business, and financial occupations	546	4.9
Professional and related occupations	4,975	45.0
Physicians and surgeons	459	4.1
Registered nurses	1,774	16.0
Dental hygienists	142	1.3
Radiology technologists and technicians	159	1.4
Health diagnosing and treating practitioner support technicians	210	1.9
Licensed nurses	552	5.0
Medical records and health information technicians	118	1.1
Service occupations	3,275	29.6
Dental assistants	237	2.1
Home health aides	261	2.4
Nursing aides, orderlies, and attendants	1,053	9.5
Medical assistants	301	2.7
Maids and housekeeping cleaners	245	2.2
Personal and home care aides	160	1.4
Office and administrative support occupations	1,987	18.0
First-line supervisors of administrative workers	147	1.3
Billing clerks and machine operators	166	1.5
Receptionists and information clerks	288	2.6
Office clerks, general	264	2.4
Medical secretaries	280	2.5

training is greater than in other segments. Segments of the industry with lower earnings employ large numbers of part-time service workers.

As in most industries, professionals and managers working in health services typically earn more than other workers do. Earnings in individual health services occupations vary as widely as their duties, level of education and training, and amount of responsibility (Table "Hourly Wages"). Earnings vary not only by type of establishment and occupation, but also by size.

Unionization is more common in hospitals. In 2000, 14 percent of hospital workers and 10 percent of workers in nursing and personal care facilities were members of unions or covered by union contracts, compared with 14 percent of all workers in private industry.

Looking simply at *acute care hospitals* is enough to illustrate the complexity of the health care personnel situation. Hospitals are considered one of the most complex organizations in modern society. With the governing board holding legal authority and responsibility, and with the medical staff making decisions regarding patient care, administrators are delegated responsibility for day-to-day operation (see Figure "Organizational Model" at the end of this chapter). The organizational model suggests a hierarchical decomposition of responsibilities and authorities for the administration of the health care organization.

12.2 Physicians

The *physician* is traditionally the primary leader of the health care team. A physician is qualified by formal education and legal authority to practice medicine. Physicians earn high salaries and have traditionally enjoyed great independence.

Table "Hourly Wages". Median hourly earnings of the largest occupations in health services, 2000

Occupation	Health services
Halth services managers	$27.12
Dental hygienists	24.70
Registered nurses	21.56
Radiology technicians	17.25
Licensed nurses	13.96
Dental assistants	12.47
Medical assistants	11.07
Receptionists and information clerks	10.15
Nursing aides and attendants	8.83
Home health aides	8.10

An acute care organization, such as a hospital, has a medical staff that includes physicians and other qualified providers, such as dentists. The primary responsibility of the medical staff is the quality of the professional services given by members of the staff. *Medical staff* in an acute care organization are organized into officers, committees, and clinical services. Within the set of responsibilities that have to be discharged in the hospital, medical staff responsibilities include recommending staff appointments, delineating clinical privileges, continuing professional education, and maintaining a high quality of patient care. Members of the medical staff review the quality of most clinically significant functions, including, for instance, surgery, pediatrics, drug dosage, and blood usage.

Historically, physicians had little external review by non-physicians of their performance. Note in the hierarchy of the hospital that the Chief of Medical Staff reports directly to the Board of Directors rather than to the President or CEO. The physicians have always preferred this relative autonomy.

While *peer-peer review* of physicians remains the predominant mode of quality control of doctors' services, the trend is toward having physicians measured by their outcomes in a quantitative way from data collected by the provider organization. The era of *profiling* hospitals arrived in the 1980s, when the Health Care Financing Administration began paying hospitals fixed case rates for Medicare patients. Hospitals, in turn, began to study the practice habits of physicians because their orders for services for Medicare inpatients determined whether or not the hospitals profited from the care they delivered.

Hospitals profile physicians' habits for economic credentialing. Hospitals may decide that certain clinicians do not warrant admitting privileges because their practice habits adversely affect the economic performance of the hospital.

When administrators at *Providence Medical Center* in Seattle presented profiling data to the medical staff, the medical staff first rebelled and said that the data was unreliable and unacceptable. Then the physicians became aware that they might lose a substantial proportion of their patients to other providers contracting with managed care plans if their outcomes were not as favorable as those of other providers. Medical staff then asked the hospital to initiate profiling. Every member of each clinical specialty department received his or her data compared to all other physicians in the same department. The range of variation discovered for most common diagnoses was much wider than

members of staff had expected. After release of these findings, interest in development of practice guidelines appeared for the first time. After one year, a retrospective assessment of the program revealed a surprisingly large decline in average length of stay (from 5.3 days to 4.8 days). This accounted for a savings of 7,700 hospital bed days and made the hospital more attractive to health plans as a contract partner.

To correct for problems found in the profiles, *clinical practice guidelines* are appropriate. A clinical practice guideline codifies expectations for inputs, the features of treatment, and the outcomes. With guidelines and computerized information systems to identify inputs and outcomes, some surveillance of adherence to guidelines can be automated. Most health care institutions have simple clinical guidelines or protocols printed on paper for clinicians to memorize and to recall when they see a patient for whom the guideline applies.

Successful implementation of guidelines requires incentives, awareness, constant reminders, and systematic profiling of those who do and do not follow the guidelines. Achieving such conditions and trying gradually to get more and more information into digital forms that will facilitate semi-automation of *guideline adherence* is a big challenge. Yet meeting this challenge is critical to the long-term impact of health information systems. Until doctors use the information systems, the benefits of the systems will not increase much.

The realization of the importance of the physician to hospital information systems leads to the suggestion that the health care organization should have a clinician CIO who works in parallel with a technical CIO. The technical CIO would supervise and manage the organization that installs and maintains computer and communications technologies. The *clinical CIO* leads clinicians to successful data standardization, collection, and analysis for clinical quality improvement and outcomes management. The clinical CIO supervises a division of clinical informatics devoted to data collection to support profiling of physicians and clinical quality improvement exercises (Ruffin, 1999).

12.3 Nurses

Since Florence Nightingale founded modern nursing in the 19th century, *nurses* have been at the center of patient care. Nursing involves both simple tasks like administering medications and complex tasks like determining the response of a patient to treatment. The specific nurse's scope of practice varies with education, specialty, institutional policy, skill, and experience. Typically, a hospital pays a salary or an hourly wage to a nurse but pays doctors for the product of their labor. Thus, the nurse is more likely to have record-keeping tasks that are dutifully performed without fear that income will be reduced due to lack of time to produce more billable patient events.

Nursing consumes 40 percent of the typical hospital-operating budget. Nursing personnel systems track all human resource planning information necessary to manage the nursing workforce. *Personnel databases* can include information regarding every position (availability and specifications) and each individual (employment history, performance tracking, wage and salary history, professional registration, credentialing, and educational history). The staff scheduling system uses the database provided by the personnel management system and functions with the patient classification system to generate staff schedules based on specific patient care requirements (Mills and O'Keefe, 1991).

When a health information system has come from multiple vendors, the nurse is likely to be the user most confronted with the dilemma of dealing with it. The nurse is often the link between the physician, the departments, and the patient. The nurse may need to have different passwords for different systems and to learn different computer commands and interface styles.

Nurses are responsible for collecting information from patients of the following sorts (Tranbarger, 1991):

- vital signs, including temperature, pulse, blood pressure, and respirations;
- medications, including type of drug given, when, by what route, and dosage;
- intravenous fluids, including volume hung, amount infused, rate of flow, substances added, and location of access line;
- standard measures, including weight, height, intake and output, response to treatment, and laboratory values; and
- other values monitored at bedsides, including arrhythmia patterns and blood pressure.

Appropriate data elements are included in a nurse's *admission assessment* and updated at regular intervals. The information may have to be recorded in different parts of the patient record or in different online databases. This places a burden on the nurse who must identify what needs to be done, perform the function, and record the results. One function may cause the nurse to visit five different sites, look through several different forms, and then document

the same information in multiple sites. Computerization can make this process easier or harder depending on how it is done. If all information has to be entered at computer terminals in a central location but most functions are performed at the bedside, then the difference between these two locations is a problem. Handheld data entry devices and bedside terminals might help the nurse perform the data entry functions.

Estimates of time spent by professional nurses on *documentation* vary from 40 to 75 percent. This is an enormous component of the hospital budget given the number of nurses and their hourly cost. Furthermore, nurses frequently do charting after their shifts end. When nurses work after their shift, they earn overtime pay, but also the opportunities for mistake through omission increase. Information systems should help the nurse effortlessly document workflow and patient results at the point of care.

12.4 IT Staff

Administrators approve *budgets* for information systems that amount in dollars to (Ruffin, 1999):

- tens of thousands for small group practices,
- hundreds of thousands for group practices of 30 to 100 people,
- millions for single hospitals, and
- tens of millions for multi-hospital systems.

The health care organization may have various structures for dealing with information systems :

- In one extreme the entire information systems operation is outsourced and the only role in the health care organization itself for information systems is a liaison with the vendors, contractors, and consultants on hire to provide support.
- At the other extreme, the health care organization does everything itself, including developing its own unique software.

In the case where the health care organization develops, at least, a little of its own software, the organization may further have two units:

- one for operations and
- one for general user support.

The operations unit is responsible for the ongoing operation of the data processing systems. Shifts of operators keep the systems operating 24 hours a day, 7 days a week. The unit may also be responsible for the communications system of the organization. The operation's unit might include these roles:

- operations supervisor to schedule staff, maintain quality assurance, and establish directions,
- shift supervisor for the details of supervising a particular shift,
- senior and junior operators for daily work schedule implementation and troubleshooting,
- rounds technicians manage the user devices, such as terminals, printers, and telephones,
- data-entry staff for data like payroll data, and
- document control clerk to supervise data-entry staff.

A general user support unit is responsible for user coordination and support. Roles in that unit include:

- support manager oversees allocation of staff to problems and set direction,
- user support manager oversees the help desk and clinical operations,
- systems analyst evaluates application functionality required by user departments,
- programmers craft software programs based on specifications from the systems analysts,
- technical writers prepare documentation for internally developed applications,
- database managers create and maintain database software and data,
- help-line staff answer basic questions following help-line scripts, and
- trainers develop and deliver training and maintain an information technology competency inventory of the staff in the health care organization.

Further details about some job responsibilities are available from the military health system documentation. This section describes the military treatment facility (MTF) personnel's roles and responsibilities to support the Composite Health Care System (CHCS). One or more individuals may fill the roles based on the MTF's size, organization, or available skill sets at each site (DoD, 2000).

12.5 CIO

The senior information systems role is the CIO. Responsibilities, qualifications, and career paths for CIOs are diverse.

12.5.1 Responsibilities

The CIO is responsible for:

- information systems processing and development as the liaison between IS staff and senior management,
- telecommunications,
- systems maintenance and user support,

- liaising with medical records, admissions, patient accounting, and related information intensive departments of the health care organization,
- technology planning, and
- vision and strategy with senior management.

The CIO must develop an IS vision for the organization. This vision need not be obtainable in the mid-term but the organization should be able to work systematically toward it.

For a single hospital environment, the CIO may direct admissions, medical records, IS development, IS maintenance, IS operations, and IS user support (see Figure "CIO"). The CIO would report to the *chief executive officer* and have a steering committee from throughout the hospital and an IS-specific administrative staff. In a multi-corporate environment, the CIO may be responsible for IS managers at each installation as well as for centralized systems planning, development, and maintenance.

As mentioned earlier in the section on physicians, a provider organization may want to have a medical CIO and a technical or administrative CIO. The medical CIO responsibilities broadly speaking are to:

- support the development of clinical information systems that assist clinicians in the delivery of patient care and
- represent the needs and requirements of the physician community and serve as an advocate of management in promoting the use of information technology in the clinical setting.

The responsibilities in further detail from one example are listed as (Sittig,1999):

- Chairs clinical advisory groups to provide broad-based input into the design of the clinical information system.
- Leads and facilitates clinician advisory groups in the design of clinical systems to support excellence in patient care and research.
- Engages patient care providers with varying roles including physicians, nursing practitioners, nursing staff, ancillary department personnel,

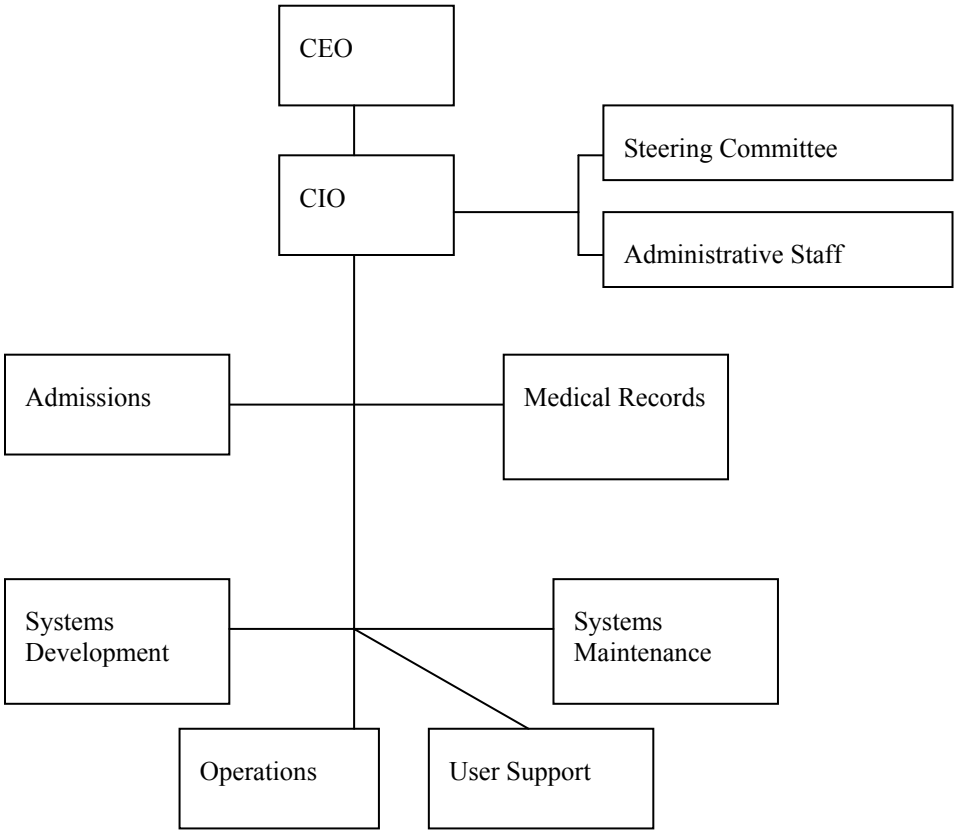


Figure "CIO": Management structure for a CIO in a single hospital environment. CEO is synonymous with President.

and medical records professionals to contribute to the development and use of the clinical information system.
- Develops empathy and understanding of physician needs and builds relationships with physicians to gain support of IT initiatives.
- Is highly responsive to users needs, including training, to assure wide spread acceptance and provider use of the clinical systems.
- Reviews medical informatics trends, experiences and approaches, develops technical and application implementation strategies and assists in the development of strategic plans for clinical information systems.
- Works in concert with Information Technology Services to design and implement systems supporting patient care and research activities.
- Leads design of clinical pathway models with physician, nursing and administrative leadership, and will assist in modification of these models to gain maximum efficacy and support for patient care and research protocols.
- Leads development of clinical 'rules' supporting patient care and protocol research as well as the design of clinical system features supporting protocol management and the use of the system to leverage the clinicians' time and maximize communication with affiliates and referring physicians.
- Designs and evaluates collection of data for clinical purposes, including tracking and interpretation of outcomes.
- Participates in clinical activities: Provides patient care in appropriate clinical setting. Reviews patient assessments and management plans. Participates in applicable clinical research. Has active medical practice in area of specialty.

The decision about who should be the *CIO* should be done with great care by a broad range of concerned individuals. By definition, the CIO will impact patient care, financial management, and administrative operations, and people from these units should all be consulted in the appointment of a CIO. The CIO should have a *background* in technical and managerial areas and should understand health care.

12.5.2 Career Paths

The CIO is responsible for managing information. This must be a collaborative effort involving both the policy setting and operational units of the organization. Three, biographical sketches of CIOs are presented next and shed insight into the requirements for the position and the type of people who fill it.

Kay Carr is the CIO at St. Luke's Hospital in the Texas Medical Center in Houston, Texas (Schriner, 1998). She was educated in finance and became a Certified Public Accountant. Her professional experiences demonstrated her managerial aptitude, and she rose through the ranks to become director of financial planning and controller. She was an outspoken critic of IT investments, and in 1995 when the hospital needed a new CIO, the CEO and CFO approached Kay. They wanted someone whose priority would be business decisions and not technical decisions. Carr brought her business experience, insider knowledge and the relationships she had developed with key stakeholders to her position. To assist her with the technical side, the hospital contracted for external technical support. Some IT staff did not want to see a CPA from the finance division become CIO and feared that IT would be overcome by finance concerns. While Carr utilizes her planning and management skill, she leaves the technical development to the technical experts. Carr says,

> Sometimes I have to put my pride on the line and say, 'I don't know what that means.'

With internal expertise and external support, Carr rapidly deployed new IT projects, including new systems for payroll, human resources, pharmacology, radiology, medical records, and a new network.

Joan Hicks is the director of health system information services for the University of Alabama Health System. Hicks began her healthcare career as a file clerk in medical records at an acute care facility (Schriner, 1998). Fourteen years later, she was medical records director with responsibilities ranging from utilization and review to medical staff services and risk management. The CEO asked her to think about taking over the CIO position. Instead of accepting the offer, Hicks decided she needed more formal training. She took a position teaching medical records skills at the University of Alabama at Birmingham. While she was a faculty member, she also earned a Master of Science in Health Informatics from the same university. After graduating, she spent two years in healthcare consulting in Atlanta before returning to Alabama to become director of medical information services for Children's Health System in Birmingham. Hicks feels that her technical knowledge is her weak suit, but she believes that technical expertise is not the most important skill for the top IT positions.

George Conklin started his career as a research psychologist and got progressively more involved in technology. He worked at New York State's Nathan Kline Institute for Psychiatric Research on database

projects to help gauge and predict the behavior of mental health patients. His work led to a job managing the clinical information systems at Columbia Presbyterian Hospital in New York. Later Conklin joined the Sisters of Charity Healthcare System as the Houston organization's first VP of information management and CIO, Conklin's philosophy is to put trust in the business managers, and win the respect of the people with whom you work. Conklin stays on top of ever-changing technology by reading IT journals and publications, meeting with vendors, and attending seminars. Conklin notes that in one job (McGee, 1998),

> I was somewhat blinded by my successes and started to appreciate less the people who worked with me and helped me achieve them. This wasn't greeted well by others, and I've reaffirmed that I can't do it myself. The successes I've had in my career are the result of a lot of people.

In addition to winning the trust of business managers, CIOs must also win the respect of the other people with whom they work.

To summarize, the three CIOs did not start with formal training in IT nor initially worked in IT. CIOs are recruited from diverse environments. Technicians tend to put less emphasis on the financial aspects. The CEO, the CFO, and the Board of Directors are asking how much a project will cost and when it is delivered because 'time is money'.

Career opportunities for those already in CIO positions are multiple (Ummel, 2003). The healthcare industry is so pluralistic that different paths exist in different situations. CIOs with business and leadership strengths may achieve new accountabilities for enterprise-wide, information-related operations like registration and scheduling, central business offices, and medical records. In entities that are undergoing mergers, as many are, the CIO has further opportunities as the critical processes of internal integration and transformation rely partly on information systems.

CIOs may grow at times not through further line responsibility but through a shift in reporting relationships. Often the CIO reports to the CFO. However, a better situation for the CIO is to report directly to the CEO or the COO. Such a realignment is promising for a CIO.

12.6 Salaries

The Health Information and Management Systems Society (HIMSS) has members in hospitals, corporate healthcare systems, clinical practice groups, vendor organizations, healthcare consulting firms, and government settings in professional levels ranging from line staff to CEOs. The 1998 HIMSS Annual Compensation Survey represented 2,200 responding members of HIMSS. The typical respondent worked in information systems at a hospital. The average salary of respondents was $60,200, while the average IT salary across the U.S. was $71,000. For the HIMSS respondents:

- Average experience in the IT industry: 11.4 years
- Average weekly hours worked: 46.3

Number of employers in last three years:

- One: 53%
- Two: 37%
- Three: 10%

Highest level of education obtained

- High school: 16%
- Associate's degree: 10%
- Bachelor's degree: 52%
- Master's degree: 21%

The following findings are an overview of each professional level surveyed in this study.

CEO/COO/CFO/Partner

- Earns $154,000 annually in total cash compensation
- Has been in current position for 10 to 14 years
- Directly supervises 6 to 10 people
- Works 54 hours per week

CIO

- Earns $125,000 annually in total cash compensation
- Has been in current position for 5 to 9 years
- Directly supervises 26 to 50 people
- Works 55 hours per week

Department Head

- Earns $81,000 annually in total cash compensation
- Received a 5% annual pay increase
- Has been in current position for 5 to 9 years
- Directly supervises 11 to 25 people
- Works 51 hours per week

Senior Staff

- Earns $70,000 annually in total cash compensation
- Has been in current position for 5 to 9 years
- Directly supervises 1 to 5 people

- Works 49 hours per week

Line Staff

- Earns $52,000 annually in total cash compensation
- Has been in current position for 2 to 4 years
- Has little, if any, supervisory responsibilities
- Works 45 hours per week

Clearly, the positions of higher managerial responsibility have higher salaries.

Healthcare, when forced to compete against other industries to retain IT employees, is often not successful because, historically, healthcare has been a relatively low-paying industry. Healthcare providers often use bonuses to try to compete more effectively with other industries for technical talent. Other industries often win a bidding war.

12.7 Medical Record Staff

The *Medical Records Department* includes several roles. For Medical Records, a Director will primarily direct the work of a clinical data manager, a record processing manager, a transcription supervisor, and a coordinator of quality control and training (see Figure "Medical Records Roles"). These roles may themselves have sub-roles. For instance, the manager of clinical data supervises coder staff and data quality staff.

Medical records administrators receive special education and certification, as do physicians, nurses, and allied health professionals. The medical records administrator has these responsibilities:

- maintaining patient information systems consistent with legal, clinical, and accreditation requirements,
- processing, compiling, maintaining, and reporting patient data, and
- abstracting and coding clinical data.

In the United States the professional society most associated with medical records administrations is the *American Health Information Management Association* (www.ahima.org) which has 40,000 members. AHIMA issues credentials in health information management. Members earn credentials through a combination of education, experience, and performance on national certification exams. AHIMA two primary certificates are:

- Registered Health Information Administrators (RHIAs) are skilled in the collection, interpretation, and analysis of patient data. Additionally, they receive the training necessary to assume managerial positions related to these functions. RHIAs interact with all levels of an

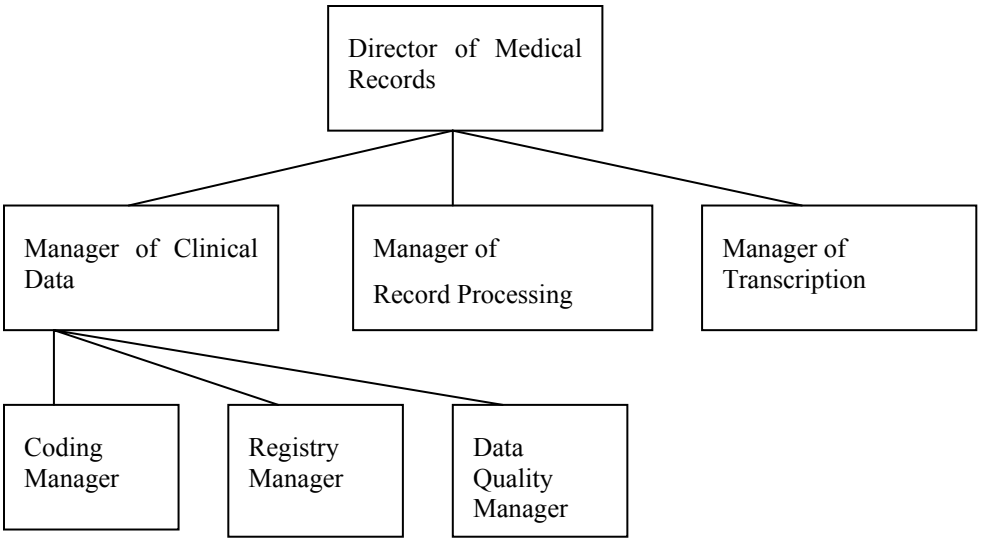


Figure "Medical Records Roles": The role hierarchy for a Medical Records Department is depicted. Underneath each of the leaf nodes are multiple line staff, such as coding staff, processing staff, and transcription staff. Additionally, some roles are omitted for simplicity's sake, such as that of trainer.

organization — clinical, financial, and administrative — that employ patient data in decision-making and everyday operations. Historically, most RHIAs have held the title of director of the health information management department of an acute care facility. As patient records evolve toward computerization and as more entities such as third-party payers require health data, RHIAs benefit from a wider selection of roles in the industry. Information security and storage, data quality assurance, and advanced assistance to consumers with their health information are among the new domains.

- Registered Health Information Technicians (RHITs) are health information technicians who ensure the quality of medical records by verifying their completeness, accuracy, and proper entry into computer systems. They may also use computer applications to assemble and analyze patient data for the purpose of improving patient care or controlling costs. RHITs often specialize in coding diagnoses and procedures in patient records for reimbursement and research. RHITs may serve as cancer registrars, compiling and maintaining data on cancer patients. The majority of RHITs are coders.

Historically, AHIMA members were basically coders. The Association encourages its members to assume aggressive professional careers and has evidence that that is happening. For instance, from 1999 to 2000 the number of AHIMA members who were compliance officers doubled; the number of information security officers has seen similar growth.

Each year, AHIMA collects professional data from its credentialed members as part of the annual membership cycle (AHIMA, 2001). The year 2001 survey includes responses from 31,000 credentialed members. About 60% had RHIT and about 40% had RHIA certificates.

One-third of the respondents report salaries exceeding $40,000. Education is a key factor in determining salary levels and job opportunities. The data illustrate a dramatic progression in salary with higher educational levels: 7 percent of members with associate's degrees earned $50,000 to $74,999, while 22 percent of members with baccalaureate degrees earned $50,000 to $74,999, and 40 percent of members with master's degrees had income in this range. About half the members have earned a baccalaureate degree or higher.

Salaries are proportional to managerial responsibility:

- Director's average salary is about $50,000 per year.
- Manager's average salary is about $42,000 per year.
- Coder average salary is about $23,000 per year.
- Consultant's average salary is about $50,000 per year.

Working in a multi-hospital or diversified network is likely to mean a higher salary than in a single hospital, mental institution, or long-term care facility.

Earnings also increase with experience in the workplace. The biggest jump into salary brackets of $50,000 or more takes place after 10 years in the workplace. Salary gains stabilize after 20 years of experience.

In the HIMSS survey, the average salary was $60,200 and this average ranged from $52,000 for a typical staff position to $116,000 for a senior management position. In the AHIMA survey, the salaries ranged from $23,000 for a coder to $50,000 for a director or consultant. Although a larger percentage of the HIMSS respondents had degrees than the AHIMA respondents (73% or the former and about 50% of the latter had Bachelors degrees or higher), this may not account for the large salary differences. AHIMA is an association that is mainly focused on medical records. HIMSS members are involved in health care applications of IT, and particularly innovative applications. IT staff in health care require higher salaries to attract and retain than medical records staff, since the IT staff have options of lucrative careers in other industries. Medical records professionals do not have the option of using their skills in a different industry in order to secure better salaries.

12.8 Questions

Reading Questions

1. How has the pattern of health personnel employment changed over the past one hundred years and what would it suggest for the patterns of the next one hundred years?
2. How is profiling affecting the physician?
3. How are the responsibilities of nurses significantly different from those for doctors?

Doing Questions

1. Consider the organizational hierarchies presented and discover information about some organization not presented, such as an ambulatory clinic, a pharmacy, or an insurance company, and indicate the personnel hierarchies that are used in that organization.

2. Physician billing is unlike lawyer billing in that lawyers charge for the hours they spend getting ready for a case, whereas doctors typically only charge for the time directly delivering care. What differences would you expect in physician involvement with health care information systems in these different situations and can you provide any evidence to support your expectations.
3. Nurses are the largest component of the health care workforce and also the portion most involved in the use of information systems. The University of Maryland at Baltimore Nursing School has one of the largest nursing informatics educational programs and many of its graduates proceed to high-level clinical information systems administrative functions in health care organizations. Some physicians think that physicians should be in the most senior position as regards directing clinical information systems. Explore what the current situation is (you could interview people, study web sites, or just speculate) and predict the changes over time.
4. Maintaining certification as a medical records administrator requires continuing education. Physicians and nurses must engage in continuing education to maintain certification. Find examples of continuing education to health care professionals that cover the topic of information systems and describe how you could develop a strategy for marketing such education online so as to take advantage of the need for re-certification through education.

Doing Question in Detail

1. The Chief Information Officer has a relatively new but a vital role in the health care system. Find on the web three descriptions of CIOs' positions in health care and summarize each briefly. You can find these from job advertisements on the web, from magazine announcements about the accomplishments of some CIOs, or other places. For each position note the organization where the CIO is employed and your source of the information.
2. Then provide another generic description of a CIO position specifically allowing you to identify by name, at least, half a dozen of the roles described in this chapter. Provide this description in list format and highlight in red each reference to a role mentioned in the chapter.

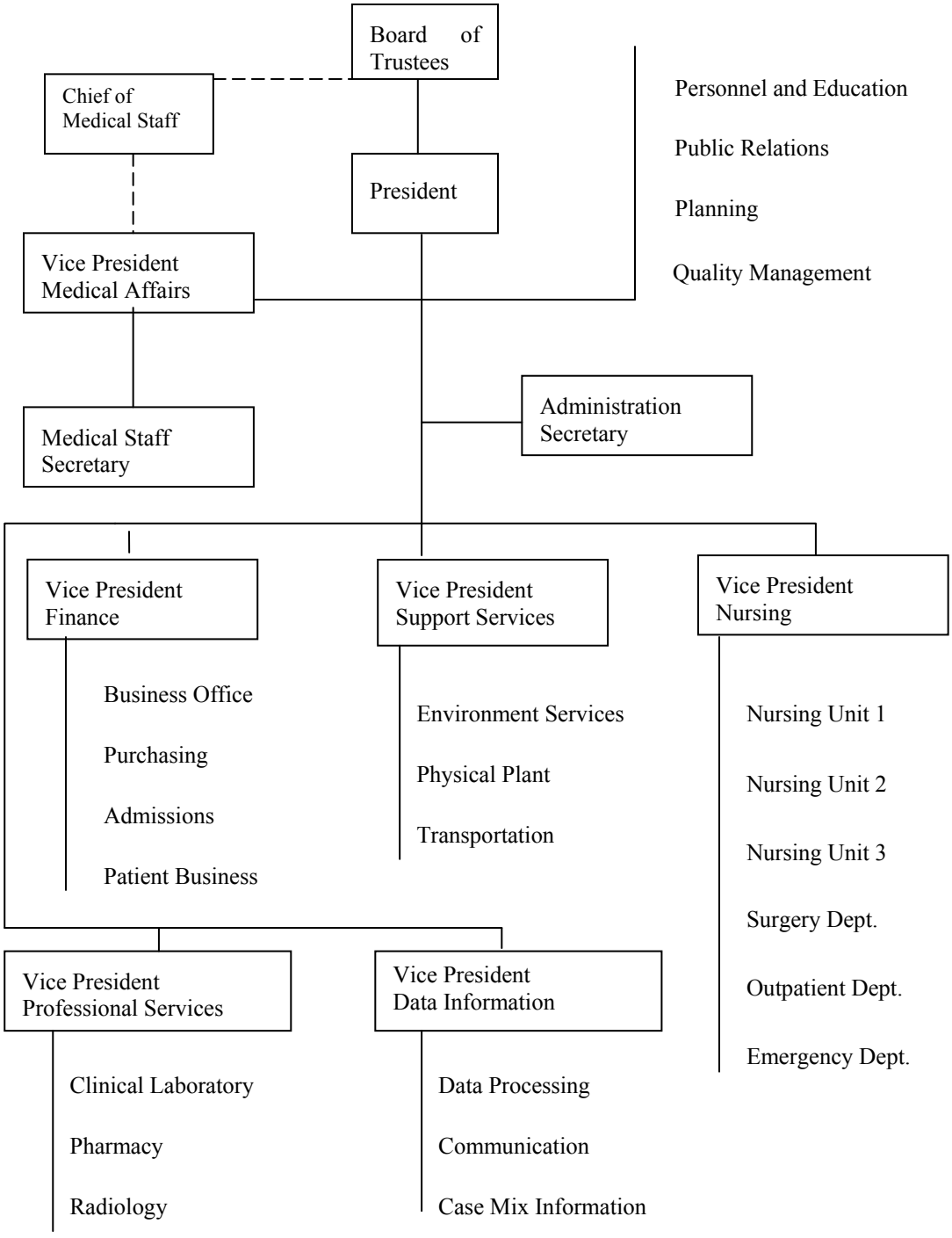


Figure "Organizational Model": This community hospital organizational chart shows the President's relation to administrative Vice-Presidents, the medical staff, and the Board (Mattingly, 1997). It omits much detail, and, for instance, does not show the Medical Records Department that might report to a vice-president or the Chief of Medical Staff.

13 Vendors


Main Points

- Consultants provide insights from other institutions to help a health care organization for special needs.
- Numerous vendors provide information system components and their web sites offer extensive information about the products.
- A typical example of a suite of offerings from a vendor shows that many of the functionalities that a health care information system could have are already available off-the-shelf from vendors.
- Contract development between large health care providers and large vendors should begin on the provider's side with a careful evaluation of competing offerings and follow with constructive negotiations designed to maximize the mutual commitment to the project.
- For vendors to small clients, the marketing approach must emphasize a one-on-one relationship and simple, fast results.

A *vendor* is any person or company that sells goods or services to someone else in the economic production chain. Parts manufacturers are vendors of parts to other manufacturers that assemble the parts into something sold to wholesalers or retailers. Retailers are vendors of products to consumers. In information technology, the term is applied to suppliers of goods and services to other companies. This chapter reviews attributes of IT vendors in health care. IT consultants who provide services to the health care industry are described and then the vendors of software and services.

13.1 IT Consultants

Cost-effective utilization of IT consultants is a skill essential to the health care Chief Information Officer. In an interview of fifteen hospital administrators about consultants, the responses were varied but all said that they paid more than planned, the engagement took longer than expected, and accomplishments fell short of what was expected (Childs, 1991). Nonetheless, 11 of the 15 were relatively happy with their consultant's work, and all 15 indicated that they would be engaging another *consultant* within the year.

Consulting is a *service industry* in the purest sense. A consulting firm's primary assets are its personnel. These assets produce revenue by providing services to clients. Individual consultants have specialized skills and proven experience, are established in their fields, and often have previously worked for a vendor, a hospital, or both.

The *services* that a typical healthcare information systems consultant offers are (Ball, 1991):

- selection and evaluation of information systems,
- contract negotiations,
- implementation support,
- long-range information systems planning,
- system testing,
- policy and procedure documentation,
- project management,
- quality assurance,
- reorganization, and
- interface support.

Healthcare institutions will request consultants for the following reasons:

- Experience: The consultant may have performed the task at other institutions or be familiar with the vendor whose solution is being installed in the institution. Thus the consultant can provide expertise that the healthcare institution is lacking (see Figure "Secrets of Health Care Consulting").
- Temporary Solution: A hospital may have need for a certain resource for a few months but no longer. In this situation of needing someone to perform a temporary job, a properly prepared consultant is more effective than a new employee who needs training but then is shortly no longer needed.
- Objective: Consultants are hired to review and evaluate organizational structures. The consultant brings objectivity and neutrality that the organization needs but may have difficulty obtaining internally.
- Reference: Consultants bring experience with systems and other hospitals that can help a hospital make a successful implementation of a new system.

- Ownership: Sometimes no one wants to finish some work that is required for some external reason. For instance, the Joint Commission on the Accreditation of Hospitals requires hospitals to have written policies. Typically staff do not want to write the policies in the form required for Accreditation, so consultants may be hired to finish the job.
- Risk: Consultants may be hired when extra help is needed to complete a job or when the job seems in danger of failing. The hiring entity may want help and also a potential scapegoat in case the job is not finished successfully.

A typical response from a young consultant as to the

Secrets of Health Care Consulting

Let me share my jaundiced view of the four rules of success for large healthcare consulting companies. This is information never put on the consulting company websites.

The first rule is charge very expensive rates. Healthcare consulting firms sell their services to hospitals and Health Maintenance Organizations (HMO) by saying that they are top healthcare experts and have experienced the problems experienced by the client, have resolved them, and will bring to the client invaluable experience. The firms charge clients anywhere from $85 per hour for a Staff Consultant to $300 per hour for a Vice President. Staff Consultants should be billable 90 to 100% of their employment time. Vice Presidents are billable 10 to 20% of the time. 80% of the Vice President's time is spent on marketing.

The second rule in consulting is selective hiring. Consulting firms hire workers that can open doors in the health care industry. If the consulting firm wants to compete in the private sector, they will pay employment agencies (head hunters) to search through existing hospitals and managed care organizations looking for IT directors, managers, and programmers who have skill sets needed for current or future projects. The firm offers the prospective candidates higher salaries and a chance (or requirement) to travel. The candidates bring knowledge and contacts into hospitals and HMO's. For the public sector, the consulting firms seek former congressmen or retired military officers. These people have connections into these markets, too. Next, to offset the high salaries being paid to the experienced executives, the consulting firms hire recent college graduates and pay them very little. Electronic Data Systems (EDS) uses this model. Basically, untrained college students are employed and sign a three year financing commitment with EDS to pay for the programmer training given to them by EDS at the EDS Training facility in Dallas, Texas.

The third rule for the big consulting companies is to compete in guaranteed win situations. For example, all of the consulting firms provide Strategic Planning, System Selections, System Implementation (Management Consulting), and Facilities Management. Exploring Strategic Planning and Systems Selection in detail illustrates how a guaranteed win occurs:

- Strategic planning has no risk. Basically, the consulting firm comes into a facility, reviews the existing software, hardware, and networking capabilities, and then creates a notebook or Power Point presentation recommending how the healthcare organization should plan for the future. This is no risk for the firm and is quick to accomplish. The firm will charge anywhere from 25,000 to 100,000 thousand dollars for this service depending on the size of the organization and number of consultants used.
- System Selections are even more profitable. System Selections are when hospitals and HMO's desire to change their existing application for a new one. The hospital or HMO contracts with a consulting firm to write the Request for Information (RFI) or Request for Proposal (RFP). Since these consulting firms have done RFI's and RFP's several times, the firm can supply the hospital or HMO with a standard set of questions that they can submit to software vendors. In other words, the hospital or HMO is paying the firm $25,000 dollars for an existing document.

The fourth and final rule for consulting success is fitting into the corporate image. Successful consulting firms require their consultants to dress in three-piece suits. CFO's of hospitals and HMO's want to see contracted labor that looks like it deserves the rates being paid.

In conclusion, consulting is a very profitable business. Firms that use the above rules make themselves very rich and very big.

Figure "Secrets of Health Care Consulting": Sam Wright shares four rules for market success in consulting.

attractiveness of these various situations follows:

- Experience: The client needs something that I have done before, and I feel comfortable and confident to do it successfully. This is the best scenario for a consultant.
- Temporary Solution: Not only might the job itself be temporary, but also the client may be inclined to treat the consultant in a lowly way in this 'temporary solution' situation. Since the consultant might put such jobs on a low priority, the consultant might ironically ask for higher pay for such work.
- Objective: The client wants the consultant because the consultant is an outsider. The consultant can expect an active working environment, and people will pay attention to the views of the consultant rather than only expect the consultant to get the job done.
- Reference: This reference situation is also good for the consultant, as the client will be interested in the consultant's view.
- Ownership: The client has difficulty finding someone to take ownership, and that's why the consultant is there. The work may be less stressful given that no one else particularly cared to do the work, and the consultant might expect an easy job.

- **Data Dictionary Analyst –** Near New York City, client looking for specialist to develop, test, implement and monitor data dictionaries. Wants understanding of ASTM, HL7, LOINC and or ANSI standards. ADT, billing, scheduling and clinical systems experience is a plus. Proficiency with current tools for multi-tiered database development tools.
- **Security Specialists –** Requires knowledge of systems security, platforms, operating systems and networks. Moderate to high travel. HIPAA a plus. Location varies depending on experience.
- **IT Security Officer** needed in the South. HIPAA required. No travel.
- **Senior Sales Support Representative.** Client wants experienced presentations/sales specialist. Competitive comp plan. Stable environment.
- **Contracts Manager –** East Coast location, consultant function. Responsible for the development and administration of IT/Telecommunications capital agreements. Aid provider clients with advice/direction on acquisition of major systems purchases.
- **HR System Specialists** in Minneapolis, Atlanta, Dallas, Los Angeles and Boston. Position requires knowledge of HR functions and use of a major Human Resources package**.**
- **Interim CIOs.** High travel, usually involves temporary living arrangements. Ability to sell additional services a plus. High travel. Can be located anywhere.
- **Product Manager – Benchmarking Systems.** Low travel, great location on the East Coast.
- **Two Senior PACS Consultants.** Preferably located on East Coast or willing to locate there. Responsibilities involve systems selection and strategic planning. Client wants one to be more marketing oriented.
- **Transition Management Consultant –** Provide senior-level industry expertise to Hospital Management team. Develop transition strategies. Organizational development, strategic planning, outsourcing strategy, etc.
- **RNs** needed to hold dual roles in support and installations in Massachusetts and Texas. Also, an RN in Boston in an inside sales capacity. Low travel. Also, nurses with oncology experience needed in Phoenix, southern California, Atlanta, Boston and Connecticut.
- **Consulting Specialists - Systems Selections.** Help hospitals make critical decisions. Management-level position a possibility. Location depends on abilities. Moderate travel.
- **East Coast – Web Systems Project Manager.** 60% travel. Must have experience creating and implementing websites and /or web-based systems, as well as working with client management. Great organization. Very people-oriented.
- **Senior Palm Developer** needed in the **Northwest.** Small organization passing the breakeven point. Code Warrior required.
- **RN with oncology** experience needed. Fairly high travel implementing new systems. Northwest, systems development opening.

Figure "Sample IT Consultant Openings": This list of job availabilities comes from a recruiter of IT consultants in healthcare.

- Risk: The consultant is on the job because of the risk to fail. The consultant has an opportunity to show his capability but must be careful to not fail himself, even if the work may fail. Client staff may hesitate to help for fear of being associated with a likely failed effort. This is the worst situation for the consultant.

The preceding are not the unanimous views but typical ones. For the ownership situation, a different perspective is provided in the following scenario (Haidar, 2002):

> Suppose an organization hires you to write their policies and procedures. The medical staff told the administrators they are too busy to bother with this task. They want nothing to do with it, even when you ask them to review what you have written. You finish the task, without much input from the medical staff, and deliver the policy manual to the hospital administrator. Six months later, a suit is filed against the hospital because a doctor injured a patient. An investigation reveals that while the doctor performed the procedures in a similar manner to most of the doctors in that institution, he did not follow the written policy and procedures of the organization—a policy you wrote. The policy you wrote was based on what you thought the procedure should be rather than what was actually being done. You explain to the lawyers and hospital administrator that you asked the medical staff to review that particular policy, but they never did. What impact do you think this might have on your reputation as a consultant? Obviously, my point here is that the people who hired you may not care what result you get, unless something goes wrong. The darker, more troubling side of no one in the organization wanting to do a task is that they may be uninterested in or even resistant to your efforts. If you do not have adequate support for doing a task no one else wants to do, the risk of failure is significant.

The healthcare entity will have a contract with the consultant. The entity will want precise *contract arrangements* that include precise deliverables at fixed times. There should be no learning curve to get immediate results from the consultants. The contract might stipulate precisely who will do the consulting work and not permit substitutes. If the consultants are local, then they might be required to work on site.

A wide range of positions tends to be available for IT consultants in health care (see Figure "Sample IT Consultant Openings"). A national recruiter might be looking for experts in healthcare systems consulting, installation, development and sales. The companies doing the hiring would typically pay all fees.

There are many shapes and sizes of consulting company. According to the Gartner Group, the top three companies in the US by *gross revenue* for health information systems consulting are (with their dollars earned in healthcare consulting in one year and their web address):

- Cap Gemini Ernst & Young with $600 million,
- SAIC with $435 million, and
- CSC Healthcare with $380 million.

For these three, health care represents less than half of the company's total consulting revenue. However, numerous firms also do only health care consulting. For example, First Consulting Group

Company Name	Revenue in $ Millions	% health IT revenue	year founded	web address
Agilent	1,400	100	1999	www.agilent.com
EDS	1,346	7	1962	www.eds.com
McKessonHBOC	1,088	3	1833	www.mckessonhboc.com
GE Medical	1,000	100	2000	www.gemedicalsystems.com
CSC	523	6	1959	www.csc.com
ASC	435	20	1988	www.acs-inc.com
Cerner	405	100	1979	www.cerner.com
Ingenix	375	100	1997	www.ingenix.com
Medquist	364	100	1970	www.medquist.com
IDX Systems	342	100	1969	www.idx.com

Table "Top Ten": Companies have been ranked by revenue from software and associated services for healthcare (Le, 2001). Companies that did not share their revenue figures were not eligible for inclusion in the listing of companies.

(www.fcgnet.com) is a provider of information-based consulting, integration, and management services to healthcare.

13.2 Vendor Characteristics

Most hospital computer systems, which were initially introduced to solve problems such as accounting and billing, are obsolete. As various departments added their own systems for admissions, radiology, laboratory, emergency room and pharmacy services, they created an electronic Tower of Babel, with none of the systems capable of speaking to one another. The solutions range from starting from scratch with a single supplier to upgrading the legacy software.

Hospital clinical information systems tend to be purchased from a single vendor (Gardner, 1989). Two-thirds of about 1,700 hospitals reported using a single vendor for the clinical information system. However, only one-third of hospitals used the same vendor to both automate finance and clinical functions.

Single vendor systems tend to limit choice when more than one automated function is desired. Systems may have good order entry, while offering only mediocre reporting functions. One way to get the best *components* is to purchase from different vendors and insist on the components being adequately connected on the computer network (Tranbarger, 1991).

Revenues for vendors of hospital information systems were $7 billion in 2003. Market participants in the industry range greatly in size from small systems integrators to well-established firms with billions of dollars per year in revenues (see Table "Top Ten"). Large enterprise software companies, including Oracle, SAP, and PeopleSoft, are in the health care market. Manufacturers, such as General Electric and Siemens, also have significant health care information systems components. A handful of specialists in medical-information management systems are also competing, such as Cerner and IDX Systems. No one company has more than a sliver of this highly fragmented business. Based on 2000 revenues, Siemens had the largest market share, with 4.9%, followed by McKesson, with 4.8% and Cerner with 2.1%. McKesson has the largest installed base, but the market share of the six biggest players amounts to only 16%.

13.3 Sample Components

Cerner, Shared Medical Systems, IDX Systems Corporation, and Eclipsys Corporation have similar product lines, target audiences, client base, and corporate characteristics. Each offers a suite of products that compete with one another's. A generalized, fictional description of one such company (call the company Health Information Systems Limited or HISL) follows:

> HISL commits significant resources to developing new health information system products. One thousand employees were engaged full-time in product development activities. Expenditure for the development and enhancement of the Company's products is approximately $80 million per year each of the past 3 years.

A detailed description of the product line of HISL follows.

HISL's Enterprise System automates processes across the entire health system:

- The 'Registrar' module automates the identification, eligibility, registration and scheduling processes across provider organizations. It includes a structured repository for the storage and viewing of health plan information, records, contracts, eligibility and coverage data.
- The 'Community Physician' module connects community-based physicians to health systems for referrals, authorizations, claims, eligibility, and reporting.
- 'Clinician Chart' is the enterprise clinician's desktop solution for viewing, ordering and documenting the electronic medical record, which is maintained in the 'Central Data Repository'. 'eClinician Chart' extends the power of this viewer to the web. Physicians can gain access to the electronic medical record to view results and documentation from any Internet-based terminal. It includes a structured repository for the storage of patient orders; discrete results; clinical reports and other documents; indexes to document images from foreign document imaging systems; and indexes to third-party dictation systems.
- The 'Central Data Repository' is a structured repository for process- and activity-related information useful for management of a healthcare organization. Information can originate from numerous sources and can be maintained in an easily accessible, standardized format. The 'Repository' can be integrated into an architecture containing products from different suppliers.

HISL's clinical systems for direct care include the *Acute Care Management System*. This system

automates the entire care process in acute or institutional settings. It collects, refines, organizes, and evaluates detailed clinical and management data. It enables the entire care team to plan and manage individual activities and plans, as well as measure outcomes and goals. The 'Acute Care Management System' consists of two major solutions:

- one automates documentation related to acute care delivery at the point of care, including nursing order entry and viewing of the patient's medical record, as well as basic registration capabilities; and
- another supports acute care planning, including pathways used to audit care, nursing care plans, and multidisciplinary pathways.

The 'Intensive Care Management System' automates the entire care process in intensive care settings.

The *Physician Office Management System* supports the broad range of clinical and business activities that occur within a physician office and ties the office together with others in the community. It automates key activities of the care team in both primary and specialty care settings. It offers staff a variety of functional capabilities, including patient tracking, clinical records access, eligibility checking, order and referral processing, and reference library access.

HISL's *Home Care Management System* automates the clinical and business processes of home health organizations, such as visiting nurse associations and hospices. It is appropriate for Medicare-certified or noncertified agencies providing skilled nursing, specialized care, supervisory activities, assessments, and unskilled attendant or medical delivery services. It facilitates the documentation of care activities in the home and provides access to the electronic medical record.

The HISL *Laboratory Information System* addresses the information management needs of four clinical areas: general laboratory, microbiology, blood bank services, and anatomic pathology. It automates the ordering and reporting of procedures, the production of accurate and timely reports, and the maintenance of accessible clinical records. To facilitate electronic ordering by community physicians and to allow the rapid dissemination of lab results, HISL also provides a web-based application for both order and results.

The HISL *Radiology Information System* addresses the operational and management requirements of diagnostic radiology departments or services. It allows a department to replace its manual, paper-based system of record keeping with an efficient computer-based system. Specific modules on mammography, film tracking, and inventory management are also offered, as is the capability to display and route medical images in a viewer. Complex interfaces to major PACS (Pictorial Archive Retrieval Systems) are also offered to integrate the radiology information system to the PACS.

The HISL *Pharmacy Information System* supports pharmacy order entry and support of the clinical pharmacy in either an inpatient or outpatient setting. It streamlines medication order entry, enabling the pharmacist or technician to place all types of pharmaceutical orders on one screen. Dispensing functions, including interfaces to automated dispensing devices also are supported. Medication fill lists, intravenous fill lists and medication administration records are produced automatically or on demand.

The HISL *Surgery Information System* addresses the needs of the surgical department, including automating the functions of resource and equipment scheduling, inventory management, anesthesia management and operating room management. Case cart management, preference cards, and peri-operative documentation are attributes of the system. The HISL Emergency Medicine Information System provides basic emergency department functionality, including quick admits, tracking, triage, and patient history, as well as a graphical reference to patient location and order status.

Within the area of decision support systems, HISL *Expert System* is an event-driven, rule-based, decision support software application that allows users to define clinical and management rules that apply to data that is captured by other HISL applications. HISL's comparative data warehouse for benchmarking information and services for subscribers supports their own improvement processes. Data is provided from client's information systems as well as national and regional data sets. The warehouse is hosted at HISL's World Headquarters and accessed via the web.

The *Financial and Operational Management System* is HISL's system for revenue accounting, billing and accounts receivables for the entire health system as well as each individual domain or organization. The Agreement Management System automates the managed care processes around membership, eligibility tracking, claims processing and contract management. The Enterprise Management System uses the Central Data Repository to help an organization complete its strategic plans, including clinical metrics, case profiling, and performance profiling of individuals and organizations. The Health Information Management System helps meet the

operations management needs of the medical records department and includes functionality for the various chart tracking and completion tasks commonly associated with maintaining medical records. The Materials Management System automates the business operations around supply chain management.

HISL's *Demand Management System* includes applications and services to automate and manage the operations of a call center, including protocol-based triage, referral management, and person information. The Call Center Management System enables call centers to automate the telecare function for providers, as well as health plans or disease management companies.

HISL's *Internet-based Home Software* extends medical care to the consumer's home. It provides a way for the consumer to interact on a regular basis with a healthcare provider. By providing health appraisals and personalized health plans, it takes the first step toward improving health education for members in a community. Relevant health information can be shared among providers and the patient under control of the patient.

One can see that HISL offers a large suite of complex software tailored to the healthcare provider market. Several other companies have similar product suites. For both the vendor and the healthcare provider, the challenge is to find the right match.

13.4 Large Client

The relationship that a healthcare institution has with a software vendor can significantly impact the implementation of applications. The probability of success is increased if those people involved assume the responsibility for creating a positive business relationship (Kock, 1991). Historically, business relationships have been formed between the vendor and the *purchasing department* or the information systems department, but this relationship must be broadened.

The purchase of a Healthcare Information System (HIS) is a complex undertaking. The first task is to obtain all the required, organizational approvals. The second task is to determine and manage a reasonable process timeline. The timeline will indicate five phases (Fox et al, 2001):

1. the window-shopping phase,
2. the planning phase,
3. the acquisition phase,
4. the installation phase, and
5. the operations phase.

Given that project personnel turnover is frequent and project expectations constantly change, the timeline must be flexible.

13.4.1 Evaluations

HIS *vendor evaluations* are most noticeable during the acquisition phase. However, evaluations should occur during each phase. The evaluations require top expertise and affect quality control. Unfortunately, the cost of the required expertise over time is rarely included in a healthcare organization's IT budget.

In general, a useful analogy for the management of a healthcare IT project, including the projects' required evaluations of HIS vendors, is the management of an organization's building projects. Many healthcare organizations retain legal, architectural, construction, and maintenance firms throughout building projects to maximize the value from the projects' massive investments. IT investments are equally complex and massive, requiring comparable expertise throughout. HIS vendor evaluations should include a careful analysis of a limited number of pre-selected vendors. The analysis should be based on a series of 'face-to-face' vendor meetings. These meetings should include follow-up documentation to be used as addenda to the contract; on-site, hands-on system demonstrations with scripts; off-site, telephone, and email vendor reference checks; and, evidence of software 'walk-throughs'.

13.4.2 Contract Negotiations

After completion of the comprehensive vendor evaluation and selection of finalists, the organization is ready to proceed to the next phase, where the focus is on *contract negotiations*. Many companies make the mistake of advising a vendor that it has been selected as the winner of the 'request for proposal' contest, and all that remains is to enter into a contract. By doing so, the purchaser has seriously undermined its bargaining position, since the vendor now knows that no one else is in the running. It is much more effective to select the top two vendors, then advise the preferred vendor that if negotiations break down or do not go as well as expected, the second choice is waiting in the wings.

Similarly, the healthcare entity need not disclose to the vendor the amount of money budgeted for the project. Often when this is done, the *contract price* will come in close to the budget price. Despite trying to negotiate low cost and high service, the healthcare entity must take care to maintain a positive relationship. Unlike other contract negotiations, when purchasing a complex and expensive healthcare information system, the purchaser and vendor will have to work together for an extended period of time.

If the negotiations have been too mean spirited, there may be at least two unpleasant outcomes:

- in the future, when the purchaser needs something from the vendor which is not covered by the contract, the vendor may impose a high charge in an attempt to make up for perceived losses at the outset; or
- the purchaser has squeezed so much out of the initial pricing of the contract that the vendor's business ultimately fails.

The *Definitions* section of the contract should cover terms like programs, software, system, hardware, third-party software, source code, installation, acceptance, documentation, and permitted users. How these terms are defined may well make the difference between a successful project and a failure. For instance, if the 'documentation' does not include the vendor's response to the RFP and a listing of functional and performance specifications, a warranty that "the system will operate in accordance with the documentation" will not be very helpful. Also, it is essential to determine the correct type of license for the organization's particular use. For example, there are:

- site licenses, covering a specific geographical location;
- enterprise-wide licenses, encompassing an entire business or institution; and
- licenses governing the right to use software on a subscription-type basis.

Each of these and other types of licenses has its unique issues.

In reference to *payment terms*, objectively measurable performance milestones are best. These milestones should be coordinated with detailed acceptance testing criteria. For example,

- 10% of the contract price will be paid upon execution,
- 20% upon delivery,
- 30% upon completion of installation, and
- 40% upon final acceptance.

The entire acceptance testing procedure should be detailed, including testing procedures and protocols, re-tests, and options if the tests are not successful.

Another significant contractual issue concerns access to the *source code*. Without it, the software cannot be adequately maintained. The issue may arise in the context of the vendor's bankruptcy, but is equally applicable if the vendor simply ceases to support the software. The purchaser wants access to the source code. This may be accomplished through a source code escrow arrangement or direct licensing of the code.

The inclusion of contract provisions for alternative dispute resolution may help avoid expensive litigation. An *Escalation Provision* defines the specific hierarchy of employees who are to be involved in resolving any problems that arise. If first level managers are unable to successfully reach an agreement, the problem is escalated to the next level of management within a specified amount of time. If this informal process is unsuccessful, the contract may require binding arbitration, which offers advantages over a court battle.

13.4.3 WellSpan Health System

WellSpan Health System serves the healthcare needs of more than 500,000 people in Pennsylvania. WellSpan has developed specific guidelines for business analysis, RFP development, the vendor selection process, contract negotiations, and system implementation.

Wellspan and the vendor assume responsibilities as follows:

- WellSpan's responsibilities in the client-vendor partnership are to provide the designated resources to support the implementation plan, complete acceptance testing on-schedule, notify the vendor in a timely manner of problems, serve as a positive reference if appropriate, attend executive and user conferences, provide constructive feedback and notify vendor of changes in WellSpan's business objectives.
- The vendor responsibilities in the partnership include: client agent for 'Best of Breed' services, being a partner across the continuum of change, help WellSpan to achieve competitive advantage, deliver business results, benefit the client organization, patients and community, provide a flexible approach to partnering and maintain strategic alliances with suppliers and competitors.

An integral part of any client-vendor relationship is a sound contract. At WellSpan, a sound contract establishes a 'win-win' for both parties.

13.4.4 Parkview Memorial Hospital

Parkview Memorial Hospital in Fort Wayne, Indiana has 600 beds. In 1986 the hospital decided to pursue the acquisition of an integrated hospital information system. A selection team was formed of the patient care system coordinator, the director of information systems, the vice president of finance, and a representative of nursing administration. Selection criteria were developed, and two vendors were

identified as most suitable. Phone interviews and then site visits to other hospitals that had implemented the systems of the vendors were performed. During the product demonstrations and many meetings clarifying what the product would do, the business relationship continued to develop.

Following the selection of a system, the hospital and the vendor entered into a series of meetings to negotiate various terms of the contract. After a yearlong selection and negotiation process, Parkview Memorial purchased its total information system. The next step was implementation and that also involved extensive involvement from various hospital departments and the vendor over many months.

The relationship between vendors of health information systems and providers of health care is important to the successful implementation of a health information system. As health care systems become more complex and more dependent on information systems, the need for close fits between an organization's information system and every action taken within that organization increases. The differences in the actual functioning of the software provided by one vendor or another may be only one of many factors that enter into the determination of whether or not a vendor and a provider will work together successfully.

13.5 Small Client

When a vendor tries to sell a large product to a large healthcare entity, the stakes are high, the proposal tends to be detailed, and negotiations involve large teams from both the vendor and the provider. When a vendor tries to sell a small product to a small healthcare entity, the stakes are low, the proposal tends to be short, and negotiations involve a few one-on-one interactions. The client does not want to spend much time in the product review and wants clear results immediately demonstrated.

A successful vendor in this small client environment will promise to show immediate results and to take almost no time. A true story follows from a vendor representative:

> It was interesting to market practice management to dentists. My approach was to walk into an office cold and talk to the receptionists. I would stay no longer than 5 minutes and just ask general questions to see if they were using computers and if so for what. Usually they were doing letters and other things in word processing. Some were doing general accounting in something like Peachtree (www.peachtree.com). This was in the late 1980s.
>
> The next day I would send a letter to the receptionist thanking her for her time and asking if she thought the office manager would grant me a 15 minute appointment. The only question I wanted the office manager to answer for me was "If there was one problem you would like me to solve for you, then what would it be?"
>
> I usually got the appointment. When I found out what their worst problem was I had my direction.
>
> Then I would send another thank you letter to the office manager which in dental offices was frequently the dentist's wife. In that letter I would indicate that perhaps I could help solve their problem and would they like for me to do a free analysis of their workflow to see if a computerized program would help solve the problem and save them money.
>
> Again I seldom failed to get that meeting. But I would not grant that meeting unless the dentist signed-on at this point. The analysis was free, but I would not conduct it unless the dentist agreed that if I could show them how I could solve the problem for them and save them money, they would purchase the system from me.
>
> At this point I got about a 50% positive. Sometimes when I did the analysis, I found it was management problems that were causing the problem and no computer was going to solve it. In that case I would terminate the analysis and report the problem as I saw it.
>
> But of the ones for which I completed the analysis and made a recommendation, 90% ended in a sale.
>
> We marketed a comprehensive modular system. The system saved the doctors money through EDI of claims and prompt payments. If the patient did not have dental insurance, then the dentist switched to presentation of the bill to the patient at the time of service and found that 80% of the patients paid during the visit. The cash flow improvements paid for the system.
>
> We programmed the forms reports for each dental insurance company and the doctors paid us by the hour. We had one guy who

had been a dentist, and he understood the workings in the dental office so he did the forms. That was lucrative 'after-sales' money for our forms work.

The vendor representative has followed these steps:

- a 5-minute visit to learn the terrain,
- a 15-minute appointment to identify a problem, and
- a free analysis for the solution to the problem.

The free analysis is done under the condition that the dentist agrees to buy the vendor solution should the vendor representative convince the dentist of its cost-effectiveness. While 50% of the contacts are lost at this stage, the sales effort will not succeed until the decision-maker at the client (in the dentist office case the decision-maker is the dentist) supports the purchase. The term vendor representative is used rather than salesperson because this person has served not only the role of salesperson but also the role of business analyst.

In the role of business analyst the vendor representative has been honest enough to note when a problem requires a solution that the software product does not support. For instance, the problem may be that the office intentionally does not respond to queries from the health insurance company for additional information on claims, and thus the insurance company does not pay the claims. The work process, as in responding to insurance queries, must be in the right direction before the software can help the work process be executed efficiently. The vendor finds that a good relationship with a customer can lead to further business. Thus, being able to correctly solve the problem is important.

13.6 Questions

Reading Questions

1. List some of the largest companies by revenue from healthcare IT services.
2. An extensive example of a fictional vendor's health information systems portfolio is presented (the vendor is called HISL). What functionalities described as important for all four top-level components of a health information system are covered by HISL's offerings?
3. List some key components of the contract negotiation process between a provider and a vendor.

Doing Questions in Brief

1. Explore what different vendors offer by way of clinical support department systems, such as radiology and pharmacy, and analyze the extent to which messages from one department to another are supported.
2. Draft a contract to be signed between a provider and an IT vendor.
3. Information systems consultants are needed by health care organizations for various reasons. Consider your own strengths and weaknesses as a potential consultant and describe what strengths you would emphasize in trying to successfully find a niche for yourself in the health information systems consulting business.
4. Identify a vendor of a healthcare information system and summarize the characteristics of the information system that the vendor provides. Distinguish the vendor's products that you describe relative to the other competing products on the market.
5. Compare and contrast what SAIC and CSC do for health care with IT.

Doing Question in Detail

The objective of this exercise is to learn about positions available in the industry and to use that also as a way to gain further insight about the employers. Choose 3 companies in the healthcare IT arena. Go to the web sites of the companies and search for the jobs available. Describe

- how easy or difficult was the work of finding relevant jobs on the web,
- how many positions with the keyword 'health' are available,
- what is the pattern of available positions in the 'health' area in each company and across companies,
- what is the geographical distribution of positions,
- what are the fringe benefits of employment.

Comment on the companies in terms of their market.

Part VII: Knowledge & Diffusion

14 Knowledge


Learning Objectives

- Identify key standards in the health care information systems arena and indicate how they support interoperability
- Delineate the pros and cons of various representation and reasoning schemes for medical knowledge -- flow charts, databases, decision theory, and rule-based expert systems.
- Demonstrate how data warehousing applications improve a wide range of health care industry activities.
- Construct a situation under which a decision-support system is likely to succeed in practice.
- Differentiate vision and robotic systems from medical diagnosis systems.
- Use effectively a medical literature retrieval system.

Coordination is the top event in a hierarchy that proceeds from

- a common language,
- to communication,
- to decision-making, and
- to coordination.

The common language is a standard for communicating.

14.1 Standards

Before a project can progress, it must choose a common language. For person-to-person conversation, the language might be English. For messages between computers, the choice is less obvious. Common languages for computer-computer communication derive from standardization efforts.

14.1.1 Definition

A standard is defined as

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

Standards arise either from official standards activity or arise by the force of practice. An official standard is a de jure standard, while those that 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 that 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).

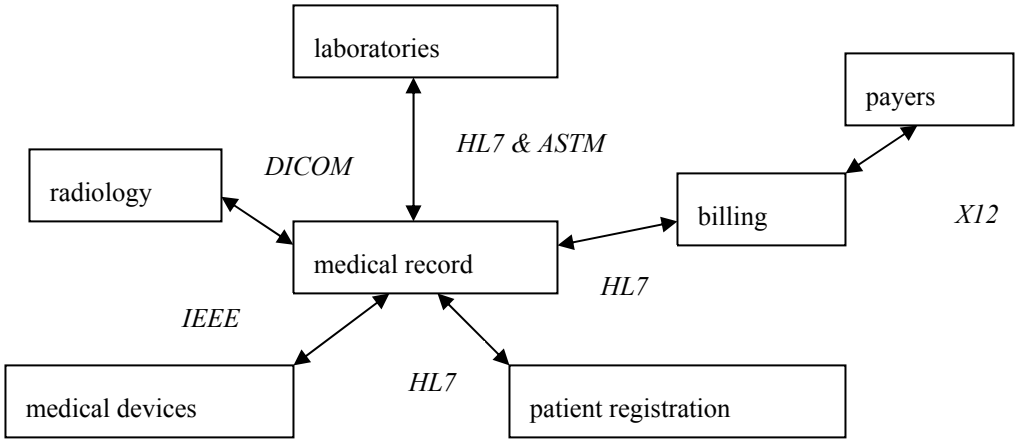


Figure "Messages": Medical record in center connected to other activities via messaging. The square boxes are the activities. The arrows indicate the flow of messages. The italicized term refers to the standard organization that has a standard relevant to that message or transaction.

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 HIPAA Transaction Rule is powerful because the government has mandated that healthcare organizations comply with the standards indicated in the Rule.

14.1.2 Standards Organizations

The principal stakeholders with active involvement in standards are:

- Providers and Payers: Providers and payers communicate healthcare data.
- Government: The federal and state governments are large payers and — in some cases — providers of healthcare. The federal government frames national healthcare policy, regulates the industry, and sets standards, as in the case of HIPAA. States also regulate and license providers and payers.
- Standards Development Organizations: These are defined later in this section.
- Vendors: Most healthcare organizations purchase their software from healthcare information systems vendors. Thus interoperability standards depend on support from the vendor community. Interoperability standards and how they work in the information value chain are critical business issues for vendors. Generally, hospital information systems vendors claim HL7 compatibility, and imaging vendors support DICOM standards.

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. Health Level 7 (HL7) is the primary standards development organization for standards for system interfacing within provider organizations. Like HL7 in the clinical domain, ASC X12N is the acknowledged leader in the healthcare financial domain.

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.

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.

14.1.3 Interoperability

High quality health care depends on comprehensive patient medical record information. While health care has adopted information technology for financial and administrative systems, it has made limited progress in utilizing information technology to support patient care. One impediment to the adoption of information technology is the lack of comprehensive *standards* for patient medical record information.

The U.S. *National Committee on Vital and Health Statistics* concluded that an adequate computerized patient record requires that clinically specific data are captured once at the point of care and that all other legitimate data needs are derived from those data. This requires *interoperability*.

Interoperability is the ability of one computer system to exchange data with another computer system. Today, health care employs many different information systems, both within an organization and across organizations. For example, a hospital may have a laboratory system from one vendor, a pharmacy system from another vendor, and a patient care documentation system from a third vendor. Physicians affiliated with the hospital also have different systems in their offices, yet need access to data from the hospital on their patients. To achieve coordination among the components of the health care system, the components must first share a *common vocabulary* and then communicate to make decisions.

To achieve interoperability between different information systems, the healthcare delivery system has message format standards. These standards have a high degree of optionality to accommodate the variability of workflow and availability of information in different care settings. This optionality creates the need for costly and time-consuming customization when implementing message format standards. In addition, vendors and providers have developed their own implementation guides that differ from the standards. Finally, there is little or no conformance testing of message format standards. *Non-standard implementations* result in the need for costly and time-consuming customization to allow information systems to seamlessly exchange data with one another. These customized solutions contribute to high cost of systems. Such high cost, in turn, restricts the broadest possible adoption of information systems by providers. If, by accelerating uniform message format standards development and implementation, the cost of these healthcare information systems can be lowered, their market acceptance would increase. This would contribute directly to improved quality of care, improved provider productivity, and reduced healthcare costs.

Lack of comparable data can directly impact patient care. A simple example is the use by physical therapists of a pain scale that ranges from 1 to 4, and another used by nurses that ranges from 1 to 10. Obviously, pain designated at 'level 3' carries vastly different meanings to these professionals. *Comparability* requires that the meaning of data is consistent when shared among different parties. Standard healthcare vocabularies would assure that data shared across systems are comparable at the most detailed level. Information system vendors and healthcare providers who wish to use detailed vocabularies, have had to create their own proprietary set of terms that are not comparable with other vocabularies, or have had to choose from one of several commercially-available vocabularies that do not necessarily cover all clinical areas. Without national standard vocabularies, precise clinical data collection and accurate interpretation of such data is difficult to achieve. Further, this lack of standard vocabularies makes it difficult to study best practices and develop clinical decision support.

14.2 Knowledge-based Systems

In the 1960s and early 1970s, the emphasis in hospital information systems was on operational control – active monitoring of routine task performance, with emphasis on doing highly structured tasks better, faster, and cheaper. This *operational control* has been extensively achieved with systems such as patient accounting and medical records. The next era of application, which followed in the late 1970s and early 1980s, shifted attention toward functional effectiveness in the form of management control (Tan, 2000). This contributes to the achievement of managerial goals beyond those of efficient task performance. In practice, this is often accomplished by data aggregation, analysis, interpretation, and presentation.

14.2.1 Background

The diffusion of computer support in the late 1980s and early 1990s led to new levels of automated assistance for health professionals and managers. These computing applications empower end-users through support of expert methods in patient care and health service management. Intelligent applications can transfer knowledge and expertise to the end-user.

Intelligent systems in health care are best developed by thoroughly understanding the human decision-making and knowledge manipulating processes. This kind of study can result in new knowledge-based tools for practitioners but also may result in new insights about health care practice. Schwartz (1970) speaks of

> the possibility that the computer as an intellectual tool can reshape the present system of health care, fundamentally alter the role of the physician, and profoundly change the nature of medical manpower recruitment and medical education .... The key technical developments leading to this reshaping will almost certainly involve exploitation of the computer as an 'intellectual,' 'deductive' instrument--a consultant that is built into the very structure of the medical-care system and that augments or replaces many traditional activities of the physician.

Historically, the three main approaches to this 'intelligent' type of medical computing were:

- the clinical algorithm or flowchart,
- applications of decision theory, and
- the matching of cases to large data bases of previous cases.

A *flowchart* is conceptually the simplest decision making tool. It might encode the sequences of actions a good clinician would perform for some population of patients. For example, one could record all sequences of questions asked, answers given, procedures performed, laboratory analyses obtained and eventual diagnoses, treatments and outcomes for a number of patients who present at the emergency room with severe chest pain. A suitable sequence of actions to take under all possible circumstances might be identified and codified in a flowchart. The principal deficiency of the flowchart as a general technique for encoding medical decision-making knowledge is its lack of compactness and perspicuity (Szolovits, 1982).

Decision theory is a mathematical theory of decision making under uncertainty. One quantifies the a priori and conditional likelihood of existing states and their manifestations and determines the utility of all contemplated outcomes. Given these data, decision theory offers a normative, rational theory of optimal decision-making. The chief disadvantages of the decision theoretic approach are the difficulties of obtaining reasonable estimates of probabilities and utilities for a particular analysis.

14.2.2 Evidence-Based Medicine

A variety of factors go into making health-related decisions of which one is scientific evidence. A system for finding and appraising scientific information is called evidence-based medicine. Evidence is, however, not sufficient for decisions. People also have preferences and constraints which may or may not be consistent with scientific evidence. Examples of evidence, preferences, and constraints follow:

- Evidence: patient data, basic and clinical research, systematic reviews,
- Preferences: cultural beliefs, personal values, education, experience,
- Constraints: policies and laws, time, finance.

The intersection (Mulrow et al, 1997) of

- evidence and preferences provides the knowledge for decision-making,
- evidence and constraints forms guidelines, and
- preferences and constrains forms ethics.

The intersection of the three represents everything that is considered in a healthcare decision.

14.2.3 Database Systems

Large databases of clinical histories of patients sharing a common presentation or disease are being collected in several fields. For clinical purposes, the typical use of large *databases* is to select a set of previously known cases that are most similar to the case at hand by some statistical measures of similarity. Then, diagnostic, therapeutic and prognostic conclusions may be drawn by assuming the current case is drawn from the same sample as members of that set and extrapolating the known outcomes of the past cases to the current one. Limitations to this approach include:

- the collection and maintenance of the data in a consistent and accessible form is costly and
- old data are difficult to reconcile with the new, because of continual refinements.

Databases abound in many parts of healthcare and are used for many purposes.

One example follows of databases for pharmaceutical salespeople. Pharmaceutical companies have vast stores of information amassed in their sales, marketing, and research organizations. (Gambon, 1996). At many companies, sales-force automation programs are evolving from simple contact-management software to robust data warehouse applications. For example, Pfizer Inc., a $10 billion pharmaceutical firm, has a sales-force automation program that enables 2,700 sales representatives to customize their sales pitches. Sales people can quickly provide doctors with highly detailed information about each product's effectiveness, side effects, and costs. The information is stored in an Oracle database that sales people access through customized territory-management software. Sales representatives no longer simply send call reports into headquarters to show which doctors they visited. Instead, they use data warehouse tools to assess whether managed-care contracts, which stipulate what drugs a doctor can prescribe, are being followed. They also maintain information about the status of accounts, customers' credit ratings, their last call to the company, and records of complaints.

14.2.4 Expert Systems

Encoding *human expertise* in the computer is amazingly difficult. The difficulty rests both on

- a lack of understanding of how people know what they know and
- technical problems of structuring and accessing large amounts of knowledge in the machine.

The following scenario illustrates the subtlety of the problem:

> Mrs. Eloise Dobbs, 38, is married to a feed storeowner and she comes to her physician, Dr. Elwood Schmidt, complaining of chest pain. The following dialogue ensues:
>
> "This whole side of my chest hurts, Elwood. It really hurts."
>
> "What about your heart--any irregular beats?"
>
> "I haven't noticed any. Elwood, I just want to feel good again."
>
> "That's a reasonable request, and I think it's very possible you will."
>
> "But what do you think? Is it my heart? Is it my lungs?"
>
> "Now, you won't believe this-but I don't know. I do not know. But I wonder. Are you lifting any sacks down at the store?"
>
> "I lift some. But only fifty pounds or so. And only for the woman customers."
>
> "I think you'd better let your lady customers lift their own sacks If I know those ladies, they can do it just as well as you can. Maybe better."

The doctor in this story relies not only on his understanding of the physiological basis of pain but also on his knowledge of the patient and her occupation, the common practices of small-town stores, and the weight of typical sacks of feed. A computer program with the latest patho-physiological theory would not arrive at the parsimonious diagnosis of the local doctor.

Representing the reasoning of Dr. Elwood is difficult. Reasoning becomes simpler if the structure of the representation reflects the structure of the reality. Early *representation languages* were based on the predicate calculus, in which each fact, or item of knowledge, was represented as a single expression in the language. Newer representation languages incorporate automatic mechanisms to make the simple, local deductions implied by the conventions of their knowledge representation scheme.

Expert systems have been developed for many medical, diagnostic problems and typically have been successful within a certain sense. Understanding this sense and its implications is vital to properly anticipating the future of expert systems in health care. First, however, the technology and experience with it should be introduced.

The *MYCIN system* was developed at Stanford University originally for the diagnosis and treatment of bacterial infections of the blood. The complex behavior of a program that might require a flowchart of hundreds of pages to implement as a clinical algorithm was reproduced by a few hundred concise rules and a simple recursive algorithm. The recursive algorithm is to apply each rule just when it promised to yield information needed by another rule. For example, if the identity of some organism is required to decide whether some rule's conclusion is to be made, then those rules that are capable of concluding about the identities of organisms are automatically brought to bear on the question. Each individual rule can be independently created, analyzed by a group of experts, experimentally modified, or discarded, always incrementally modifying the behavior of the overall program in a relatively simple manner.

Another advantage of the simple, uniform representation of knowledge is that the system can reason not only with the knowledge in the rules but also about them. Thus, methods can be created to:

- help acquire new rules from the expert user when the expert and program disagree,
- suggest generalizations of some of the rules based on their similarity to others, and
- explain the knowledge of the rules and how they are used to the system's users (Shortliffe, 1976).

This *meta-reasoning* about rules also supports machine learning.

Numerous *experiments* were done with MYCIN under rigorous conditions. The program needed to get precise input about the signs, symptoms, and laboratory values for a patient. The experiments assumed the patient had an infectious disease of the blood. Given these constraints, Mycin was able to give more accurate diagnoses consistently than the average infectious disease experts.

In practice, Mycin was not used. With government research funding, Mycin was installed in various clinic settings, but doctors did not want to use it. The first interpretation of the researchers was that the system was lacking certain vital functions, like the ability to explain its behavior. The system was extended with ability to give to the physician the rules that had been most instrumental in any given diagnosis, and these rules were put into attractively understandable natural language. However, this additional feature did not increase the *usage* by practitioners.

Another direction of expansion of such systems was that of covering more than a few diseases. The *Internist-1* system for diagnosis of diseases in internal medicine was developed in the early 1980s at the University of Pittsburgh (Miller et al, 1992). The Internist-1 system included 500 diseases and 3550 findings. For each disease a list of findings was defined that are connected with this disease. The program proceeds through the findings on the patient and computes the likelihood that each disease is associated with the particular history, signs, symptoms, and lab values of the patient. Internist-1, like Mycin, proved competent in doing diagnosis. Experts did not perform better than Internist-1. However, the developers of Internist-1 have also been largely unable to achieve significant usage of their system by practicing physicians.

The story of new expert systems continues. Evans et al (1994) evaluated a computerized *antibiotic consultant* to assist physicians in the selection of appropriate antibiotics. Physicians who used the computer consultant suggested an antibiotic to which all isolated pathogens were susceptible 94 percent of the time, compared with 77 percent of the physicians who did not employ the consultant. The use of the consultant also decreased the elapsed time between the collection of culture specimens and the ordering of the antibiotics. Moreover, 88 percent of the physicians who used the consultant stated that they would recommend the program to other physicians, 85 percent said the program improved their antibiotic selection, and 81 percent said they felt use of the program improved patient care.

As the body of health care knowledge continues to increase, information systems are also being called on to provide practitioners with tools to manage this flood of new information. A number of health care organizations have experimented with computerized decision-support systems that can assist practitioners by issuing reminders, offering a menu of options, or providing links to relevant journal articles. Such decision-support systems are tools in moving toward *evidence-based practice* and can enhance the ability of the health care system to encourage the adoption of care techniques of demonstrated effectiveness. Clinicians who receive computerized alerts and reminders tend to respond faster to changes in their patient's condition (Safran et al, 1996). Studies of computerized decision support for nursing practice have found that such programs can improve nursing care in a range of areas, such as the care of incontinent patients and prenatal care (Marin et al., 1994).

The history of medical expert systems is a long and rich one. Thousands of medical expert systems have been implemented and shown experimentally to manifest intelligence. However, by and large, these systems have not been practically used as intended. What is the explanation for this phenomenon? Clinicians must confront patients in intense, intimate, time-pressured, face-to-face, *belly-to-belly* events. Typically, the patient record is not digital. Even when significant portions of the medical record are digitized, the patient-physician encounter does not occur with a computer between the two people. The physician is collecting vital information from the patient in real-time and going through a heuristic and pattern recognizing diagnostic process that is almost instantaneous. To use the expert systems, the physician needs to take several steps that do not fit comfortably into the situation at hand. First the physician needs to be seated before a computer screen and entering data collected from the patient, then the physician must wait for the computer to determine what it can from the information available, and then the physician must assess the feedback and decide how relevant it is to the situation at hand. If the computer program only handles a narrow range of diseases, such as Mycin did, then the utility is of course substantially reduced. However, even at the

first step of needing to enter data collected from the patient into the computer, the physician faces a barrier or a cost that proves greater than the benefit given the way the health care system operates. The physician can make a good enough conclusion on his or her own without the support of an expert system relative to the cost of using the expert system.

Interesting medical *malpractice* issues arise when considering expert systems. What if a physician follows the advice of an expert system, but the advice proves faulty for the particular patient? Is the physician or the provider of the expert system responsible? On the other hand, if the physician does not use an expert system, and someone can show that the physician made a decision that would have been better had the physician used an expert system, then is the physician guilty of malpractice for not using an expert system.

The reasons for the failure to use expert systems suggest the conditions under which expert systems will succeed. The data needed by the intelligent system should be on the computer from some previous process and should not create an extra demand on the health care professional at a critical time of patient care. For instance, pharmacy and laboratory systems may be receiving data online and processing it by computer before returning it to the health care practitioner. Some expert systems monitor the prescribed drug therapies and provide appropriate advisory messages when it detects potential adverse drug interactions. Another similar class of expert or knowledge-based systems looks at the blood values computed by machines in the pathology laboratory and provides interpretation as to what the diagnosis might be along with returning the raw data to the physician. Such programs require no *extra effort* from the physician to obtain and can be valuable aids to diagnosis. This is the area in which expert systems find the most utility.

Intelligent systems will be increasingly used in health care, but the *precondition* for this use will be the digital availability of information. These insights about the importance of integrated systems to the ability of computers to provide intelligent support are not new insights but have been appreciated for decades (Rada, 1983). The problem is that achieving this digital availability is a slow process. The integrated health care information system is the key to the diffusion of intelligent systems. The integrated system is the subject of the next section and cannot be under-estimated for its importance to the general utility of health information systems. As the ability to share information across applications and institutions grows, so does the ability of the computer to support health care.

The possible applications of *intelligent systems* are not limited to medical applications. Strategic information systems that are a component of administrative systems are a type of decision-support or intelligent system. In general, any part of a health information system can include extensions that incorporate further rules about how the organization works and further semi-automate decision-making, thus making that part of the system more intelligent. Intelligent systems can detect fraudulent claims processes, suggest optimal allocations of physicians to patients, and so on. Anywhere that knowledge and reasoning relevant to the health care enterprise can be somehow captured in the computer, the exercise of that knowledge and reasoning can be automated or semi-automated.

14.2.5 Vision and Robotics

The field of artificial intelligence can be divided into sub-disciplines including computer vision, robotics, natural language processing, neural networks, and expert systems. *Computer vision* uses complicated techniques and mathematical algorithms and can simulate what the human vision system is able to accomplish. Some examples of applications of computer vision in health care include (Armoni, 2000):

- An example of pathological diagnosis occurs when on-line cytological diagnosis is applied to the data supplied by a needle introduced into a suspected tumor
- Radiological diagnosis occurs when the computer interprets a computerized axial tomogram of the brain and determines what disease, if any, is present.
- Recognition of the structure of materials can be achieved by comparing known examples of structures with new samples. For instance, mineral bone composition can be determined and osteoporosis assessed.
- Graph analysis of results of vision tests can lead to interpretation of vision tests and is also a valid approach to interpretation of electroencephalograms.

Robotic behavior is very difficult to achieve in the general case. For example, although it seems that housework is simpler than precision welding, from the robot's point of view the housework is harder because it is less well defined. Medical robotic applications need a well-defined domain. In hip replacement a robot assists in the entire process of planning, locating, directing, and performing the

surgery. A 3-dimensional knowledge of the anatomy allows the robot to work with the surgeon and automatically do the required drilling and cutting at the optimal location. Industrial-type robots have been used in warehouses and manufacturing plants for years and have now arrived in health care. One system enables the computerized locating of drugs at pharmacies and conveying them to the party ordering the drugs.

Natural language processing can be applied in many aspects of health care. Physically disabled people can give instructions by voice to steer a wheelchair or operate electrical appliances. Radiologists can dictate radiological interpretations and have them automatically transcribed in the medical record by computer. The machine may require a vocabulary of 30,000 words, and the machine needs to adjust to the varying speech habits of different radiologists.

Robotics, vision processing, and natural language processing remain challenging areas because the human performance of the task is often difficult to replicate by machine. The sub-discipline of neural computing, by contrast, is not trying to reproduce the performance of people but rather to apply adaptive, statistical methods to data, and such methods are the forte of computer scientists. *Neural network computing* can be applied to statistical classification, signal processing, and image processing. Neural networks process numeric results of tests, signals from electrocardiograms, and images and are capable of finding complicated statistical correlation hidden from human view and thus improve the standard of diagnosis in certain cases. They might recognize relevant facts for diagnosis from among hundreds of variables. In research projects, neural networks have proven able to improve diagnosis in many areas of medicine.

14.3 Research Systems

Knowledge-based systems give to and get from *research systems*. Research systems, in turn, include 'literature systems' and 'clinical research systems'. These systems put unique demands on a health information system.

14.3.1 Literature Systems

Eighty percent of American adults who use the Internet search for health information (Taylor, 2002). Ninety percent of physicians use the Internet. The most common uses of the Internet by physicians in decreasing order of usage are:

- Non-patient related email,
- Accessing medical information sources,
- Collecting travel information,
- Obtaining product information, and
- Communicating with other professionals.

Healthcare professionals recognize that they have unmet information needs. Most are highly specific to patient problems. Usually physicians decided against pursuing answers for the questions. Ely et al (1999) found that answers were pursued only 30% of the time. When information was pursued, the most common sources were other humans. Use of journal articles as well as computer sources was low.

Scientists, educators, and physicians seek information in many ways (Siegel, et al, 1990):

- Direct personal communication with peers and experts is frequently the easiest way to gain assistance in problem solving.
- Within large organizations, technical communications often take place through a gatekeeper. The gatekeeper is a person who maintains a high level of external communication and, through contacts, keeps colleagues informed of new developments.
- Attendance at meetings and conferences also serves to keep individuals informed of recent developments in specialized fields.
- The broadest and most comprehensive access to innovations and new knowledge, however, comes from an examination of the published literature.

For many years health care professionals relied on personal or institutional *libraries* of books and journals to which they turned when they needed literature. However, the sheer volume of written material makes the medical literature unusable without special auxiliary methods, including computer systems.

The *National Library of Medicine* (NLM) is the world's largest medical library. NLM indexes about 3,400 journals. These 3,400 journals are carefully chosen from the over 20,000 journals published each year to represent the premiere journals. The journal article index, and more, is today available in the database MEDLINE via the World Wide Web. MEDLINE has more than 10 million journal article references and abstracts going back to the early sixties. Through the Web at www.nlm.nih.gov health professionals, scientists, librarians, and the public do some 250 million searches of MEDLINE each year. There are increasing links between article references and full text.

Prior to the late 1990s people doing searches on MEDLINE paid a fee for each search. The American government that funds NLM had a principle that private enterprises should not be prevented from competing with government services and thus the services had to be charged at full cost to produce the service. However, by the 1990s and with the wide popularity of the Web, the government was persuaded that *free access* to a medical literature index was more important as a public service than was economic competition.

The information in MEDLINE is massive and could be exploited by numerous computer applications. NLM maintains a 100,000-concept thesaurus, called the Medical Subject Headings (MeSH), for indexing medical literature. This *thesaurus* itself is a valuable knowledge base of medicine. One important property of a thesaurus is that it indicates parent-child relationships. For instance, the concept 'cardiovascular disease' has a parent of 'disease' and a child of 'heart attack'. To query MeSH one might go to the NLM web site and then in the 'Search' menu select the 'MeSH' option, enter the term 'Management Information Systems' in the 'for' text box, and select 'go'. Once the term appears with its definition, if the user selects the term, then the user will be given its hierarchical position. The relationships are indicated in top-down order with indentations as in:

Information Systems
    Management Information Systems
        Ambulatory Care Information Systems

where 'Management Information Systems' is the child of 'Information Systems' and 'Ambulatory Care Information Systems' is the child of 'Management Information Systems'.

Each article is indexed into about ten concepts from MeSH. This indexing creates an enormous semantic network atop the world's premiere medical literature and can be used by artificial intelligence programs to support information retrieval and decision-making (Rada et al, 1990). When a user performs a search on *MEDLINE*, the user can request to get various views of the information. Typical users will take the default, tailored view that gives only the essential information. However, to see how highly structured and extensive the information can be for each article in the collection an arbitrary example is presented in the Figure "MEDLINE Article Index".

The NLM has created a special Web site, MEDLINEplus, to link the general public to many sources of consumer health information. *MEDLINEplus* is designed to help users find appropriate, authoritative health information. To do this, NLM provides access to information produced by the National Institutes of Health, a database of full-text drug information, an illustrated medical encyclopedia, and much more. MEDLINEplus contains pages that link to other web sites. The *selection guidelines* for links demonstrate high standards for quality and reliability. The service provided by MEDLINEplus competes with some commercial health information resources such as WebMD but has the advantages of being unbiased by any particular commercial concern and having the quality standards and long-term commitment of the government behind it.

With the growth of the Web, a new form of publishing has emerged, mostly removed from traditional scientific publishing. Some of this information may be flawed. For instance, Lissman

UI - 20319562
AU - Gupta A
AU - Masthoff J
AU - Zwart P
TI - Improving the user interface to increase patient throughput.
MH - *Efficiency, Organizational
MH - Human
MH - Inservice Training
MH - Radiology Department, Hospital/*standards
MH - *Radiology Information Systems
MH - *User-Computer Interface
AB - One of the main goals of a radiology department is to optimize patient throughput. We have observed a number of factors that reduce patient throughput, one of them being suboptimal system usage. In this article, we distinguish and discuss two ways to reduce suboptimal operation: improved design of the user-interface and active support for learning during system usage, i.e., during examinations. We outline the rationale for this by looking at the current situation and trends in radiology departments. We have based our work firmly on the principles of user-centered design. Observations, task modeling, user involvement, and prototyping have been undertaken.
AD - Philips Research Laboratories, Redhill, United Kingdom.
SO - Top Health Inf Manage 2000 May;20(4):67-77

Figure "MEDLINE Article Index": This information from MEDLINE shows for a particular article these items: AU for author, TI for title, MH for Medical Subject Heading, AB for Abstract, AD for address of authors, and SO for source of article.

and Boehnlein (2001) assessed sites on treatment of depression and found that only half mentioned any symptoms or criteria for depression and that less than half made any mention of medications, psychotherapy, or professional consultation as suggested treatments of depression.

Numerous other concerns exist about the quality of information outside the gated, library resources. For instance, over half of authors of clinical practice guidelines endorsed by major medical societies have received financial support from the pharmaceutical industry, and a majority of these guidelines have no mechanism to disclose such support (Choudhry, Stelfox et al, 2002). For another instance, of 149 scientific meeting research presentations that received substantial attention in the news media, 76% were nonrandomized, 25% had fewer than 30 subjects, and 15% were nonhuman studies (Schwartz et al, 2002). Furthermore, half were not subsequently published in Medline-indexed journals.

14.3.2 Clinical Research

The goal of *clinical research* is to advance the state of medical science and thus to improve the practice of medicine. In many scientific disciplines, researchers can investigate problems by conducting controlled laboratory experiments. Ethical and practical concerns, however, limit experimentation in medical care. In general, clinical researchers must be content with observing interventions and the resulting outcomes as physicians try alternative therapies to help patients regain health (Wiederhold and Perreault, 1990).

Two of the central tasks of clinical research are data management and data analysis. The most scientifically desirable form of clinical research is the randomized *clinical trial* in which patients are randomly assigned to alternate groups, and are treated according to a study protocol. Investigators collect data and compare the results obtained from each group to determine whether patients who receive different interventions experience significantly different outcomes. One technique to minimize bias is called blinding. In single-blind studies, patients do not know which treatment they are receiving. They may, for example, be given a placebo instead of an active drug. In double-blind studies, neither patient nor researcher knows to which group the subject belongs, thus avoiding systematic bias in the way treatments are given or in the way results are reported. The blinding approach makes good sense from the research perspective but raises problems as regards patient rights-to-know. In any case, information systems are crucial to the successful implementation of a clinical trial.

Various types of professionals participate in the clinical research process:

- the physicians, nurses, and other health care providers who administer treatments and collect data;
- the medical-records personnel who enter, store, and retrieve data;
- the epidemiologists and statisticians who model the problem and analyze the data; and
- the patients themselves as subjects.

Clinical researchers often use *database management systems* to help in the tasks of data entry, multi-user access to data, and long-term maintenance of stored information.

Clinical researchers use a variety of statistical techniques to analyze data. *Statistical packages* are collections of programs that can be invoked to perform calculations on data and generate reports. Statistical packages are well developed. The Statistical Package of the Social Sciences (SPSS at www.spss.com) and the Statistical Analysis System (SAS at www.sas.com) are two well-known packages.

Various computer systems offer specialized support for clinical research. One such system, called MEDLOG (www.medlog.net), is tailored for medical data management incorporating a Time-Oriented Design that supports tracking variables which are measured repeatedly over time. *MEDLOG* also provides a clinical data management system.

Research also benefits from registries. The mission, design, size, methodology, and use of technology vary with each kind of registry. Examples of some of the most widely used registries include cancer, AIDS, birth defects, diabetes, organ transplants, and trauma. Cancer registries are the most common and are elaborated here. Physicians and epidemiologists concerned with assessing cancer incidence, treatment, and end results have long accepted the collection, retrieval, and analysis of cancer data as essential. The types of cancer registries are defined as either hospital-based or population-based (Smith, 2000).

The primary goal of hospital-based *cancer registries* is to improve patient care. The data are used:

- to make certain the optimal care is provided,
- to compare the institution's morbidity and survival rates with regional statistics,
- to determine the need for education programs, and
- to allocate resources.

Data items routinely collected include patient identification and demographic information, cancer diagnosis, treatment given, prognosis factors, and outcomes. Hospitals generally have no legal requirement to keep cancer registries.

The three types of population-based cancer registry are

- incidence only,
- cancer control, and
- research.

Most *incidence only registries* are operated by a government health agency and are designed to calculate cancer rates, usually required by law. *Cancer control registries* often combine incidence, patient care, and end results reporting with various other cancer control activities, such as cancer screening and quit smoking programs. Many *research-oriented registries* are maintained by medical schools to conduct epidemiological research focused on etiology. Information is shared with public servants and health care providers, and often published in medical journals. The legislative mandate or funding sources normally determine the focus – incidence monitoring, cancer control, or research.

14.4 Questions

1. What is the role of standards development organizations in the development of de jure standards and how does this differ from the role of those organizations that develop de facto standards?
2. Compare and contrast methods of putting knowledge in computers that rely on flowcharts, decision theory, databases, and rules?
3. Why were medical expert systems not wanted by practitioners?
4. How are vision and robotics systems used in health care?
5. What contributions has the National Library of Medicine made to health care information systems?
6. How are registries important in clinical research?

15 Diffusion

Learning Objectives

- Apply the 3 phases of agricultural diffusion to HIS diffusion.
- Identify four types of health care systems globally and provide examples of countries employing each type and relate this to information systems impact.

Developing a health information system requires overcoming many barriers. Under what conditions will a health information system be successfully adopted by its intended target audience? The theoretical issues for *diffusion* are presented. Then a detailed case of preparing to implement one large system shows some preparation needed to diffuse a system.

15.1 Theory

While many reports exist of successful health information systems implementations, the evidence suggests that the majority of implementations are failures (Heeks et al, 2000). These *failures* take many forms:

- from a complete collapse,
- to working initially but failing later, or
- from working in the test site but not in the intended deployment site.

The advice provided decades earlier by people like *Barnett* (1968) remains applicable today, namely, the system must be:

- carefully attuned to the needs of its users,
- fit gracefully into the workflow of those who are expected to use it, and
- show clear benefits to its usage.

Students of history, sociology, and engineering note a number of stages that technical innovations go through before becoming accepted as traditional marketplace items or services. Frequently, the sequence is

- research,
- development,
- demonstration,
- commercial prototyping, and
- production.

Transitions between the stages occur at irregular intervals, and the total cost of each phase increases as one moves toward the market.

While many ideas and practices have moved rapidly through modern medicine, the spread of information systems has been irregular. For better or worse, the *rate of diffusion* of HIS technology has been slow. Classical studies of diffusion of innovation have been made with respect to agricultural practices. The first bag of fertilizer applied to a farm essentially represents a commitment to testing, analysis, and correction of soil conditions ad infinitum. Lionberger (1960) constructed a taxonomy of agricultural innovation as follows:

- Grade One: easily understood and demonstrated, use of pesticides for instance.
- Grade Two: somewhat more difficult to understand and demonstrable only over a minimum time of a crop cycle; use of improved fertilizers for instance.
- Grade Three: more difficult to understand and demonstrable only over multiple years; for instance, improved genetic management of crops.

Counterparts to these agricultural innovation examples can be found in the HIS field.

- Grade One: Automation of a current simple practice, such as patient accounting. This is easily understood, and the demonstration of feasibility and efficacy does not take long. This is especially true when a single package can be adopted to handle the entire patient accounting problem. More than 85% of all U.S. hospitals used computer systems in connection with their patient billing, collections, and third party reimbursements already by 1975.
- Grade Two: Automation of a current, more complex procedure such as analysis of electrocardiographic (EKG) signals. The general nature of the task is well understood – to interpret the EKG. The demonstration of successful operation of the automation is also rather easily shown over a matter of minutes. The automation of EKG interpretation has spread pervasively through the health care system.
- Grade Three: Automation of an entire system, such as a computerized medical record, is rather more difficult. The concept is not easily explained. It demands coordination of actions of many people. The execution must be timely. The beneficial results are indirect and relatively

> remote in time with respect to the actions of the system. Indeed, there may be no benefit unless all of the subsystem components perform their jobs properly. In these respects the concept of the computerized patient record is analogous to the concept of improved genetic practices in agriculture.

Nothing about the computer techniques in HIS makes them fundamentally different from such systems in non-medical fields. There are, however, two special non-technical barriers: medical knowledge and medical management.

Much of medicine remains an *art*. Mental health is a good example of an area in which the knowledge of the biological processes remains primitive. Unlike the monitoring of physiological parameters on a patient in the intensive care unit where alerts are readily generated for physiological signals gone askew, the monitoring of mental health patients is less precise. So what can be expected of a medical system for different patients with different conditions varies and for some patients little scientific or algorithmically defined intervention seems relevant given the current understanding of disease.

The second barrier peculiar to health care is the management, social, or political environment. The health care system is composed of thousands of relatively *autonomous units*. Hospitals are themselves made of units that operate somewhat autonomously within the hospital. To the extent that health care institutions do not operate smoothly and sensibly with one another, the HIS cannot be shared or transplanted. To the extent that the institutions are balkanized, so are their information systems.

Ruffin (1999) has gone so far as to say that the critical factor is *political* as follows:

> The successful selection, procurement, and implementation of information and communication systems are far more political than technical. … Ignore the political issues and the technical issues will not matter, because implementation will fail and the potential benefits promised by the technology will not materialize. 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. … Without excruciatingly exact formatting, data cannot flow from one computer to another. Without that excruciatingly exact formatting, data cannot flow from the laboratory system of a hospital to a communication network and into the computers in the offices of physicians.

To achieve this precise agreed formatting among units requires standardization, which in turn is essentially a political act.

15.2 Practice

IT will remain a cost center, if it maintains the traditional practices. To overcome this the IT plan must be fully integrated with the organization's vision. IT investments then are predicated on a Return-on-Investment (ROI) to both implement and sustain key business goals by automating newly redesigned processes (Ummel, 2003).

These proactive measures can help transform an environment from one in which IT is an optional cost to one in which IT is a critical enterprise investment (Ummel, 2003):

- The CEO assumes responsibility for the CIO.
- An IT Steering Committee is chaired by a senior executive other than the CIO and does knowledge gathering, planning, priority setting, and ROI-based investing. The members of the Committee are senior management, the CIO, some clinicians, and some departmental managers.
- A management incentive plan rewards achieving IT milestones.
- Operating managers and executives participate in vendor evaluation and selection.
- All IT projects are preceded by solid business cases, necessary and significant process redesign in applicable areas, and full accounting of the post-implementation results over the ensuring 3 years.
- Executives and managers are fully accountable for predetermined IT benefit realization in their annual performance review. Disciplinary actions are consistently enforced.

IT projects will be ineffectual until the people who control the business processes change their core processes as an adjunct to automation.

Information systems are critical to quality health care, but *clinician resistance* is a key barrier to diffusion. 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 (IOM, 1997).

Supporters of automation see great potential in using computer-generated 'reminders' to prompt clinicians to ask patients certain questions or run particular tests. Clinicians, however, may see this as cookbook medicine that limits their professional autonomy (Dowling, 1987).

Improved information systems will greatly enhance the capability to report and track *errors* and other problems with care. If, however, this information is primarily used to identify 'poor performers' rather than to guide improvement efforts, health professionals may view the system with suspicion.

While dialog between clinicians and administrators will play a critical role in addressing many of these concerns, changes in the *education* and training of health care professionals also will be critical. The educational experience of health care professionals can shape attitudes toward, and provide the skills for, using health care information systems. Historically medical schools have de-emphasized education about the use of information systems or the functioning of health care enterprises in order to have enough time for the traditional topics, like anatomy, pharmacology, and pathology. Also the increasing knowledge about the molecular basis of disease must fit into the curriculum, and time for information systems education is hard to find. However, nursing colleges are increasingly including informatics and the use of information technology into the nursing curriculum, especially at the master's and Ph.D. levels.

The National Library of Medicine has been active in funding physicians to study information systems but that impact has been small compared to the need for information systems *education for clinicians*. No ready solution to this education problem – namely the problem of reducing the gap between what clinicians might usefully know about information systems and what they have time to learn -- is in sight.

15.3 Department of Defense

What are the detailed steps for implementing a major system so as to work against user rejection of the system? An example from the military illustrates the necessary steps for implementation of an integrated health information system, in this case the *Composite Health Care System* (CHCS).

The *CHCS Program Office* is responsible for the diffusion of the CHCS. CHCS must be installed first in a treatment facility and pass an Operational Test and Evaluation before worldwide implementation can begin. Implementation of the system requires commitment and teamwork at all levels from the Program Office to the sites.

The *Implementation Guide* describes the activities necessary for the successful implementation of the CHCS in Medical Treatment Facilities (MTFs) worldwide. The Implementation Guide outlines roles and responsibilities, identifies points of contact, specifies business process changes, details key implementation and training activities, establishes timelines, and provides the framework for site level implementation planning and preparation.

The first step in planning for the CHCS implementation at a site is the acceptance of the CHCS *Site Agreement*. Experience with system implementation has shown that a clear understanding by all participants of the roles, responsibilities, and expectations is paramount to successful implementation, training, and testing activities. The Site Agreement was developed to ensure implementation participants understand the key success factors and to achieve consensual agreement to perform the required tasks. Only after signature by the CHCS Program Manager and the Commanders of each of the participating facilities, will implementation activities begin.

The CHCS Program Office (PO) interfaces with the personnel appointed by the MTF Commanders. The MTF Commander selects a military physician to serve as MTF *Project Officer*. This individual should be viewed as the commander's personal representative for this project, and should have sufficient rank, experience, and commitment to interact with higher headquarters staff, the CHCS PO staff, and to successfully orchestrate a myriad of tasks at the local level.

The CHCS Site Coordinator performs a *site survey* at each facility 7-9 months prior to scheduled installation. The purpose of the survey is to determine the requirements to prepare the MTF to receive CHCS. During the pre-implementation phase, site leaders ensure that CHCS site level data is contained in the *Health Data Dictionary* information model.

A set of Core Standardized Templates is available to each MTF as part of CHCS. The *templates* include medical specialty specific templates as well as generic encounter templates. Documentation flexibility for providers is afforded through the use of Encounter Templates. Providers may use one of the templates in the Core Set or construct their own encounter templates by identifying the desired template components.

Training duration varies by user. Front desk and administrative personnel receive a 4-hour course. Support staff receive an 8-hour course. Medical Providers, Nurses, and Nurse Practitioners receive 2 days of CHCS training that includes guided exercises and hands on scenarios. Users receive their system identifiers and passwords after they have completed training.

15.4 International Health

Moving from the concerns of large global organizations, such as the American military to the concerns of countries, what does one see as the likelihood of diffusion of health information systems *internationally*? A person may travel from country to country and require health care wherever he or she may be. How will the health records of that individual be accessible to providers anywhere? Epidemics know no national boundaries. For example, AIDS originating in one country and spreading to another is of concern to both countries, and both countries want to know what is happening in the other to deal with this problem. The reasons for information systems to saddle national boundaries are many. However, the first problem to confront in this regard is that health care systems are different from country to country.

15.4.1 Policy

In all countries the *government* plays some role in health, but the extent of this role varies widely. In the United Kingdom the government essentially owns the health care system. In many countries the government owns some of the health care system and some is owned by other entities.

In *countries* such as the United States, where private health insurance is widespread, the health care plans offered by insurers play a major role in setting the conditions for care. In countries with public or statutory health care insurance, there may be a single payer (usually a governmental unit, as in Canada). Alternatively, a plurality of insurers either quasi-public or private (as in Germany and France), may share these intermediary administrative tasks (Wessen, 1999).

Broadly speaking, health care systems nationally may be divided into 4 categories (Roemer, 1992):

- entrepreneurial,
- welfare-oriented,
- comprehensive, and
- socialist.

The only highly developed country with a basically entrepreneurial health system is the United States. Of middle-income, developing countries, the Philippines has an entrepreneurial system and of low-income, developing countries, Kenya provides an example of an entrepreneurial system.

Welfare-oriented systems are typical of Western Europe, Canada, Japan, and Australia. In 1883 Germany enacted legislation for mandatory health insurance. This insurance is now carried by hundreds of 'sickness' funds financed by the government and regulated by the Ministry of Labor and Social Affairs at the federal level and in each 'lander' or province. The sickness funds enter into contracts with associations of physicians, which are paid periodic per capita amounts according to each fund's membership. Then the medical association reviews and pays the fees charged by the physicians. Government funds account for about 75 percent of the German health expenditure and about 25 percent comes from private funds. Peru and India are examples of low-income, developing countries with welfare-oriented health care systems.

The best-known *comprehensive health system* is that of Great Britain. From World War II until 1990, the British health care system could be characterized as one in which 100 percent of the population was entitled to complete health care, and the financial support was entirely from the government. Almost all health facilities were under the direct control of the government. The Scandinavian countries, Italy, and some other advanced countries have a similar comprehensive system. In a socialist health system the government controls all physical and human resources, and health services are available to everyone. Such is the case in Cuba, Russia, and China.

The debate about appropriate health system policies and strategies has been hampered by inadequate information about the extent to which systems contribute to a set of socially desirable goals. The World Health Report 2000 proposed a framework for measuring the attainment of health systems in terms of socially desirable goals. The defining goal of health systems is to improve health. But people also expect them to be responsive to their legitimate non-health needs and to ensure that financial contributions to the system are distributed fairly across households. The goals of improving health and responsiveness contain two components – improving the average level and reducing inequalities. Accordingly, five indicators of goal attainment were defined - the level of population health, inequalities in health outcomes, the level of responsiveness, inequalities in responsiveness, and the fairness of household financial contributions to health. The World Health

Report measured the inputs used to achieving these goals – health system and non-health system inputs – and an index of the efficiency with which the goals were attained given these inputs.

Major conceptual and methodological debates emerge. The major conceptual issues relate to the boundaries of the system, the concept of causality, the question of attribution of responsibility for outcomes, and whether goals are universal. Methodological debates focus on the measurement of healthy life expectancy, health inequalities, responsiveness, fairness of household financial contributions and efficiency. Information systems work is required to deal with the volume of data and the sophistication of analysis. Linking the measurement of outcomes and inputs with the analysis of the functions of health systems leads to the development of practical policy implications for ways to improve health system performance internationally (Murray, 2001).

15.4.2 Technology

The *United Kingdom National Health Service* plan for information technology in health care is that local and national networks are integrated. In particular, integration of systems is encouraged so that any single data is collected only once. A network of shared administrative databases holding basic patient details has been replacing existing isolated databases.

The *Australian Institute of Health and Welfare* produced a National Health Information Model that provides a framework for the management of health information at the national level. It was developed using a 'top-down' approach, allowing the model to reflect how health information should be structured rather than reflecting necessarily how health information is currently structured (AIHW, 1997). The model incorporates health information activities that meet agreed national priorities. These activities range from standard data charts of hospital accounts to health outcome measures. A key element of the model is a National Health Data Dictionary, which consists of a set of national standard definitions. The definitions extend beyond institutional health care and include the health labor force, outpatients, and mental health.

Fragmented health markets in the *European Union* hamper innovation and the spread of best practice. European Union governments spend, on average, 8% of Gross Domestic Product on health. Digital technologies can improve the productivity and scope of health care. This potential is not being fully exploited – only 1% of total health spending in Europe is used on information technology. The goals of the European Union are:

- Healthcare best practices in networking, health monitoring, surveillance of communicable diseases, and on links between hospitals, laboratories, pharmacies, doctors, primary care centers and homes are identified.
- All European citizens have the possibility to have a health smart card to enable secure and confidential access to networked patient information.
- All health professionals and managers are linked to a computerized health information infrastructure for prevention, diagnosis, and treatment.

This does not mean controlling national health care at a European Union level. However, it does mean conducting health information systems research, agreeing health information standards, and building pan-European medical libraries.

The *United Nations* is involved in various global health care activities and information systems efforts. However, goals such as an international health care card for each citizen are only remote possibilities given the vast differences in health systems from country to country The international activities in health information systems could benefit by further coordination at global levels though this seems unlikely to happen anytime soon.

15.5 Questions

Reading Questions

1. Compare agricultural diffusion theory to health care information systems diffusion theory.
2. What kinds of health care systems do different countries have?

Doing Questions

1. The medical school curriculum has too much material to cover for the time available and under these conditions introducing new education about health care information systems is very difficult. How do you suggest that medical schools might introduce education about information systems into the curriculum? Please provide some evidence of your approach succeeding in some school(s).
2. Consider the three stages of diffusion as found in agriculture and health information systems. Find some examples of health information systems currently in use and categorize them according to

where they would fit as to the type of diffusion that was necessary for them to succeed.

3. How might the wide diffusion of the World Wide Web have changed the conditions under which certain health information systems might be expected to diffuse? Provide arguments and examples.

16 Conclusion

Main Points

- Information systems must fit into the workflow of people.
- Health care trends are toward further cost control.
- Information system trends are to further use of the Internet.
- The health care and information systems trends combine to suggest a vision in which information systems are used to further control costs by bringing more players, particularly patients, more closely into the activities of health care.

Health information systems have been relatively under-developed compared to the systems in other industries, such as financial, manufacturing, retail, and publishing industries. The reasons for this under-development have been presented along with the steps to change the situation. The investment in health information systems is growing, and the principles and examples given in this book can help the reader take advantage of this growth and contribute to it.

16.1 Summary

The study of health information systems is multi-disciplinary. In particular, the topic benefits from the fields of health care, management, and information systems. As distinct from a typical textbook in management information systems, this book looks exclusively at the experiences gained from health care.

This book focuses on health care information systems in the US. Health care systems are so connected to the political and economic situation of a country that detailed, practical insights are hard to obtain that apply equally well across countries. The US system has evolved over the past one hundred and fifty years from one that revolved around a solo private physician in a rural setting whose patients paid him directly for whatever services he rendered to a massive industry of insurance companies, multi-hospital networks, and mobile patients.

Many of the insights of pioneers in health information systems from almost half a century ago remain equally valid today. Lindberg felt that information systems could make a big difference in the effectiveness and efficiency of health care. Barnett emphasized that the challenge is to fit into the workflow of those who are to use the system. Kissinger saw that the complexity of the environment continually increases and thus the challenge of fitting into the workflow also grows.

Many books have been written about health information systems with usually a distinct audience in mind each time. For instance, one can find books for

- physicians with practical tips on how to use computers in the private office,
- Chief Information Officers on strategies for implementing enterprise-wide systems,
- nursing students on support systems in the hospital that nurses use to help patient care, and
- medical students on computer-supported diagnosis.

This book is for students of information systems and of health care administration and for professionals responsible for decisions about information systems in health care enterprises.

16.1.1 Challenges

Rising costs have been one of the greatest problems for the American health care system. The costs have risen more than costs of other services in the country. Some say this is due to the increase in costly treatments. However, in some other highly developed countries the portion of gross national product spent on health care is much less than in the U.S. and yet the quality of health for citizens on average in those countries is no less than that of citizens in the US.

Against the backdrop of high costs and sophisticated equipment, Americans are surprised at the large number of errors by healthcare providers. One hundred thousand people die each year in the US from medical errors that occur in hospitals.

Information systems could reduce errors, if used properly.

To deal with high costs, the health care industry is moving towards less care in the hospital and more care in the outpatient setting. Information systems are likewise increasingly addressing the connections that are needed among the various parts of the health care enterprise.

Most health care organizations spend less than 5% of their budget on information systems. This is considerably less than one might expect for an information intensive business. The financial industry spends more than double that amount on information systems. However, the amount of investment in information systems in health care is increasing.

16.1.2 Design

The delivery of health care is a professional business. This contrasts with businesses that are either entrepreneurial or machine in character. The professional business lends itself less to systematic use of information systems since the professionals prefer autonomy. The implication for design is that the design team has to work very closely with the users and carefully probe the nuances of the work environment. Whatever is proposed for implementation must very closely match the way the professionals are accustomed to work.

In addition to the close match to the work styles of the intended users, successful design projects in health care need to also pay close attention to the administrative situation. The support of all relevant levels of administration should be assured at the outset and carefully nurtured throughout the lifetime of the information systems project.

One approach to design of a hospital information system emphasizes the use of pictures to convey what happens in the health care entity. These pictures are produced by the designers in working closely with the end users. The users give feedback based on the pictures, and refinements can proceed based on this iterative process of developing easy-to-interpret representations of the flow of information and work.

The kernel of a hospital information system provides the basic communication and processing capabilities. As such, it must make some assumptions about the control over the communication and decision-making in the hospital. This kernel thus must also be developed with great care in order to respect adequately the diverse political interests in the entity. A prototype should be constructed with which users can experiment so that they become comfortable with the basic assumptions.

16.1.3 Providers and Payers

The system components of a provider organization are reasonably well delineated. The initial component that patients typically face is the admissions or registration system. This system is connected to the billing and medical records system. The financial and resource management aspects of health care have been the first and most consistently computerized.

At the next stage of the patient experience is diagnosis and treatment. This stage remains dependent on subtle, imprecise factors that work against computerization. However, certain departments, such as the pathology laboratory, the radiology laboratory, and the pharmacy, have proven amenable to semi-automation, and computers are used in abundance in those departments. Connecting highly computerized facilities with manual facilities is difficult. Those components that revolve around the patient record and the collection of signs and symptoms from the patient are still often paper-based.

Some activities are readily digitized. Some departments proceed with their automation independently and move quickly. To achieve integration across departments is difficult. Departments must agree on standard languages for communicating parts of the patient record and other information. An example of a large military systems implementation reveals the extent of resource required to move even slowly forward in achieving integration across a health care system.

The basic operations of a health plan are to enroll members, contract with providers, accept claims from providers, adjudicate claims, make payments to providers, and audit the quality and efficiency of the health care delivery. The health plans are both part of the financial industry and part of the health care industry. The staff of a health plan are less autonomous than physicians and more readily cooperate with information systems staff in implementing systems that automate work. Health plans also place a greater fraction of their budget into information systems.

The plans are involved with diverse entities. Employers often pay a large fraction of the premiums of an employee and this puts health plans and employers in intimate relationships. The government operates the countries largest health plan in the form of Medicare and Medicaid but these are distinctly different from the private health plans due to the

source of the money that the plan spends. Another entity that is important in the health plan scene is the clearinghouse. The clearinghouse is an intermediary between providers and health plans.

Health plans operate differently when serving individuals, small groups, and large organizations. They also face different laws and regulations at state and federal levels depending on the kind of customer they are serving. The laws and regulations represent a delicate balance between the government's intention to guarantee health for its citizens and at the same time to maintain a capitalist health system.

16.1.4 Regulations

The government regulates the health care industry in many ways. This book has focused on two particularly important components of the health care regulation environment: fraud and administrative simplification.

Fraud occurs when a claim is made that is not fair. The *False Claims Act* was passed during the American Civil War. Much corruption occurred in federal procurements during that 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.

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.

The government now uses 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.

16.1.5 Ecommerce and Transactions

A considerable portion of every healthcare dollar is spent on provider-payer transactions. HIPAA was passed in 1996 in part to reduce costs in health care by standardizing transactions between providers and payers. When the Congress realized that such standardization might also increase the accessibility of electronic health information to the wrong people, Congress added privacy and security requirements to HIPAA.

While not all aspects of a health care provider are touched by the provider-payer transactions, almost every health care entity is affected by this standardization. The standards apply to the envelope and format of the messages and to the codes used in the fields inside the messages. The major codes for diagnosis come from the International Classification of Diseases and the major codes for treatments come from 'Current Procedure and Terminology'.

16.1.6 Privacy and Security

The privacy component of HIPAA requires health care entities to treat individually identifiable health information with respect for privacy. Business associates cannot see the information without agreeing to certain contracts. Everyone in the health care entity should be careful to only use the information needed to do the job well.

The Privacy Rule gives patients new federal rights. Patients must be given copies of their medical records when the patients request it. The patient can request amendments to the medical record.

The Security Rule mandates common sense approaches to information security. Entities should have contingency plans, should ensure passwords are handled properly, should encrypt messages sent on the Internet, and so on.

16.1.7 Personnel and Vendors

People are the key to the success of any technology advance. The patients and the front-line care providers, namely, the doctors, nurses, and allied health professionals are the basis of the enterprise. The changes over the past one hundred years in the distribution of staff in the health care field are noteworthy. Originally, the system was served almost entirely by doctors working alone. Now over half of the workforce is allied health professionals. The next largest category is nurses who number over three million in the U.S. Physicians number less than one million. This move to increasing reliance on diverse support staff makes sense in terms of the move to a cost-conscious, massive industry. The increasing reliance on support staff should also speak favorably to the likelihood of the industry increasing the use of computers because the support staff have proven more amenable to the use of information systems tools in their work.

Each large health care enterprise also has a staff of information systems specialists. The Chief Information Officer is the senior members of this staff and is responsible for both vision and

negotiating for resources with other components of the entity. The CIO's staff will both support users and engage in operations to continue the infrastructure activities of the entity.

Vendors of information systems play an important role in the health care industry. Hospital information systems would be difficult for the average hospital to build on its own. Some vendors are parts of massive information technology conglomerates with subsidiaries addressing the health sector. Other vendors focus exclusively on health care. In either case, a vendor with a large health care activity may offer a wide suite of systems to serve every part of the health care enterprise.

For diverse information systems problems, the health care entity may lack the staff with expertise to deal with the problems, and so the entity will hire consultants. Consultants assume roles not readily filled by anyone else, particularly when they have state-of-the-art technical knowledge and knowledge of best practices at comparable organizations. Consultants typically charge high prices, come from the environment in which they do consulting, and face the challenge of needing to continually find customers.

16.1.8 Knowledge and Diffusion

Knowledge-based systems can extend the value of information systems by adding intelligence to the processing of the information. For instance, a computer can look at a drug prescription, check a patient's record, check a knowledge base of adverse drug-drug interactions, and tell the care provider whether this new order is safe. Capturing the knowledge from people and encoding it into the computer is not easy. However, the greatest challenge is to get the knowledge-based systems to integrate with the work flow of the intended users.

Diffusion of technology has been studied in many disciplines. The basic conclusion is that the technology must fit easily into the workflow of the intended user and show immediate benefit. This is difficult to show with something like an integrated patient record system whose gains may only be obvious after substantial effort to get information into the appropriate forms in the records. Analogies to agriculture are interesting. Pesticides can show immediate results, whereas genetic management of crops only reaps benefits over years. Automation of claims shows immediate results, whereas computerized patient records reap benefits after the entity's information systems are integrated.

A patient's or a society's health concerns go beyond a single hospital or city. Countries have health care systems that vary enormously from one to another. The European Union manifests some intriguing efforts to spread good practices across national boundaries.

16.2 Healthcare Trends

The healthcare delivery industry in the United States is highly fragmented, very complex and remarkably inefficient. While science and medical technology continue to make significant progress in dealing with human disease and injury, the management and clinical processes of these complex delivery organizations have made little progress. 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. 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. 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.

A number of for-profit business models were created attempting to find the leverage point that would transform the healthcare delivery system. The models included for-profit acute care, physician practice management companies and the focused factories specializing in one element of healthcare, such as cardiology. Most of these efforts have been unsuccessful.

Federal government policy in the United States has also been an active force shaping the health care environment. The policy impact includes the focus on health care reform in the Medicare Fraud and Abuse compliance program. The regulations of the Health Insurance Portability and Accountability Act guide standardization of provider-payer transactions but also require extensive privacy efforts.

16.3 Information Systems Trends

The healthcare information systems industry is 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 'best of breed' systems resulting in disparate and disconnected information systems within the institution. Most recently, 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.

Health care enterprises are deploying information systems solutions that internally automate the paper-based medical record system and externally create smart connections between the major participants in health care: the consumer, the physician, the hospital, and the health plan. The emergence of Internet connectivity has enabled a new class of solutions that help the consumer participate in care management.

The same infrastructure that is automating the clinical and managerial operations of the medical center and clinic is extending to trading partners within the healthcare industry. Managed care authorizations, referrals, claims and remittance can be submitted to local, regional, and national exchanges for rapid processing. Orders for tests and results can be transmitted over the Internet to physicians and consumers alike. Most importantly, consumers have the option of working closely with their local healthcare organization to organize and manage their care or selectively work with providers on an as-needed basis. An Internet-based personal health record may emerge to assist patients and caregivers with maintaining care-related information.

16.4 Vision

The vision of those working with healthcare information systems is to enable the transformation of healthcare through the implementation of information systems and the deployment of medical knowledge. As a result of the rapid changes in the healthcare and information technology industries, a 'New Health Enterprise' may emerge with an information 'backbone' which connects consumers, providers, and plans to service the healthcare needs of a community (Cerner, 1999).

The New Health Enterprise will require information systems that can manage care delivery virtually across a community, while simultaneously managing the business services side of healthcare. This will require managing care from the patient's home to the Intensive Care Unit in a paperless fashion. In this digital environment, consumers and physicians will be able to choose from a variety of electronic access devices to connect to the clinical process of care and create or review a complete health record for each individual. This precise and specific personal medical information will create large data repositories storing and tracking health outcomes over multiple lifetimes. New knowledge and medical insights will be harvested from this data.

Healthcare information systems will securely manage health care transactions from each point of access to their destination. Healthcare information systems will allow customizations to consumers and physicians, embed clinical rules to monitor care safety and quality, and use business and compliance rules to create more efficient business management.

Purchasers of health care services should insist that providers and plans be able to produce quantitative evidence of quality as a means of encouraging investment in information systems. Group purchasers should work with health plans and providers to implement standards for information systems.

The availability of secure, standardized, digital information will be lost on a population unprepared to deal with it. The training of health care professionals should include the use of information technology in clinical settings. Graduates of professional schools should be experienced in the use of automated patient records and computerized decision-support tools. Education programs for paraprofessionals and other health care workers should also incorporate training in the use of information technology. There is a need for continuing education programs to train the existing health care workforce in the use of these systems.

The vision and objectives of any given health care entity must be related to health care trends and information systems trends. These trends call for increased support of the health care enterprise by information systems that will require enlightened

participation of an increasingly large portion of those people who participate in the health care process.

This book has emphasized the information systems needs of the health care enterprise. However, the consumer trends that were described in an earlier chapter might become a dominating factor. The Web might allow for new socio-technical developments not previously anticipated. All of the developed countries have experienced powerful forces of demographic, cultural, and economic change that have shaped their health care 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 health care and the development of progressively more complex and specialized health care practices. This common heritage has led to patients demanding more and better care but society not satisfying these demands. One hope is that an enlightened citizenry through the advantages of global information systems might become better informed about health, more successfully treat itself, and turn the health care 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.

16.5 Questions

1. Which healthcare trends and information technology trends do you think are most significant for health information systems and why?
2. The vision calls for an integrated information system. One could imagine this achieved by having one vendor producing one masterful, comprehensive system or many vendors producing modules all of which communicated readily through standard interfaces with modules of all other vendors. Neither scenario seems particularly likely. If you were to put your money on one approach or the other to win, which would it be and why?

17 References

17.1 A-L

Armoni, Adi editor (2000) *Healthcare Information Systems: Challenges of the New Millenium,* Idea Group Publishing: Hershey, Pennsylvania.

ASTM (1996) E1762 Guide for Electronic Authentication of Healthcare Information, American Society for Testing and Materials.

Ball, Elizabeth (1991) "Maximizing the Benefits of Using Consultants" in *HealthCare Information Management Systems*, ed. Marion Ball, et al, pp 326-330, Springer-Verlag: New York.

Barnett, G Octo (1968) "Computers and Patient Care" *New England Journal of Medicine, Vol. 279*, pp 1321-1327.

Barnett, G Octo (1990) "History of the Development of Medical Information Systems at the Laboratory of Computer Science at Massachusetts General Hospital" in *A History of Medical Informatics* edited by B Blum and K Duncan, ACM Press, New York, New York, pp 141-154.

Barnett, G Octo and Robert Greenes (1969) "Interface Aspects of a Hospital Information System" *Annals of New York Academy of Science, Vol. 161*, pp 756-768.

Bass, Steve, Lisa Miller, and Bryan Nylin (2002) *HIPAA Compliance Solutions: Comprehensive Strategies from Microsoft and Washington Publishing Company*, Microsoft Press: Redmond, WA.

Bates DW, Teich JM, Lee J, Seger D, Kuperman GJ, Ma'Luf N, Boyle D, Leape L. (1999) "The impact of computerized physician order entry on medication error prevention" *Jr American Medical Informatics Association, Vol 6*, pp 313-21.

Beshears, Fred (2001) "Mintzberg's Classification of Organizational Forms" http://ist-socrates.berkeley.edu/~fmb/articles/mintzberg/, last accessed July 2005.

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.

Cerner Corporation (1999) *1999 Annual Report*, Kansas City, Kansas, http://www.cerner.com/.

Childs, Bill (1991) "Consulting: State of the Art" in *HealthCare Information Management Systems*, ed. Marion Ball, et al, pp 319-325, Springer-Verlag: New York.

CITPO (2005) *Composite Health Care Systems II*, US Military, http://citpo.ha.osd.mil, last accessed July 2005

Cupito, Mary Carmen (1998) "Paper cuts? HIPAA's new rules" *Health Management Technology, Vol. 19 Issue 8*, p34, 5p.

DeLuca, Joseph (1991) Health Care Information Systems: an executive's guide for successful management. American Hospital Publishing, Inc. an American Hospital Association company.

Denton, Ira (2001) "Will Patients Use Personal Health Records?" *Journal of HealthCare Information Management, Vol. 15, No. 3*, pp. 251-259.

DHHS (2001) *Final Privacy Regulation Text*, Department of Health and Human Services, http://aspe.hhs.gov/admnsimp/final/PvcTxt01.htm, last accessed July 2005.

DHHS (2005) "HHS Releases Report on Nationwide Health Information Exchange", Department of Health and Human Services Press Release of June 3, 2005, www.os.dhhs.gov/news/press/2005pres/20050603.html, last accessed July 2005.

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.

Duncan, Karen (1994) *Health Information and Health Reform,* Jossey-Bass: San Francisco, California.

Ely, J, J Osheroff, et al (1999) "Analysis of questions asked by family doctors regarding patient care" *British Medical Journal, Vol 319*, pp 358-361.

Etzioni, Amitai (1999) *The Limits of Privacy*, Basic Books: New York.

Evans R. Scott, David C. Classen, Stanley L. Pestotnik, et al., "Improving Empiric Antibiotic Selection Using Computer Decision Support," *Archives of Internal Medicine* 154(8):878-884, April 25, 1994.

Evans RS, Pestotnik SL, Classen DC et al (1997) "A computer assisted management program for antibiotics and other anti-infective agents" *New*

England Jr. Medicine, Vol. 338, No. 4, pp. 232-8.

Feld, Andrew (2005) "The Health Insurance Portability and Accountability Act (HIPAA): Its Broad Effect on Practice" *American Jr Gastroenterology, Vol 100, No. 7,* p 1440

Fogoros, Richard (2001) "Surviving the Health Care System" in *About Heart Disease* at http://heartdisease.about.com/library/ blhcs03.htm, last accessed July 2005.

Fox, Steven, William Gillespie, and Deborah Kohn (2001) "Vendor/Product Evaluations and Contract Negotiations under HIPAA" *Proceedings HIMSS'2001*, Workshop M, Health Information and Management Systems Society 2001 Annual Conference, New Orleans, LA February 2001.

Gambon, Jill (1996) "Data Warehouses in Pharmaceutical Companies" *InformationWeek, Issue 596*, September 09, 1996.

Gardner, E. (1989) "Finding a Strategy that does the Trick" *Modern Healthcare, Vol. 19, No. 27*, pp 28-52.

Goddard, Thomas G and Guy D'Adrea (1999) "PPO Accountability through Accreditation" in the *PPO Guide* published by American Accreditation Healthcare Commission, Washington, D.C.

Goldberg, Alan and Jocelyn Gordon (1999) *Telemedicine: Emerging Legal Issues, 2nd Edition*, American Health Lawyers Association Publishers: Washington, D.C.

Grove, Andrew (1996) *Only the Paranoid Survive; How to Exploit the Crisis Points, that Challenge every Company and Career*; Bantam Books.

Haidar, Tracy (2002) "CMS versus BCBS, Fraud, and Staff" report posted to the graduate course in health care information systems IFSM 661c at University of Maryland, Baltimore County, March 2002.

Hannah, K J and Marion Ball (2000) *Nursing Informatics: Where Caring and Technology Meet, 3rd edition*, Springer-Verlag: New York.

HCPro (2002) "Two all-digital hospitals in the works" *Healthcare IT Weekly, Vol. 1 No. 3*, May 27, 2002

Heeks, Richard, David Mundy, and Angel Salazar (2000) "Understanding Success and Failure of Health Care Information Systems" pp 96-128 in *HealthCare Information Systems; Challenges of the New Millenium* edited by Adi Armoni, Idea Group Publishing: Hershey, USA.

Hellerstein, David (1999) "HIPAA's Impact on Healthcare" *Health Management Technology, Vol. 20, Issue 3,* p10-15.

Huynh, Minh and Sal Angihothri (2000) "Healthcare Process Redesign: A Case Study" pp 27-49 in *HealthCare Information Systems; Challenges of the New Millenium* edited by Adi Armoni, Idea Group Publishing: Hershey, USA.

Kaushal, Rainu and Bates, David (2001) "Chapter 6. Computerized Physician Order Entry (CPOE) with Clinical Decision Support Systems (CDSSs)" in *Evidence Report/Technology Assessment, No. 43 Making Health Care Safer: A Critical Analysis of Patient Safety Practices*, published in Nov. 2001, available at http://www.ahcpr.gov/clinic/ptsafety/, last accessed July 2005.

Kim, Anya, Marion C. Meissner, Lance J. Hoffman, Jeff Collmann, Seong K. Mun (1997) "Risk Analysis of Electronic Renal Care Patient Management System" CPRI Toolkit, Section 4.5.2 Case Study: Project Phoenix - Risk Management Plan, available from www.himss.org/CPRIToolkit/html/4.5.2.html, last accessed July 2005.

Kissinger, Kerry and Sandra Borchardt, Editors (1996) *Information Technology for Integrated Health Systems: Positioning for the Future*, from the Ernst & Young Information Management Series, John Wiley & Sons: New York.

Kock, Linda (1991) "Nursing's Relationship with Information System Vendors" in *HealthCare Information Management Systems*, ed. Marion Ball, et al, pp 125-131, Springer-Verlag: New York.

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/.

Krabbel, Anita, Ingrid Wetzel, Sabine Ratuski (1996) "Participation of Heterogeneous User Groups: Providing an Integrated Hospital Information System" in J. Blomberg, F. Kensing, E. Dykstra-Erickson (Eds.): *PDC'96 Proceedings of the Participatory Design Conference*, Cambridge, Massachusetts, November 1996, pp. 241-249.

Labor Bureau (2004) "Career Guide to Industries: Health Services" Bureau of Labor Statistics, U.S. Department of Labor, http://www.bls.gov/oco/cg/cgs035.htm, last accessed July 2005.

Langabeer, Jim (2005) "The Evolving Role of Supply Chain Management Technology in Healthcare" *Jr. Healthcare Information Management*, V. 19, No. 2, pp 27-33.

Le, Yen (2001) “The Healthcare Informatics 100” *Healthcare Informatics* June 2001, p 35-76 also available at www.healthcare-informatics.com.

Lindberg, Donald (1979) *The Growth of Medical Information Systems in the United States*, Lexington Books: Lexington Massachusetts.

Lindberg, Donald (1990) “In Praise of Computing” in *A History of Medical Informatics* edited by B Blum and K Duncan, ACM Press, New York, New York, p 4-12.

Lindsey, Bonnie (1980) *The Administrative Medical Assistant*, Robert Brady Company: Bowie, Maryland.

Lionberger, H F (1960) *Adoption of New Ideas and Practices*, Iowa State University Press: Ames, Iowa.

Lissman,T and Boehnlein, J (2001) “A Critical Review of Internet Information about Depression” *Psychiatric Services, Vol. 52*, pp 1046-1050.

17.2 M-Z

Marin, K.D., M.P. Ramos, L.A. Santos, and D. Ancao-Sigulem (1994) "Expert System in Prenatal Care: Validation and Implementation," in Susan J. Grobe and Elly S.P. Pluyter-Wenting, eds., *Nursing Informatics: An International Overview for Nursing in a Technological Era*, Elsevier: Amsterdam.

Mattingly, Rozella (1997) *Management of Health Information: Functions & Applications*, Delmar Publishers: Albany, New York.

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.

Miller, R. A., H. E. Pople, and J D Myers (1992) “INTERNIST-1, an experimental computer based diagnostic consultant for general internal medicine”, *New England Journal of Medicine, Volume 307*, pp 468-476.

Mills, Mary Etta and Sharon O’Keefe (1991) “Computerization: A Challenge in Nursing Administration” in *HealthCare Information Management Systems*, ed. Marion Ball, et al, pp 103-113, Springer-Verlag: New York.

Mintzberg, Henry (1979) *The Structuring of Organizations*, Prentice Hall.

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.

Mulrow, C, Cook, D, et al (1997) Systematic Reviews: Crticial Links in the Great Chain of Evidence” *Annals of Internal Medicine, Vol 126*, pp. 389-391.

Murray, Christopher (2001) "The World Health Organization programme to measure health systems performance, and how it can help governments in improving performance" in *OECD Health Conference on Performance Measurement and Reporting*, 5-7 November 2001, Ottawa, Canada.

National Committee for Quality Assurance (1997) *A Road Map for Information Systems: Evolving Systems to Support Performance Measurement* Washington, DC.

NCVHS (2000) *Report on Uniform Data Standards for Patient Medical Record Information*, National Committee on Vital and Health Statistics, July 6, 2000 http://www.ncvhs.hhs.gov/

NHCAA (2005) “Health Care Fraud: A Serious and Costly Reality for all Americans” National Healthcare Anti-Fraud Association, http://www.nhcaa.org/, last accessed July 2005.

Nightengale, Florence (1863) *Notes on Hospitals, 3rd Edition*, Longman, Green, and Company: London, England.

NIST (1996) *Generally Accepted Principles and Practices for Securing Information Technology Systems*, National Institute of Standards and Technology, *Special Publication 800-14,* September 1996, available for free download from http://csrc.nist.gov/publications/nistpubs/.

NIST (2001) *Underlying Technical Models for Information Technology Security*, National Institute of Standards and Technology (NIST), *Special Publication 800-33,* December 2001, available for free download from http://csrc.nist.gov/publications/nistpubs/.

NIST (2002) “Risk Management Guide for Information Technology Systems” NIST SP 800-30 chapters 3 and 4, January 2002.

Noss, Brian and Richard Zall (2002) “A Review of CHIN Initiatives: What Works and Why”, *Jr. Healthcare Information Management, Vol. 16, No. 2*, pp 35-39.

Odorisio, L (1999) “Imaging and Workflow” *Inform, Vol. 13, Number 2*, pp 40-42.

Paramore, Miriam (2001) “Permitted Disclosures under GLB and HIPAA” presented Oct. 25, 2001 at the *Third National HIPAA Summit* at the Grand Hyatt Hotel in Washington, D.C. available at www.hipaasummit.com/ past3/agenda/day2.html, last accessed July 2005.

Payne, Velma and Joan Kiel (2005) “Web-based Communication to Enhance Outcomes: A Case Study in Patient Relations” *Jr. Healthcare*

Information Management, V. 19, No. 2, pp 56-63.

Rada, Roy (1993) "Standards: the Language for Success" *Communications of the ACM, 36, 12* pp 17-18.

Rada, Roy (2001) "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, George S Carson, Chris Haynes (1994) "Standards: the Role of Consensus" *Communications of the ACM, 37, 3* pp 15-16, April 1994.

Rada, Roy, Pieter Zanstra, Jan Potharst, Judith Barlow, Pieter de Vries Robbe, Djujan Bijstra (1990) Expertext for Medical Care and Literature Retrieval, *Artificial Intelligence in Medicine, 2, 6*, pp. 341-355

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.

Reschke, Elaine (1980) *The Medical Office: Organization and Management*, Harper & Row: New York.

Roemer, Milton (1992) "National Health Systems throughout the World" in *An Introduction to the U.S. Health Care System, 3rd Edition*, edited by Steven Jonas, pp 169-190, Springer Publishing Company: New York.

Ross, David (1998) "Information Network for Public Health Officials: Addressing the need for a public health information infrastructure" http://www.nlm.nih.gov/nichsr/pres/mla98/ross/tsld001.htm, last accessed July 2005.

Ross, Sheri, Marilyn Gore, Wes Radulski, Ann Warnock-Matheron, and Kathryn Hanna (1991) "Nursing's Role in Defining Systems" in *HealthCare Information Management Systems*, ed. Marion Ball, et al, pp 114-124, Springer-Verlag: New York.

Ross SE, J Todd J, LA Moore, BL Beaty, L Wittevrongel, C Lin (2005) "Expectations of Patients and Physicians Regarding Patient-Accessible Medical Records" *J Med Internet Res* 7(2):e13

Rundle, Rhonda (2000) "E-Commerce Coming To Health-Care Industry" *Wall Street Journal*, February 28, 2000. p B4.

Ryckman, Douglas (1991) "Financial Systems: Trends and Strategies" in *HealthCare Information Management Systems*, ed. Marion Ball, pp 209-220, Springer-Verlag: New York.

Ruffin, Marshall de Graffenried Junior (1999) *Digital Doctors,* American College of Health Executives: Tampa, Florida.

Safran, Charles, David M. Rind, Roger B. Davis (1996) "Effects of a Knowledge-Based Electronic Patient Record on Adherence to Practice Guidelines" *M.D. Computing, Vol. 13, No. 1*, pp. 55-63, January-February 1996.

Schriner, Maureen (1998) "Who's Growing CIOs?" *Healthcare Informatics*, November 1998, www.healthcare-informatics.com/issues/1998/11_98/cios.htm, last accessed July 2005.

Schwartz, L, Woloshin, S, et al (2002) "Media Coverage of Scientific Meetings: Too Much, Too Soon?" *Journal of the American Medical Association, Vol. 287*, pp 2859-2863.

Schwartz, W. B., (1970) "Medicine and the Computer: The Promise and Problems of Change," *New Engl. J. Medicine, Vol. 283*, pp 1257-1264.

Shortliffe, E H (1976) *Computer-based Medical Consultations: MYCIN*, Elsevier Scientific Publishers: New York.

Shortliffe, Edward, Leslie Perreault, Geo Weiderhold, and Lawrence Fagan editors (2000) *Medical Informatics: Computer Applications in Health Care and Biomedicine, 2nd Edition*, Springer-Verlag: New York.

Sittig, Dean (1999) "Chief Medical Information Officer" *The Informatics Review: e-journal of the Association of Medical Directors of Information Systems*, available at www.informatics-review.com/jobdesc/sample3.htm, last accessed July 2005.

Smith, Jack (2000) *Health Management Information Systems: A Handbook for Decision-Makers*, Open University Press: Buckingham, England.

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.

Stegwee R.A., P.J.B. Lagendijk (2001), Health Care Information and Communication Standards Framework, in: R.A. Stegwee & T.A.M. Spil, *Strategies for Health care Information Systems*, Idea Group Publishing: Hershey, PA.

Szolovits, P. (1982) "Artificial Intelligence and Medicine" Chapter 1 in Szolovits, P. (Ed.) *Artificial Intelligence in Medicine*, Westview Press: Boulder, Colorado.

Tan, Joseph (2000) *Health Management Information Systems: Methods and Practical Applications , 2nd Edition*, Aspen Publications: Gaithersburg, Maryland.

Taylor, H (2002) *Cyberchondrias Update. Harris Interactive*. http://www.harrisinteractive. Com/harris_poll/, last accessed July 2005.

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.

Torrens, Paul (1993) "Historical Evolution and Overview of Health Care Systems in the United States" pp 1-28, in *Introduction to Health Services* edited by S. Williams and P Torrens, Delmar Publishers: Albany, New York.

Torrens, Paul and Stephen Williams (1993) "Understanding the Present, Planning for the Future: The Dynamics of Health Care in the United States in the 1990s" pp 421-429 in *Introduction to Health Services* edited by S. Williams and P Torrens, Delmar Publishers: Albany, New York.

Tranbarger, Russell (1991) "Nurses and Computers: At the Point of Care" in *HealthCare Information Management Systems*, ed. Marion Ball, et al, pp 95-102, Springer-Verlag: New York.

Ummel, Stephen (2003) "An Interview with Stephen Ummel, Principal Cap Gemini Ernst & Young Health Consulting" *Journal of Healthcare Information Management, Vol. 17, No. 1*, pp. 27-30.

Walston, S. L. and J R Kimberly (1997) "Reengineering Hospitals: Evidence from the Field" *Hospitals and Health Services Administration, Vol. 42, No. 2*, pp 143-163.

Warner, Homer (1979) *Computer-Assisted Medical Decision-Making*, Academic Press: New York.

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 www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html, last accessed July 2005).

WEDI (2005) *Bringing Partners Together: Successful EDI Testing and Validation Practices*; released June 2005 by Workgroup for Electronic Data Interchange: Reston, VA, accessible from www.wedi.org, last accessed July 2005.

Wessen, Albert (1999) "The Comparative Study of Health Care Reform" in *Health Care Systems in Transition: An International Perspective* edited by Francis Powell and Albert Wessen, pp 3-25, Sage Publications: Thousand Oaks, California.

Wetzel, Ingrid (2001) "Information Systems Development with Anticipation of Change Focusing on Professional Bureaucracies" *Proc. of Hawai'i International Conference on System Sciences, HICCS-34*, Maui, January 2001. also available at http://swt-www.informatik.uni-hamburg.de/publications/details.php?id=177, last accessed July 2005.

Wiederhold, Gio and Leslie Perreault (1990) "Clinical Research Systems" in *Medical Informatics: Computer Applications in Health Care* pp 503-535, edited by E. Shortliffe, L. Perreault, G. Wiederhold, and L. Fagan, Addison-Wesley Publishing: Reading, Massachusetts.

Williams H., F. Li, J. Whalley (2000), Interoperability and Electronic Commerce: A New Policy Framework for Evaluating Strategic Options*, JCMC 5 (3)*

Worthley, John (2000) *Managing Information in Healthcare: Concepts and Cases,* Health Administration Press of College of Healthcare Executives: Chicago, Illinois.

18 Index of Terms

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

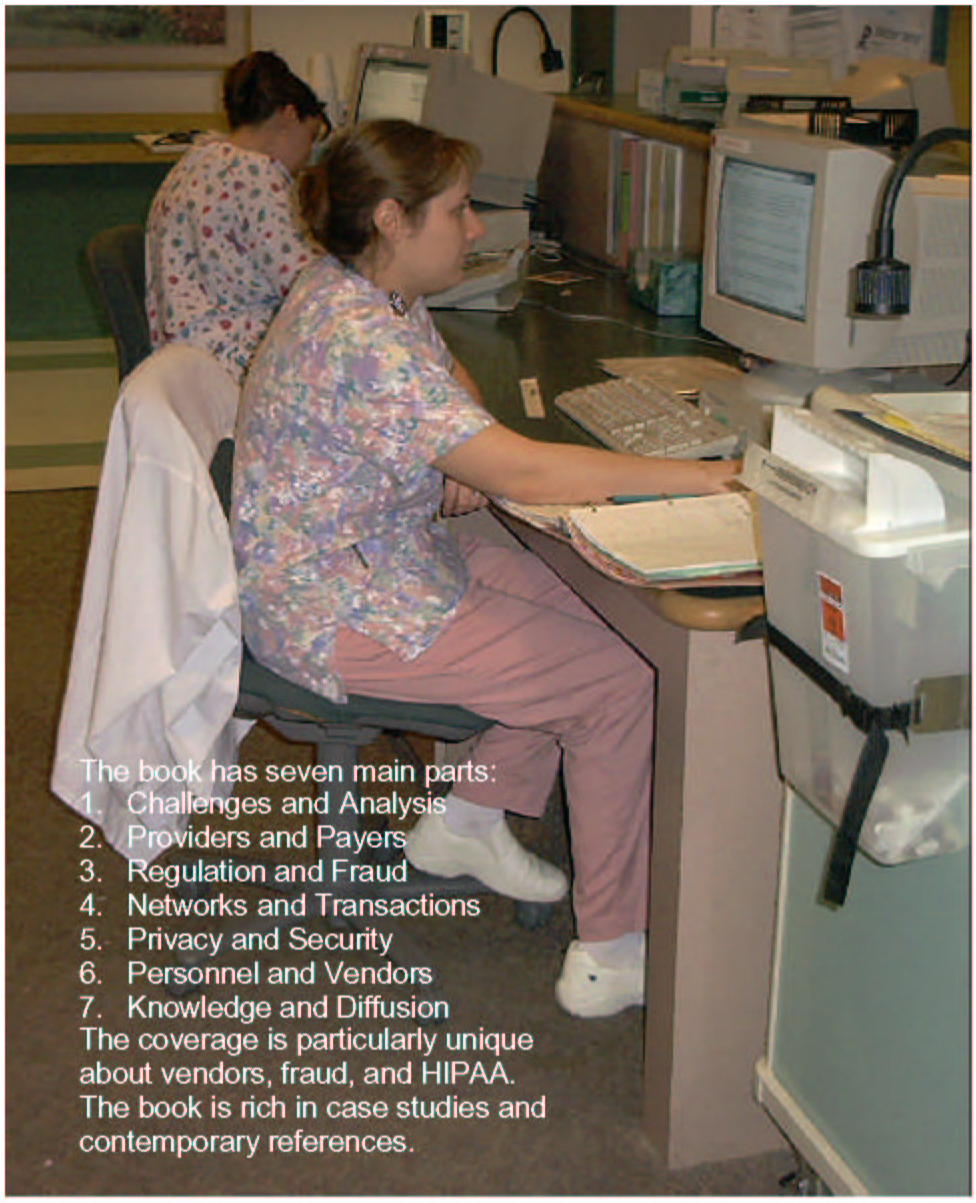
S

T

U

V

W



Interesting subject matter that presented a great deal of new information to me. … I've recommend your material to many others.

Bruce Yelovich
Systems Librarian
Mount Saint Mary's College

I alloted extra time because of the learning value. My work experience is mainly technical. This helps me clarify the requirements, design, and implementation of healthcare information systems.

Kin Ung, CISSP
Information Security
pharmaceutical industry

... gave new insight to another industry. The subject matter is important -- patients, providers, payers, policies -- and sparked an interest in a career path that I had not considered.

Information Systems for Health Care Enterprises, 3rd Edition introduces health care information systems to students of information systems or health care administration or for professionals responsible for information systems in health care.

The author **Roy Rada, M.D., Ph.D.**, has been researching and consulting in health care informatics for over a quarter of a century. He is a professor of information systems at the University of Maryland, Baltimore County

Hypermedia Solutions Limited

ISBN 190185726-3
90000>
9 781901 857269