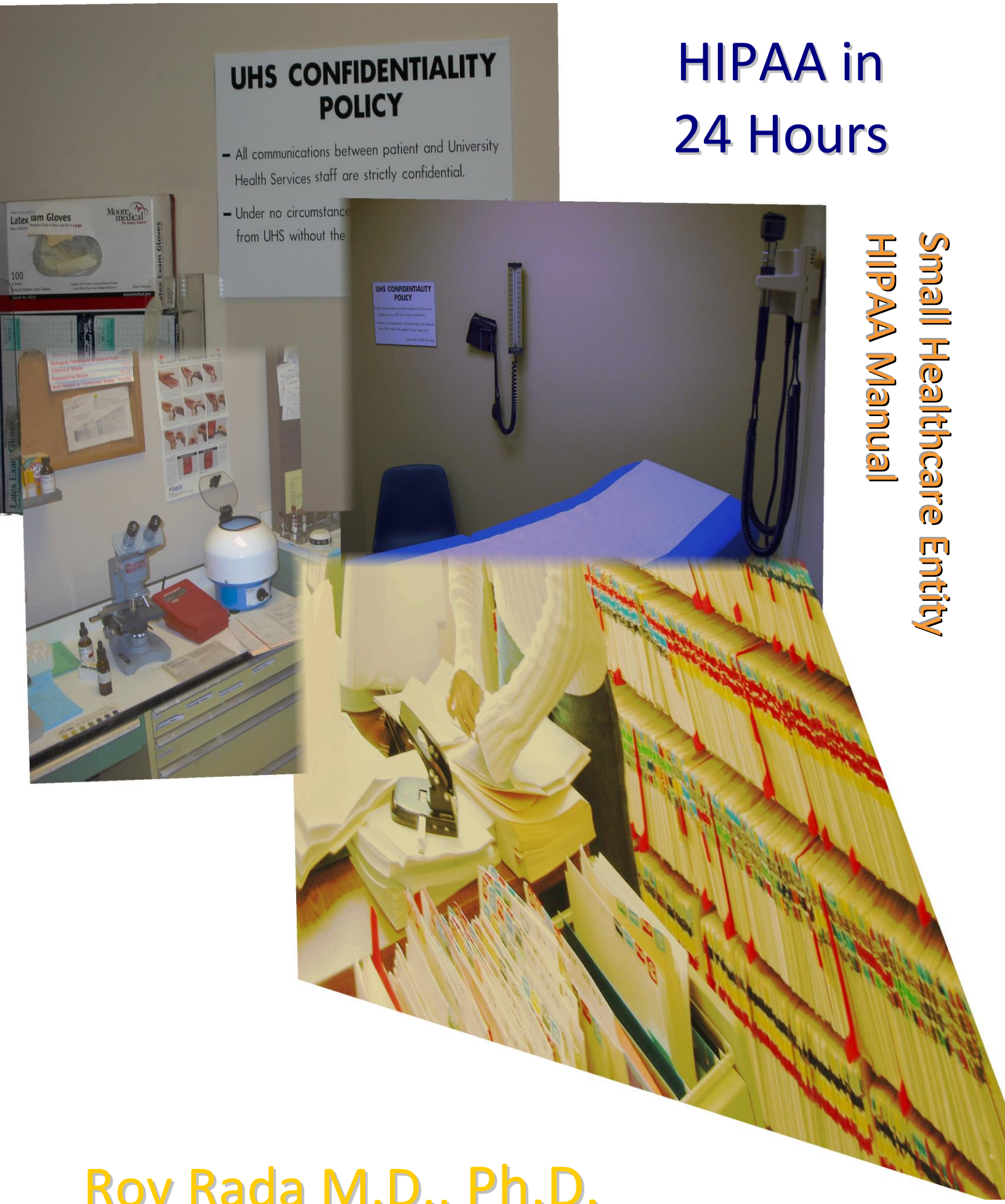
HIPAA in 24 Hours

Small Healthcare Entity HIPAA Manual



Roy Rada M.D., Ph.D.

Published by: **HIPAA-IT LLC**
Electronic copies available at **www.hipaa-it.com**

British Library Cataloguing (in process)

Rada, R. (Roy), 1951-

Title: *HIPAA in 24 Hours: Small Healthcare Entity HIPAA Manual*
ISBN: 1-901857-11-5

For further information, please contact:
- email rada@hipaa-it.com
- web www.hipaa-it.com
- phone 410-747-6712
- surface mail 18 Anderson Ridge, Baltimore, MD 21228

Printed December 2002

This manual does not constitute legal advice and bears no guarantee of compliance with the law. The law itself and interpretations of it may change with time. The user agrees to indemnify or hold harmless the author or publisher from any claims arising from the use of this manual.

1 Why Read this Manual?

The Health Insurance Portability and Accountability Act (HIPAA) demands change in health care provider-payer transactions and privacy. HIPAA standardizes the transactions between providers and payers and encourages them to be electronic; one could call this part of HIPAA the electronic commerce or ecommerce part. The Privacy Rule affects the way health care professionals communicate and the rights of patients. HIPAA applies to health care providers large and small, but this manual addresses the small provider.

The compliant entity will be rewarded with:

- Monetary gain through faster, cleaner electronic claims and
- Increased patient satisfaction through demonstration of the practice's respect for the confidentiality of the patient's record.

Non-standard claims may not be paid and may generate fines, and violating confidentiality can result in fines and prison terms. Compliance efforts should be underway.

In this do-it-yourself, simple compliance aid for HIPAA's privacy and ecommerce requirements, the forms, policies, procedures, spreadsheets, training material, audit tables, and contracts support a compliance program that reduces distractions for the staff, while increasing service to the patient. Small providers can not afford more than a few hours of their staff time, and HIPAA compliance must be relatively easy. The Privacy Rule recognizes the need for small entities to have different approaches from large entities. Small entities should agree on an approach to HIPAA and thus proactively define their 'standard of care'. Following this Manual, the small healthcare entity can implement a HIPAA compliance program in 24 hours – therein the title 'HIPAA in 24 Hours'.

Users of the manual have said:

- *HIPAA in 24 Hours* is the best HIPAA manual possible. The information is just what is needed -- put in easy-to-read, understandable terms with great sample forms and other helpful aids. *Donna Rieck, R.N., M.H.A., Des Moines, Iowa*
- I'm following *HIPAA in 24 Hours* very closely and besides being highly readable, it is very, very helpful. I've just had to do some adapting because of our particular office situation. *Teresa Gutierrez, L.I.S.W., Cleveland, Ohio*
- The *Manual* was very helpful. *Nicholas Nossaman, M.D., Family Practitioner, Denver, Colorado*

The Copic Insurance newsletter (www.callcopic.com) recommends *HIPAA in 24 Hours* to its readers. As a reflection of its popularity, the *Manual* is an Amazon HIPAA best seller.

.

2 Table of Contents

3 The Compliance Life Cycle

Compliance involves these essential steps:

- Awareness,
- Implementation, and
- Eternal vigilance.

As the entity may be unlikely to proactively initiate HIPAA compliance activities, other organizations might help. The local hospital, the state medical association, the health plan, or some other such entity might take the responsibility to send this simple manual (or one like it) to the entity with a cover letter inviting the chief to read the following 'Chief Awareness Essay'.

3.1 Chief Awareness Essay

Budget reforms and legal minefields challenge the practice of medicine. The latest challenge comes in the form of HIPAA's Administrative Simplification provisions. They have been headline news in the past few years and rightfully so.

Administrative Simplification started with an aborted effort by the health care industry to reduce the confusion in provider-payer transactions. Over 400 different forms and many variations on codes to complete the fields in the forms are used. The overhead costs to the industry are enormous. After years of trying unsuccessfully to standardize these transactions, the industry asked the government to intervene.

These transactions cover eligibility inquiries, claims, claims attachments, remittance advice, and more. Standardization of these transactions should mean that doctors get fewer inquiries from payers about what was meant and that the time from a claim to a remittance should reduce.

What does the private practice need to do to benefit from this bonanza of transaction standards? The practice needs to either adopt the new formats and codes or allow its billing service or clearinghouse to convert the practice's traditional forms into the standard. Since the new standard may require slightly different information at times from that expected in the old forms, the practice may need to modify the information provided by the physician -- this should happen infrequently -- and may need to train the billing clerks to deal with the new requirements.

The other aspects of HIPAA's Administrative Simplification are less obviously a benefit to the private practice. When Congress realized that standardized, electronic, provider-payer transactions would become commonplace, Congress felt obligated to add privacy and security provisions to HIPAA.

The Privacy Rule reaches into the everyday activities of all people involved in health care. The Rule essentially puts a virtual lock on all protected health information and gives everyone with a decent reason to manipulate the information a virtual key. The parts of the Privacy Rule that typically concern the small practice are described next.

Patients should acknowledge receipt of a Notice of Privacy Practices. The Notice explains that anyone involved in treatment, payment, or healthcare operations may benefit from the medical record relatively unencumbered. Authorization from the patient is typically required, if any disclosure is to be made for other than health care reasons.

The Minimum Necessary portion of the Privacy Rule asks that a staff person try not to read information about a patient when that information has no impact on the staff person's ability to serve the patient. In integrated delivery networks, 'Minimum Necessary' could mean that the receptionist working from a computer terminal is not supposed

to see the online, patient's lab results. However, the government recognizes that the small practice is based on paper records, and that the entire patient record goes from desk to desk. In the small practice all employees may handle the entire record because nothing else is practical to do.

The Privacy Rule strengthens patient rights. The patient has a right to a copy of the patient record, and the clinic can only charge the cost of providing the copy. The patient may request to add an amendment to the record. If the doctor refuses, then among other things the doctor must note in the record that an amendment was requested but refused. Finally, for those cases were disclosures are permissible and are made without explicit patient authorization, the clinic must keep track of those disclosures, and if the patient requests an accounting of those disclosures, the clinic must provide such an accounting. All these things can be practically accomplished with the paper record and straightforward procedures.

Finally, the Privacy Rule calls for the following four administrative adjustments:

- The clinic must identify a person who wears the additional hat of 'privacy officer'. This officer might be the 'office manager' who wears multiple hats anyhow.
- A policy must be adopted that describes how the clinic handles patient information.
- All staff must be trained. This can be accomplished by a brief seminar for all staff or by having staff read appropriate training manuals.
- Safeguards must be implemented to secure information. For instance, medical records could be locked in cabinets before the night cleaning crew arrives or the cleaning crew could be instructed in the importance of not browsing the medical records.

The Privacy Rule is not asking for anything beyond what some would consider common sense. Most practices already do most of the things requested by the Privacy Rule. However, through the pressures of everyday practice executives may have made decisions in the name of expedient, quality care that now need to be further tempered with concern for privacy.

The keys to success with HIPAA for the small entity are two-fold:

- First, the chief has to convey to the staff both explicitly and implicitly that standardization and privacy are important -- without this commitment, compliance with HIPAA will be impossible.
- Second, the entity should turn to its community of peers for a 'standard of care'. The various forms, manuals, policies, and other documents should be relatively the same for any given type of entity. Adopting these materials will make the job of compliance relatively easy.

The catchword is 'flexibility'. The government explicitly asks that small entities have far less complex compliance programs than large entities.

This essay does not cover the full detail of HIPAA's Administrative Simplification. The busy chief is not expected to become intimate with the rules but to understand their overlying principles and to oversee the entity's management accordingly. Please take this manual and ask your office manager to implement it with your full blessing.

3.2 Implementation

After the chief reads the *awareness essay* and is convinced of the merits of a simple HIPAA compliance program, the chief should pass this manual to the office manager. In the remainder of this subsection, forms or policies that appear in this manual are indicated in italics. The office manager

1. studies the manual's entire content

2. tailors the *Notice of Privacy Practices*, *authorization form*, *staff training essay*, and *employee confidentiality form* to the particular practice, and
3. calls a meeting of the office staff.

At the staff meeting the *staff training essay* is read. Then staff are asked to read and sign the *employee confidentiality form*. The form is subsequently included in the employee's personnel record. The *record of training progress* is updated to note that staff at the meeting have been trained.

The office manager creates a folder in the front office and places the *Privacy Notice* and *authorization forms* there. The receptionist is told to check for each registering patient whether or not the patient has acknowledged receipt of the *Notice of Privacy Practice*. If not, then the patient should be given the Notice of Privacy Practices and asked to sign an acknowledgement form. The signed acknowledgement form is placed in the medical record beside the patient's insurance information.

The *fax policy* is posted beside the fax machine. Anyone engaged in email with protected health information is given the *email policy*. When issues of *authorizations*, *access*, *amendment*, *accounting*, or *restrictions* arise, the office manager is contacted.

The office manager will complete the table "Entities Receiving Protected Health Information" to record all entities that receive protected health information (see 'Glossary'). Vendors that are used for legal, actuarial, accounting, consulting, management, administrative accreditation, data aggregation, transcription, or financial services, can be given individually identifiable health information, if those vendors sign *business associate contracts* with the practice. Otherwise, the practice needs to get *authorization* to release the information to the vendor. The office manager will negotiate the *business associate contracts* with the vendors. Completed contracts are noted in the *table of business associate contracts*.

For the ecommerce portion of HIPAA, the office manager should have applied by October 16, 2002 for an extension to the compliance deadline. The enclosed *letter to clearinghouse or vendors* should be addressed and sent.

3.3 Eternal Vigilance

Every quarter the Office Manager should review the status of compliance. A spot check of medical records should be done to confirm that any new patients seen in the quarter have acknowledged receipt of the Notice of Privacy Practices. The various tables recording authorizations and patient rights are reviewed for timeliness. If any new staff have appeared in the quarter, then they should be trained. The table of entities receiving protected health information is compared with the table of *business associate contracts*, and any discrepancies are resolved. This documentation of performance must be continually maintained.

3.4 Timeline

The implementation phase involves:

- Week 1: Chief reads Chief Awareness Essay, passes manual to Office Manager, and appoints Office Manager as Privacy Officer – time 1 hour.
- Week 2: Office Manager studies manual and tailors forms and writes to clearinghouse/vendors – time 4 hours
- Week 3: Office Manager convenes 1 hour meeting of staff – 2 hours of Office Manager and 1 hour of everyone else.
- Week 4: Forms and policies placed in various folders in the practice and staff specifically trained on responsibility vis-à-vis the forms and policies – 2 hours of Office Manager and half hour of everyone else.
- Week 5: Contracts with external entities are collected and assessed as to whether protected health information is involved and whether or not business associate contracts are required – 2 hours of Office Manager
- Week 6: Amend contracts that require business associate clauses – 3 hours.

Total time invested in first 6 weeks:

- Chief: 1 hour
- Office Manager: 13 hours
- Assistants: 1.5 hours

For an entity with 2 senior providers (such as physicians) and 4 assistants, this would mean a total time commitment of (2 * 1) + 13 + (4*1.5) hours = 21 hours.

After implementation, the maintenance effort for privacy compliance depends largely on the frequency with which patient's request special actions. Experts agree that patients are unlikely to frequently take advantage of the opportunities presented them under the privacy rule. If a small entity has 1,000 patients, then one might speculate that 10 will ask for a copy of their record in one year and only 1 will request an amendment or an accounting of disclosures. The need to create new or different business associate contracts or train new employees should happen infrequently. The training of new employees can be a few minutes of the new employee orientation. In total, one hour per quarter may suffice for maintenance of privacy compliance. Thus, in the first year the 21 hours for implementation and the 3 hours of maintenance lead to a total in the first year of 24 hours. In subsequent years, maintenance of compliance would take 4 hours per year.

4 Privacy

Compliance with the Privacy Rule is basically a matter of policy and procedures which are appropriately implemented through time. Protected health information (see 'Glossary') should be handled with care. The Table "Privacy Gap Analysis" lists questions.

Privacy Gap Analysis			
Do you have?		***Yes***	***No***
Patient Rights			
	Authorization Form		
	Notice of Privacy Practices		
	Access and Amend Policy		
	Account and Restrict Policy		
Communication			
	Phone, Email, Fax Policy		
	Medical Record Use Guidelines		
Administration			
	Privacy Officer		
	Business Associate Contract		
	Documenting Behavior		
	Safeguards		
	Staff Training		

The following subsections provide the forms, policies, and procedures to support a privacy compliance program.

4.1 Patient Rights

Editorial Note: Forms and policies, such as presented here, are mandatory under the Privacy Rule.

Patients should be given a 'Notice of Privacy Practices' and should acknowledge receipt of same. Authorization forms should be completed for non-routine use of protected health information. Patients have the right to

- Access their health record,
- Request an amendment of their record,
- Receive an accounting of certain disclosures made of their record, and
- Request restriction on use and on method of communicating.

Forms and policies to support the aforesaid are next.

4.1.1 Notice of Privacy Practices

Editorial Note: Each entity must provide a notice of HIPAA privacy practices to its patients. The Notice can have two layers with the first layer giving essentials and the second layer elaborating. The entity is required to demonstrate a good faith effort to get the patient's signed acknowledgement of receiving the Notice.

PROVIDER NOTICE
OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY. Layer one is brief, and further details are provided in layer two.

Uses and Disclosures: We use health information about you for treatment, to obtain payment for treatment, for administrative purposes, and to evaluate the quality of care that you receive. Continuity of care is part of treatment and your records may be shared with other providers to whom you are referred. Information may be shared by paper mail, electronic mail, fax, or other methods. We may use or disclose identifiable health information about you without your authorization in several situations, but beyond those situations, we will ask for your written authorization before using or disclosing any identifiable health information about you.

Your rights: In most cases, you have the right to look at or get a copy of health information about you. If you request copies, we will charge you only normal photocopy fees. You also have the right to receive a list of certain types of disclosures of your information that we made. If you believe that information in your record is incorrect, you have the right to request that we correct the existing information.

Complaints: If you are concerned that we have violated your privacy rights, or you disagree with a decision we made about access to your records, you may contact the person listed below. You also may send a written complaint to the U.S. Department of Health and Human Services. The person listed below can provide you with the appropriate address upon request.

Our legal duty: We are required by law to protect the privacy of your information, provide this notice about our information practices, follow the information practices that are described in this notice, and seek your acknowledgement of receipt of this notice. Before we make a significant change in our policies, we will change our notice and post the new notice in the waiting area. You can also request a copy of our notice at any time. For more information about our privacy practices, contact the person listed below.

If you have any questions or complaints, please contact:
Office Manager: _____
Address: _____
Phone: _____

……

Acknowledgement of receipt of Notice of Privacy Practices:

Please sign your name and print your name and date on this acknowledgement form. Then detach the form from the Notice along the dotted line and return your signed acknowledgement to the receptionist or to the address above.

Signature: _____
Printed name: _____
Date: _____

Second layer:
For further details about your rights and the federal Privacy Rule, you might read the second layer. [The reader of this manual can go to the Appendix to see the second layer].

4.1.2 Authorization Form

AUTHORIZATION for RELEASE of INFORMATION

I hereby authorize the use or disclosure of my individually identifiable health information as described below. I understand that this authorization is voluntary. I understand that if the organization authorized to receive the information is not a health plan or healthcare provider, the released information may no longer be protected by federal privacy regulations.

Patient name: _____

ID number: _____

Persons/organizations providing the information: _____

Persons/organizations receiving the information: _____

Specific description of information (includes dates): _____

What is the purpose of the use or disclosure? _____

I understand that my healthcare and the payment for my healthcare will not be affected by my signing this form.

I understand that I may see and copy the information described on this form if I ask for it, and that I get a copy of this form after I sign it.

I understand that this authorization will expire on __/__/__ (DD/MM/YR)

I understand that I may revoke this authorization at any time by notifying the providing organization in writing, but if I do, it won't have any affect on any actions they took before they received the revocation.

Signature of patient or patient's representative: _____

Date: _____

Printed name of patient's representative: _____

Relationship to the patient: _____

- You may refuse to sign this authorization
- You may not use this form to release information for treatment or payment except when the information to be released is psychotherapy notes or certain research information.

END of AUTHORIZATION

4.1.3 Access and Amendment Policy

Editorial Note: This policy and procedure would be part of the entity's documentation. Patients might be referred to this information in the Privacy Notice. Some of the choices made in the following are not mandatory. For instance, the entity could require that requests be only in writing. The intent here is to be as accommodating to the patient as practical.

Access Right

We give patients access to their health information whether we or our business associates hold that information and whether or not we were the source of the information. Exceptions to this access occur rarely, such as when the information is deemed dangerous. If we feel we need to deny access, we provide an explanation. Sometimes the patient can contest this denial, and then we will have a third party review the situation.

The patient may request access verbally or in writing, and we will record the request in a log book. We typically have 30 days in which to provide the information. We will charge the patient the cost of photocopying.

Amendment Right

The patient may request verbally or in writing that we amend our records about the patient. We will log the patient request and reply within 60 days. We may deny the patient request, if we were not the originators of the information or we believe the information is accurate.

When we make an amendment, we add a note to the record to indicate the change but do not delete the original information. If we deny the patient request, then we provide an explanation to the patient and in the record. The patient may contest our denial and among other things we will document the patient concerns in the record.

4.1.4 Accounting and Restrictions Policy

Editorial Note: Patients have numerous rights that the entity should observe. Again, the Privacy Rule provides options not all detailed here, but the description here gives the benefit to the patient each time. For instance, under 'disclosures' the policy here allows the patient to request in writing or verbally, but the Privacy Rule would allow the entity to require that all requests are in writing.

Accounting of Disclosures

The patient has a right to receive an accounting of certain disclosures of the patient's protected health information. The patient's request may occur in writing on verbally and we will record the request in our log. We have 60 days to respond. Our accounting to the patient will:

- Be in writing,
- Include the dates of disclosure and to whom the information was sent,
- Describe what information was sent, and
- State the purpose of the disclosure.

Only a very restricted set of disclosures are tracked, of which an example is a report of a positive test result to a public health agency. Disclosures are not subject to the accounting requirement when:

- for treatment, payment, or health care operations;
- made with patient authorization;
- covered by a business associate agreement;
- for national security or intelligence purposes; or
- to correctional institutions or law enforcement officials.

In any given 12-month period, we will provide one accounting at no cost. The accounting only covers disclosures since Privacy Rule Compliance was required.

Restrictions on Use and Disclosure

The patient may request restrictions on our use or disclosure of the patient's protected health information beyond those restrictions already imposed by the government. We may elect to accept the restriction or not. However, if we accept the request, then we must abide by it and could only reverse our position after notifying the patient appropriately first.

Restrictions on Communication Method

We will accommodate a request that we communicate with the patient by alternative means, if we can practically implement such an alternative. The patient is not required to explain why he or she wants such an alternative means of communication. Our agreement with the patient for an alternative communication channel will be documented and included in the patient's medical record.

4.2 Communication

Editorial Note: The policies suggested here are NOT mandatory for the entity. The Privacy Rule requires that an entity handle communication carefully and document that care. The communication policies in this subsection are simply illustrative.

The Privacy Rule requires policy on dealing with protected health information but is not specific. An entity might have policy on how it handles correspondence in email, fax, phone, or face-to-face mode. The medical record is an important medium of communication, and the 'minimum necessary' sharing should occur.

4.2.1 Phone and Face-to-Face

When patients are brought into the consulting room to see the doctor or nurse their consultation is private -- behind closed doors. However, in the reception area the patient is in the presence of others who do not have a need to know the patient's private details. Staff should not give information about a patient to another person without the patient's permission. The same principle applies to the phone. When staff contact the patient for reminders about appointments they should take reasonable steps to avoid conveying protected health information to other than the patient or patient guardian.

4.2.2 Email Policy

Editorial Note: An email policy is not required by the Privacy Rule. This draft policy indicates what an email policy could be. For an entity that does not use email, having an email policy is of course NOT necessary.

Ownership and User Privacy of E-Mail

Use of electronic mail is a part of <ENTITY> business processes. All e-mail originating within or received into <ENTITY> is the property of <ENTITY>.

Confidentiality of Electronic Mail

When e-mail is used for communication of individually identifiable health information:

- A notation referring to the confidential nature of the information should be made in the subject line.
- The information is to be distributed only to those with a legitimate need to know.

Retention of Electronic Mail

Often, e-mail messages are non-vital and may be discarded routinely. However, some e-mail may be considered a formal record and should be retained. For instance, all clinically relevant e-mail messages, including the full text of a patient's query, as well as the reply, should be stored in the patient's medical record.

Provider/Patient Use of E-mail

The patient should acknowledge these conditions for email use:

- E-mail communication is a convenience and not appropriate for emergencies or time-sensitive issues.
- No one can guarantee the privacy of e-mail messages. Employers generally have the right to access any e-mail received or sent by a person at work.

4.2.3 Fax Policy

The Privacy Rule does not specifically allow or prohibit facsimile transmission. Each covered entity is responsible to have a reasonable policy given its circumstances.

Sending

Faxing is fast and efficient from the viewpoint of the sender. Copies do not have to be made because originals can be fed into the machine. The major liability is misdirection. Many states restrict the faxing of certain types of health information, such as information relating to AIDS, HIV, or behavioral health services. Every fax should have a cover page that specifies the addressee and sender and includes a confidentiality notice something like this:

> This telecopy transmission contains confidential information belonging to the sender that is legally privileged. This information is intended only for the use of the individual or entity named above. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this telecopy in error, please notify the sender immediately to arrange for return of these documents.

Receiving

Faxing is NOT efficient on the receiving end. Fax machines are routinely shared by many people and typically installed in a centralized, high traffic area. As transmissions print out open face, confidentiality is difficult to maintain. Thus, for each fax machine a specific staff person is responsible to

- Remove documents promptly
- Notify senders of problems
- Follow the instructions on the cover page

The office manager has oversight responsibility that all fax machines are appropriately monitored.

4.2.4 De-identification

The Privacy Rule applies to 'individually identifiable health information' and not to de-identified information. The Rule says that you can share a de-identified record with anyone anytime for any reason. The following identifiers of the individual or of relatives must be removed: names; addresses, dates, telephone/fax numbers, internet addresses, social security numbers, medical record numbers, account numbers, device numbers, photographs or fingerprints, and any other unique identifying number, characteristic, or code.

4.2.5 Medical Records

In addition to guidelines about communication, the entity should have guidelines about the handling of medical records regardless of whether they stay on paper or are communicated via phone, face-to-face, email, or fax. If the structure of the medical record makes it likely that some staff may see information that they do not need to see, training should be provided to guide that staff to ignore that information. The Privacy Rule specifies a 'Minimum Necessary Standard' which expects that people should use only the information that they need. For a small entity, one could say that everyone should be allowed and expected to see everything. For a larger entity, one might indicate that in the normal situation, the entity would expect responsibilities as indicated in the table "Roles to Information" and elaborated in the corresponding diagram.

Table "Roles to Information"	
Role	Information
Chief	everything
Assistant	health care
Receptionist	front office
Information Manager	back office

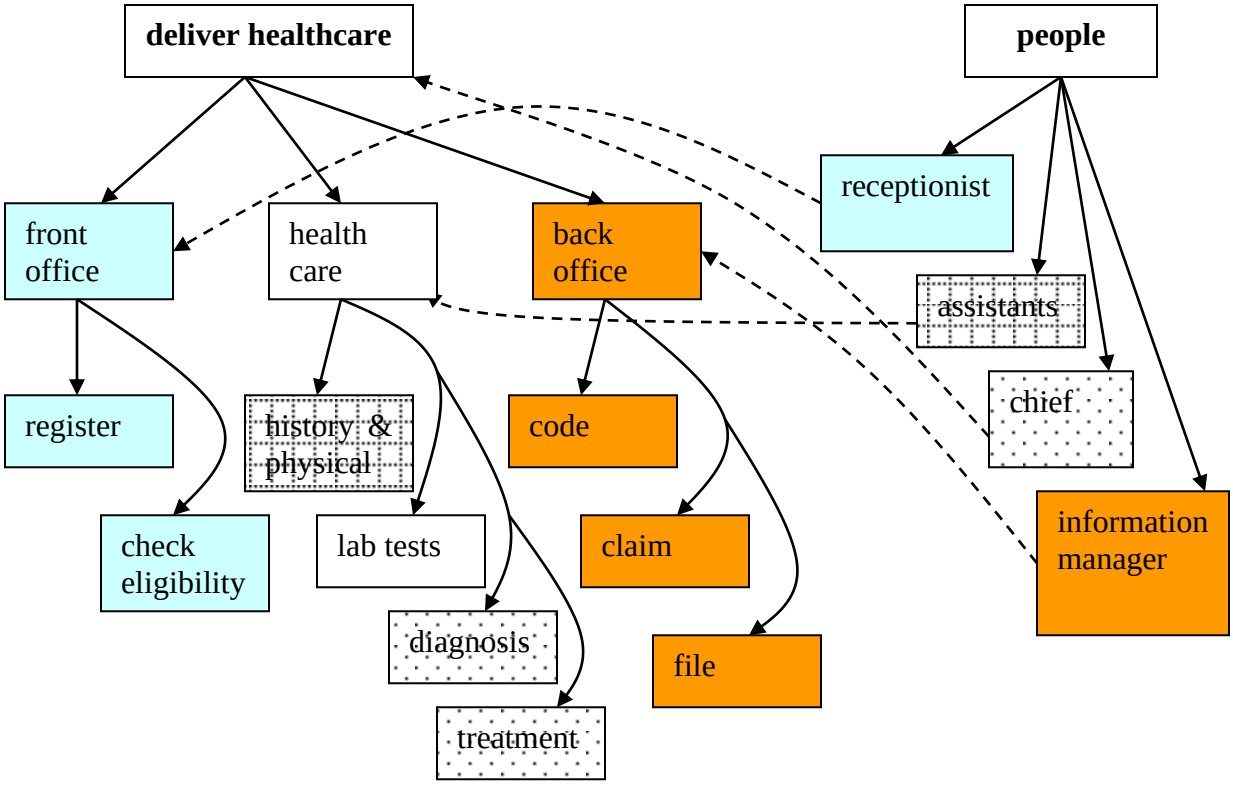


Figure "Roles to Information": The functions of a physician group practice are depicted in the left-hand tree -- three major functions of 'front office', 'health care', and 'back office' are shown. The roles of the people are shown in the right-hand of the diagram. Each person in a role is expected to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

4.3 Administration

The Privacy Rule requires that

- Someone in the practice be the privacy officer,
- Sharing of information via the business associate relationship be accompanied by an appropriate contract,
- Performance is tracked, and sanctions are in place for violators of policy,
- Policies and procedures are documented,
- Information is safeguarded,
- State laws stricter than the Privacy Rule pre-empt the Privacy Rule, and
- All staff be trained on privacy,

Guidelines, contracts, and tables that support the above requirements are next.

4.3.1 Privacy Officer

Editorial Note: The Privacy Rule does not designate who must serve as the Privacy Officer, qualifications for the Privacy Officer, or how the Privacy Officer performs his or her functions. For a small group physician practice, the most likely person to wear the hat of 'Privacy Officer' is the Office Manager.

The Privacy Officer responsibilities listed in the Privacy Rule are:

- Establish and implement privacy policies [this manual provides such],
- Receive complaints and provide guidance on making further complaints and provide information about privacy,
- Oversee training,
- Ensure that safeguards are in place,
- Establish and apply sanctions for privacy misbehavior,
- Mitigate harmful effects of wrongful disclosures, and
- Ensure that a copy is maintained for 6 years of all relevant documentation of privacy efforts.

The Privacy Officer may, of course, wear other hats too.

4.3.2 Business Associate Privacy Contract

Editorial Note: You may disclose protected health information without explicit, patient authorization when a business associate relationship exists. Business associates are vendors that provide legal, accounting, management, accreditation, or transcription services for you with your patients' protected health information You do not need a business associate agreement with a vendor that only incidentally sees protected health information; for instance, the cleaning service or the computer maintenance company only see protected health information incidentally, and you do not ask for a business associate contract with them. A business associate privacy contract is provided next. The covered entity might modify an existing contract with the business associate to accommodate the requirements here or use this business associate privacy contract in its entirety as a separate agreement. After the contract are examples of relationships requiring and not requiring business associate contracts are presented next.

START OF BUSINESS ASSOCIATE CONTRACT

THIS CONTRACT is entered into on this _____ day of _____ between _____ ("ENTITY") and _____ ("ASSOCIATE").

WHEREAS, ENTITY will make available to ASSOCIATE certain Information that is confidential and must be afforded special treatment and protection.
WHEREAS, ASSOCIATE will have access to and/or receive from ENTITY certain Information that can be used or disclosed only in accordance with this Contract and the Department of Health and Human Services (HHS) Privacy Regulations.

NOW, THEREFORE, ENTITY and ASSOCIATE agree as follows:

1. The term of this Contract shall commence as of _____ (the "Effective Date"), and shall expire when all of the Information provided by ENTITY to ASSOCIATE is destroyed or returned to ENTITY.
2. The Parties hereby agree that ASSOCIATE shall be permitted to use and/or disclose Information provided or made available from ENTITY for the following stated purposes:

   _____
   _____
   _____

3. ASSOCIATE OBLIGATIONS:
   a. ASSOCIATE hereby agrees that the Information provided or made available by ENTITY shall not be further used or disclosed other than as permitted or required by the Contract or as required by law and that appropriate safeguards will be in place
   b. ASSOCIATE hereby agrees that it shall report to ENTITY within two (2) days of discovery any use or disclosure of Information not provided for or allowed by this Contract.
   c. ASSOCIATE hereby agrees that anytime Information is provided or made available to any subcontractors or agents, ASSOCIATE must enter into a subcontract with the subcontractor or agent that contains the same terms, conditions and restrictions on the use and disclosure of Information as contained in this Contract.

d. ASSOCIATE hereby agrees to make available and provide a right of access to Information by an Individual, to make Information available for amendment and to incorporate any amendments to Information, and to provide an accounting of disclosures in accordance with the Privacy Rule.
e. ASSOCIATE hereby agrees to make its internal practices, books, and records relating to the use or disclosure of Information received from, or created or received by ASSOCIATE on behalf of the ENTITY, available to HHS for purposes of determining compliance with the HHS Privacy Regulations.
f. ASSOCIATE agrees to have procedures in place for mitigating, to the maximum extent practicable, any deleterious effect from the use or disclosure of Information in a manner contrary to this Contract or the HHS Privacy Regulations.

4. ASSOCIATE agrees that ENTITY has the right to immediately terminate this Contract and seek relief if ENTITY determines that ASSOCIATE has violated this Contract.

IN WITNESS WHEREOF, ASSOCIATE and ENTITY have caused this Contract to be signed and delivered by their duly authorized representatives, as of the date set forth above.
ASSOCIATE
By:_____
Print Name:_____
Title:_____
ENTITY
By:_____
Print Name:_____
Title:_____

END OF BUSINESS ASSOCIATE CONTRACT

Examples of relationships that should include a business associate contract are:

- A CPA firm using protected health information while providing accounting services to a health care provider,
- An attorney whose legal services to a health plan involve access to protected health information,
- A consultant that performs utilization reviews for a hospital,
- A healthcare clearinghouse that translates and transmits a claim from a health care provider to a payer,
- An independent medical transcriptionist that provides transcription services to a physician, and
- A pharmacy benefits manager that manages a health plan's pharmacist network.

Information can be shared WITHOUT business associate contracts when information is shared for treatment purposes. Thus, a hospital needs NO business associate contract with the specialist to whom it refers a patient. Likewise, a physician needs NO business associate contract to send a specimen to a lab. Information can also be shared WITHOUT business associate contracts when:

- a health care provider discloses protected health information to a health plan for payment purposes,
- vendors, such as janitorial services or electricians, access protected health information incidentally,

- an entity is a conduit for protected health information, such as the US Postal Service, or
- a financial institution processes financial transactions for payment for health care.

4.3.3 Tracking

The Privacy Rule requires an entity to have policies to implement the objectives of the Rule. Furthermore, the entity must document that its behavior is consistent with its policy. One way to document this behavior is to record in tables the compliant activities. The Privacy Rule does not detail how the tracking should be done but the following tables serve the purpose.

Exceptional disclosures, as described in the earlier policy section, should be recorded in a table called "Disclosures". Such a table is useful because the office must be prepared to provide an accounting of these 'exceptional' disclosures.

Exceptional Disclosures for Patient _____ FOR EACH PATIENT RECORD			
Date	To whom Sent	What was Sent	Purpose

Another table would list all requests for access, amendment, accounting of disclosures, and restrictions, the date of the request, and the date the request was satisfied.

Requests for access, amendment, accounting of disclosures, or restrictions ONE TABLE FOR CENTRAL OFFICE (not in each patient record)			
Patient Name	Date of Request	Date Satisfied	Details of Request

The office staff can search the table to find all occurrences of a request by a particular person or the requests in a given time period. If a patient requests an accounting of disclosures for the second time in the same year, then the office would charge for the accounting.

For the purposes of arranging business associate contracts, the clinic might first record all entities that receive its protected health information:

Entities Receiving Protected Health Information			
Name of Entity	Type of Information Shared	Purpose of Sharing	Business Associate? Yes or No

When in doubt as to whether or not an entity is a business associate, the office manager should decide that the entity is not a business associate (and that patient authorizations rather than

business associate contracts are required). For those arrangements that fall under the conditions for business associate contracts, another table is maintained of "Business Associate Contracts":

Business Associate Contracts		
Name of Entity	Contact Address	Date of Contract

For management and compliance purposes, a table might list each member of the small healthcare entity, what material they studied, and when (see Table "Privacy Training").

Privacy Training			
	Date Completed		
Person's Name	Chief's Essay	Staff's Essay	Entire Manual

An employee confidentiality form is not mandated by the Privacy Rule. However, an employee confidentiality form might be used by an entity as part of its documentation of its ongoing effort to encourage staff to respect privacy. The signed form would be stored in the employee's personnel file.

Employee Confidentiality Form

Security and confidentiality is a matter of concern for all persons who have access to (ENTITY) information. Each person accessing (ENTITY) data and resources holds a position of trust relative to this information and must recognize the responsibilities entrusted in preserving the security and confidentiality of this information. Therefore, all persons who are authorized to access data and resources must read and comply with (ENTITY) policy. Violators may be subject to penalties, including disciplinary action, under policies of (ENTITY) and under laws of the State of (STATE NAME). By signing this, I agree that I have read, understand and will comply with the Agreement.

_____
Signature/Date

_____
Printed Name

4.3.4 Safeguards

The Privacy Rule includes a paragraph about safeguards. A draft Security Rule has been published and identifies physical, administrative, and technical security. Physical security is the common sense that we would use for our home; for instance:

- Doors should be locked when no one is inside.
- Patient records should be stored in such a way that guests are unlikely to see protected health information of someone else.

Administrative security is how the organization works. For instance, terminated employees must return their keys. Technical security involves the machines. For instance,

- Protected health information that is transmitted on the Internet might be better secured when encrypted. Encryption is, however, not a requirement of the Privacy Rule. If you want encryption, then tell your vendor you would like it to be provided at no extra cost to you. If your vendor is not willing to provide that and you are otherwise satisfied with your vendor, then continue as you are.
- If physicians or other staff access protected health information across the Internet or by phoning to a modem somewhere, then this access should be password protected (again your vendor should provide at no further cost to you a password feature).

For the small entity, vendors supporting the technical infrastructure should provide at no extra cost basic technical security, which should, in turn, be enough to satisfy the Privacy Rule.

4.3.5 State Pre-emption

The regulation of health care has often involved a balance between state and federal authority. The Privacy Rule pre-empts state law, except in the case that the state law is more stringent. A law is 'more stringent' when it 'provides greater privacy protection'.

If a state has law that significantly pre-empts HIPAA, then one can typically find information about the state law on the World Wide Web. An excellent source of information about state laws versus HIPAA's Privacy Rule is the Health Privacy Project of Georgetown University accessible at www.healthprivacy.org -- there is a complete listing state-by-state of the privacy law of that state.

4.3.6 Training

Editorial Note: Training can be different for the doctor and the other staff. The essay entitled "Chief Awareness" is 1,000-words long and addresses the requirements of HIPAA's Administrative Simplification from a top-level view. The 600-word essay entitled "Training for Staff" is intended to be read by the staff. The entity's training program could be based on assigning the non-professional staff to read the essay "Staff Training" and the chiefs to read "Chief Awareness". Further training for the Office Manager could be realized by requiring that person to read this manual.

Staff Training Essay

All staff are involved in protecting health information. Staff should be aware of the penalties that could be levied against them by the Federal government. Fines reaching $250,000 and imprisonment can be imposed on physicians, practice managers, receptionists, medical assistants, or nurses. Untrained staff may not realize that respecting privacy is important. All staff are required to undergo training on privacy.

When patients are brought into the consulting room to see the doctor or nurse their consultation is private - behind closed doors. Patients expect privacy. However, at reception the patient's privacy is sometimes compromised. For example, a receptionist might loudly ask the patient in a waiting room

- what condition do you have,
- how did you spell your name, or
- what is your address?

How many patients want to announce that they have VD? Or the receptionist might confer with a hospital on the telephone regarding a patient's condition when the receptionist can be heard by patients in the waiting room. Receptionists should not give information about a patient to another person, even to another member of the patient's family, without the patient's permission.

In addition, to constraints on communicating so that a patient's privacy is respected, the receptionist must strive to arrange the work place so as to support confidentiality. For instance, computer screens should not point towards the reception hatch or counter because patients might then see others' records.

Patients' paper records should be stored safely and not left in hallways with public access. Likewise, patient details should not be left on public bulletin boards. Records should be shredded, not left in the garbage.

Email, patient databases, or case letters should not be left on a computer screen for all to read while the operator makes a cup of coffee. If staff find medical records unattended, then they should return the records to the supervisor or doctor. If a member of staff overhears other staff conferring regarding patients' health information, then the staff concerned should be reminded that they can be overheard and also reminded of the office policy on privacy. If medical staff want to discuss patient information and contractors are in the room, then the medical staff should ask the contractors to leave the room. If the contractors' job is critical and the contractors can not leave the room, then the medical staff should leave the room and conduct their conversations of this nature in another area.

Only the necessary information should be transmitted by email, as one can never be sure who has access to the practice's email. Staff should take care to send email to the right address – a patient might not appreciate their mental health notes being sent to strangers! Staff should never share computer passwords or leave the password where someone can see it. Diskettes containing patient information should not normally be taken home.

All members of a small practice staff are involved in a patient's care in some way, but not everyone has to read everything in the patient's case notes. In small communities where everyone knows everybody else, staff may be intrigued to know their neighbor's business. For example, the nurse and the receptionist are excited to read the case notes of a candidate for Mayor of their small town – the receptionist's uncle is running against this patient in the Mayoral race – need one say more!

Staff should report abuses of patient privacy and should not fear retaliation for whistle blowing -- they are not only protecting themselves from a lawsuit but they are also protecting the practice.

5 Ecommerce

HIPAA's Administrative Simplification provisions were prompted by the desire to reduce administrative overhead in provider-payer transactions. By having one form for each type of transaction, the chances of doing the transactions electronically and semi-automating the processing are improved. The HIPAA, standardized, electronic transactions include claims, remittances, eligibility, claims status, and referrals (see Figure "HIPAA Transactions").

This section provides

- a spreadsheet that can be used to compute the reduction in labor of an electronic processing of transactions,
- a draft letter to be sent to clearinghouses or vendors to get an update on their status vis-à-vis using standard HIPAA transactions, and
- indications of an impact on coding.

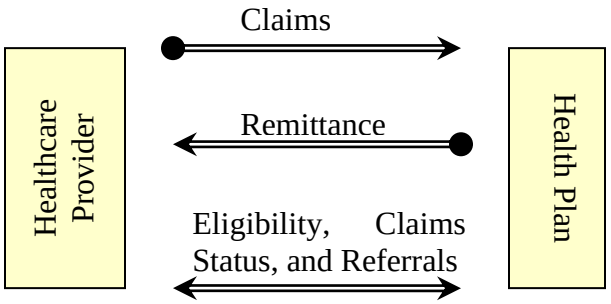


Figure "HIPAA Transactions": The indicated transactions must be done in standard format. The pointed arrow indicates a direction for the transaction.

The pre-October 16, 2002 version of this manual included a completed application to request an extension to the compliance deadline but the government no longer solicits these applications.

In checklist form the questions are:

Ecommerce Checklist		
Have you	Yes	No
Analyzed business efficiency?		
Checked vendor compliance?		
Determined code gap?		

5.1 Ecommerce Benefits

One advantage to electronic transactions is a saving in time. 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.

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. A detailed, interactive spreadsheet with further values is provided next.

If you have the Microsoft Word 2002 version of this document, then you can modify the values in the fields and get new results. Enter whatever you want into the 'General Practice Information' and 'Amount of Time Spent to' fields. Then select any 'Yearly Cost Estimates' fields (shaded in green) and depress the F9 key to get an updated computation. To determine the savings from a reduction in bad debt, enter the values for the current bad debt and the expected bad debt after automation in the next to last row. Then select the last cell and depress F9.

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

If you do not have a Word 2002 version of this document and want to create your own spreadsheet, then the formulas you want are illustrated by the following:

- 16b. Eligibility verification is eligibility checks per week * minutes spent on eligibility * 52 weeks * staff costs per hour/ 60 minutes per hour = 6b * 10b * 52 * 5b / 60.
- 21b. Yearly Costs is 16b + 17b + 18b + 19b + 20b.
- 25. Yearly Profit from Debt Reduction is (24a - 24b) * 3b * 4b * 52.

5.2 Letter to Clearinghouse or Vendor

If the clinic uses the services of at least one clearinghouse, the clinic must learn what this clearinghouse is doing to assure that transactions will be HIPAA-compliant. Vendors supporting billing operations should be asked what they plan to do to assure that transactions are in the correct X12 format and that codes in the forms are from the appropriate code sets. *A sample letter to send to a clearinghouse or vendor follows*.

RE: **Changes for the Transactions Rule of the Health Insurance Portability and Accountability Act (HIPAA)**

To whom it may concern,

[ENTITY] is studying the changes that will be required for the electronic transactions that are standardized by HIPAA. Please explain:

- your timeline to address each of the transaction changes required by HIPAA and
- what you expect the practice to do in order to work effectively with you to achieve compliance with HIPAA?

Thank you for your continued cooperation as we meet the requirements of HIPAA.

Sincerely,

Office Manager

5.3 Codes

The new standards do impose constraints on field values that might entail a small change in data collection processes. For instance, the claim must now state the date of the last menstrual period of a pregnant woman or the nationality of a patient. If this data was not previously collected, then the clinic may need to start collecting that data. In the coding of diagnoses, procedures, or treatments, if local codes (see 'Glossary') are used, they must be replaced with a standard code.

6 Conclusion

HIPAA's ecommerce provisions were designed to help care providers get prompt payments from payers. The privacy provisions were designed to help patients feel comfortable that their health records were well managed. The small health care entity has much to gain by the correct approach to HIPAA.

The approach to HIPAA by multi-hospital networks or large health plans should naturally be different from the approach of small entities. Furthermore, small entities should share approaches so that they can both

- avoid re-inventing the wheel and
- help establish the specifics of the standard appropriate to small practices.

Some might look at some of the policies in this manual and suggest elaborations. For instance, in the policy on access to records, this manual says that the practice will try to comply within 30 days. The notice could be more elaborate in saying that the practice is obligated to reply within 30 days but that the first reply might be a notice that another 30 days will be required. The intention in this manual is to reduce complexity and to serve the best interests of the health care system. The HIPAA manual for a small entity should be small (see Figure "Hip").

Figure "Hip": The HIPAA (hip) manual ('ball') should fit into the entity work flow ('socket').

7 Appendix

7.1 Remainder of Privacy Notice

Editorial Note: This subsection of the Appendix provides the second and final layer of the Notice of Privacy Practices (for which the first layer was given in the body of this manual). In the mind of many experts, this extended notice is too long for the average individual to want to read, but the government has remained firm that the Notice should contain further details such as reflected in this second layer.

1. Uses and Disclosures of Protected Health Information

Following are examples of the types of uses and disclosures of your protected health care information that the provider is permitted to make. These examples are not meant to be exhaustive, but to describe the types of uses and disclosures.

Treatment: We will use and disclose your protected health information to provide, coordinate, or manage your health care and any related services. For example, your protected health information may be provided to a doctor to whom you have been referred to ensure that the doctor has the necessary information to diagnose or treat you.

Payment: Your protected health information will be used, as needed, in activities related to obtaining payment for your health care services. For example, obtaining approval for a hospital stay may require that your relevant protected health information be disclosed to your health insurance company to obtain approval for the hospital admission.

Healthcare Operations: We may use or disclose, as-needed, your protected health information in order to support our business activities. For example, when we review employee performance, we may need to look at what an employee has documented in your medical record.

Business Associates: We will share your protected health information with third party 'business associates' that perform various activities (e.g., billing, transcription services). Whenever an arrangement between us and a business associate involves the use or disclosure of your protected health information, we will have a written contract that contains terms that will protect the privacy of your protected health information.

Marketing: We may use or disclose certain health information in the course of providing you with information about treatment alternatives, health-related services, or fund-raising. You may contact us to request that these materials not be sent to you.

Written Authorization

Other uses and disclosures of your protected health information will be made only with your written authorization, unless otherwise permitted or required by law as described below. You may revoke this authorization, at any time, in writing.

Opportunity to Object

We may use and disclose your protected health information in the following instances. You have the opportunity to object. If you are not present or able to object, then your provider may, using professional judgment, determine whether the disclosure is in your best interest.

Facility Directories: Unless you object, we will use and disclose in our facility directory your name, the location at which you are receiving care, your condition (in general terms), and your religious affiliation. All of this information, except religious affiliation, will be disclosed to people that ask for you by name. Members of the clergy will be told your religious affiliation.

Others Involved in Your Healthcare: Unless you object, we may disclose to a member of your family, a relative, a close friend or any other person you identify, your protected health information that directly relates to that person's involvement in your health care.

Emergencies: In an emergency treatment situation, your provider shall try to provide you a Notice of Privacy Practices as soon as reasonably practicable after the delivery of treatment.

Communication Barriers: We may use and disclose your protected health information if your provider attempts to obtain acknowledgement from you of the Notice of Privacy Practices but is unable to do so due to substantial communication barriers and the provider determines, using professional judgment, that you would agree.

Without Opportunity to Object

We may use or disclose your protected health information in the following situations without your authorization or opportunity to object:

Public Health: for public health purposes to a public health authority or to a person who is at risk of contracting or spreading your disease.

Health Oversight: to a health oversight agency for activities authorized by law, such as audits, investigations, and inspections.

Abuse or Neglect: to an appropriate authority to report child abuse or neglect, if we believe that you have been a victim of abuse, neglect, or domestic violence.

Food and Drug Administration: as required by the Food and Drug Administration to track products.

Legal Proceedings: in the course of legal proceedings.

Law Enforcement: for law enforcement purposes, such as pertaining to victims of a crime or to prevent a crime.

Coroners, Funeral Directors, and Organ Donation: for the coroner, medical examiner, or funeral director to perform duties authorized by law and for organ donation purposes.

Research: to researchers when their research has been approved by an Institutional Review Board.

Soldiers, Inmates, and National Security: to military supervisors of Armed Forces personnel or to custodians of inmates, as necessary. Preserving national security may also necessitate sharing protected health information.

Workers' Compensation: to comply with workers' compensation laws.

Compliance: to the Department of Health and Human Services to investigate our compliance.

In general, we may use or disclose your protected health information as required by law and limited to the relevant requirements of the law.

2. Your Rights

Following is a statement of your rights with respect to your protected health information and a brief description of how you may exercise these rights.

You have the right to inspect and copy your protected health information. However, we may refuse to provide access to certain psychotherapy notes or information for a civil or criminal proceeding.

You have the right to request a restriction of your protected health information. You may ask us not to use or disclose certain parts of your protected health information for treatment, payment or healthcare operations. You may also request that information not be disclosed to family members or friends who may be involved in your care. Your request must state the specific restriction requested and to whom you want the restriction to apply. We are not required to agree to a restriction that you may request, but if we do agree, then we must behave accordingly.

You have the right to request to receive confidential communications from us by alternative means or at an alternative location. We will accommodate reasonable requests. We may also condition this accommodation by asking you for information as to how payment will be handled or specification of an alternative address or other method of contact. We will not request an explanation from you as to the basis for the request.

You may have the right to have your provider amend your protected health information. You may request an amendment of protected health information about you. If we deny your request for amendment, you have the right to file a statement of disagreement with us, and your medical record will note the disputed information.

You have the right to receive an accounting of certain disclosures we may have made. This right applies to disclosures for purposes other than treatment, payment or healthcare operations. It excludes disclosures we may have made to you, for a facility directory, to family members or friends involved in your care, or for notification purposes. You have the right to receive specific information regarding these disclosures. The right to receive this information is subject to certain exceptions, restrictions and limitations.

You have the right to obtain a paper copy of this notice from us, upon request, even if you have agreed to accept this notice electronically.

END of Second and Final Layer of Notice of Privacy Practices

7.2 Glossary

Covered Entity: A healthcare provider, a health plan, or a clearinghouse is a covered entity. HIPAA compliance is required of covered entities.

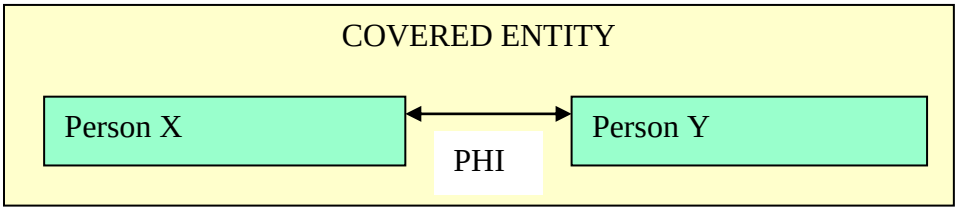
HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) was passed by the Congress in 1996. One of its five titles addressed administrative simplification, and within 'administrative simplification' we have the ecommerce and privacy requirements.

Individually identifiable health information: Any health information about a patient that includes the name, phone number, address, social security number, or other such identifier is considered 'individually identifiable health information'.

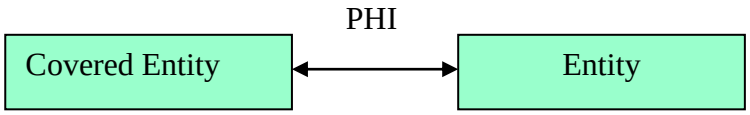
Local Codes: State Medicaid agencies and others have developed local codes. These local codes are not permitted under the HIPAA Transactions Rule.

Protected health information: 'Individually identifiable health information' in a covered entity that has at any time had any such information in electronic form.

Uses and Disclosures:



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



"Disclosure": The Covered Entity sends PHI to another Entity -- that is 'disclosure'.

The following diagram indicates when a business associate contract is appropriate as contrasted with an authorization.

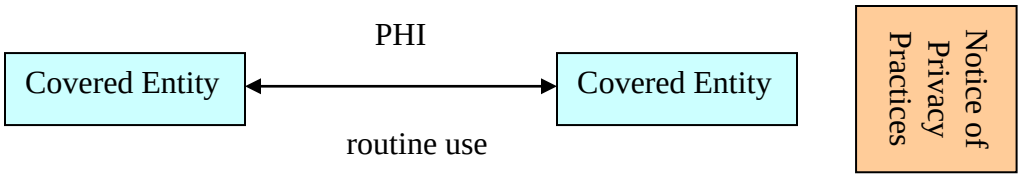


Figure "Routine Use": PHI is protected health information. Covered entities can share PHI for routine use (payment, treatment, and healthcare operations) after the patient acknowledges receipt of a Notice of Privacy Practices.

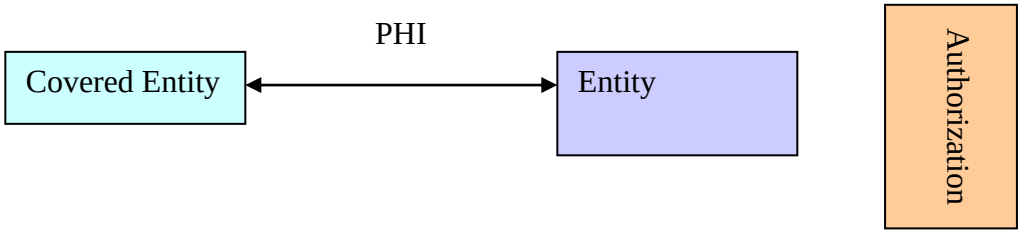


Figure "Authorization Required": A covered entity can send PHI to another entity with an authorization.

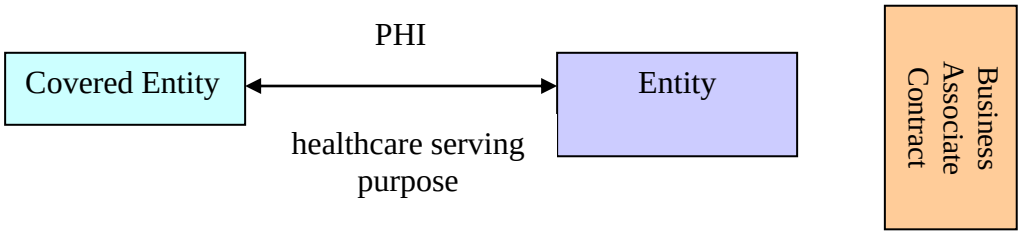
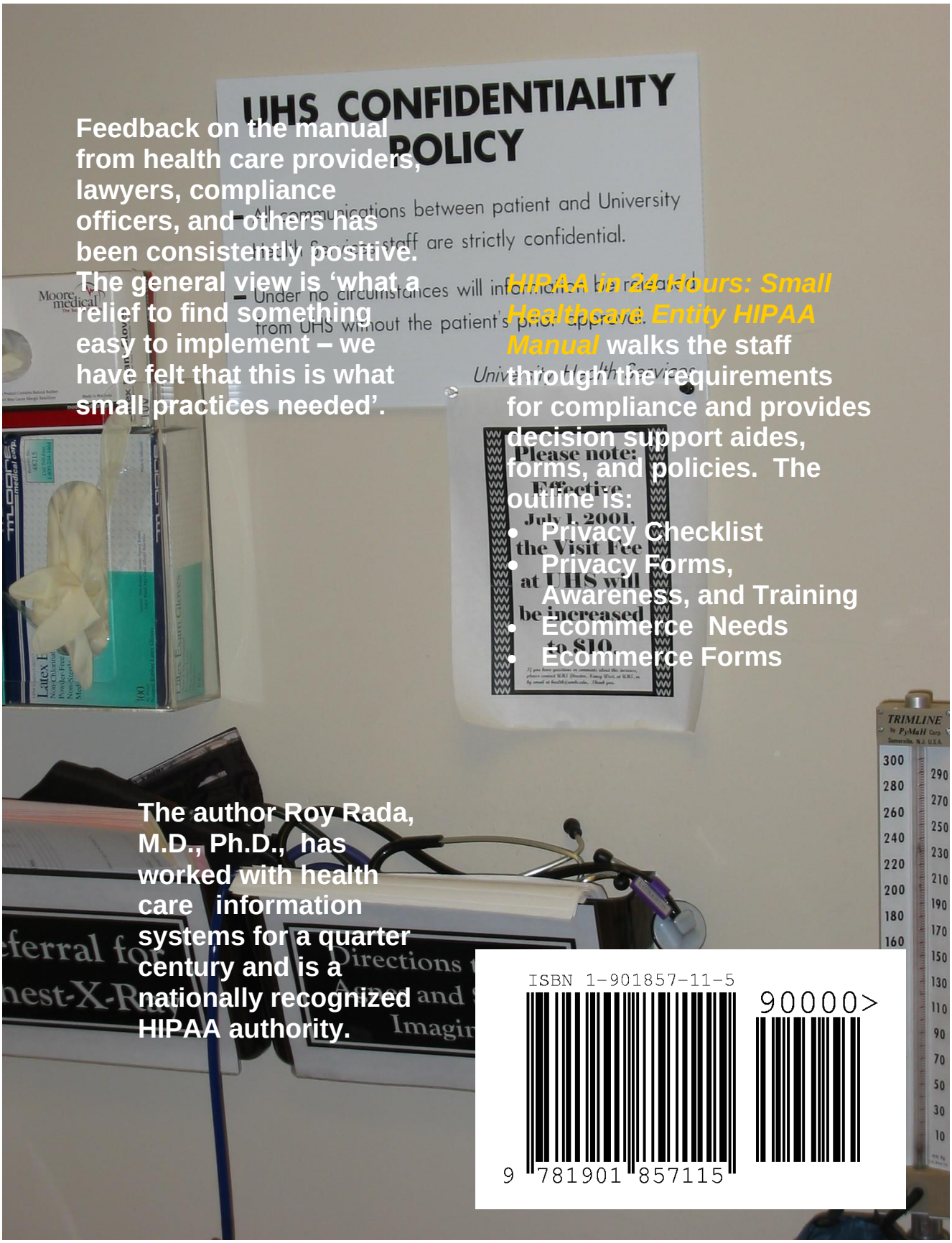


Figure "Business Associate": A covered entity can send PHI to any other entity for certain healthcare serving purposes when a 'business associate' contract has been signed.



Feedback on the manual from health care providers, lawyers, compliance officers, and others has been consistently positive. The general view is 'what a relief to find something easy to implement – we have felt that this is what small practices needed'.

HIPAA in 24 Hours: Small Healthcare Entity HIPAA Manual walks the staff through the requirements for compliance and provides decision support aides, forms, and policies. The outline is:

- Privacy Checklist
- Privacy Forms, Awareness, and Training
- Ecommerce Needs
- Ecommerce Forms

The author Roy Rada, M.D., Ph.D., has worked with health care information systems for a quarter century and is a nationally recognized HIPAA authority.

ISBN 1-901857-11-5
90000>
9 781901 857115