Chapter 2

The Health Insurance Portability and Accountability Act (HIPAA): Not All About Health Insurance

Joan M. Kiel, PhD, CHPS, *Chairman University HIPAA Compliance and Associate Professor HMS, Duquesne University, Pittsburgh, Pennsylvania*

Chapter Objectives

- Develop an understanding of the circumstances leading to the passage of Health Insurance Portability and Accountability Act (HIPAA) and the several purposes that HIPAA is intended to serve.
- Examine the portions of HIPAA that are most pertinent to working managers, specifically the significant sections of the second of the five titles of HIPAA referred to in legislation as Administrative Simplification.
- Facilitate familiarization with the rules applicable in the implementation of HIPAA.
- Define the manager's role relative to the HIPAA Privacy Rule and Security Rules.
- Review the responsibilities incumbent upon the organization for the implementation of HIPAA and its maintenance as standard operating procedure.
- Review the potential uses of personal patient health information by the organization and define the circumstances governing the release of such information.

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) is an important piece of federal legislation that has changed the way healthcare organizations do

business. When it was initially being debated, healthcare managers feared the worst, thinking of added expenses. They surmised that they would have to add staff, and they thought that patients would be upset. Through it all, healthcare managers have had to make adjustments in operations and keep abreast of HIPAA. This chapter details HIPAA and describes how a healthcare manager can successfully implement the pertinent portions of this law.

History and Rationale

What patients tell physicians can sometimes consist of some of the most confidential information that pertains to themselves. They tell it to physicians with the understanding that it will be used for their medical care and will not be passed on to others who are not involved in their care. Unfortunately, this essential confidentiality is not always observed. Consider the following examples: Information discussed by a physician and a physical therapist in a less-than-private setting is overheard by visitors leaving the adjacent office of a social worker; written information is left on a computer screen in an open nursing station when a nurse answers a call light; or information is used for financial gain when facts about a well-known patient is sold to a tabloid publication. Additionally, information stored electronically has the potential to be sent to many people with the click of a computer stroke, necessitating the implementation of security systems to prevent "healthcare hacking." Whether perpetrated purposefully or inadvertently, scenarios such as those discussed has led to federal legislation to protect patient health information.

HIPAA was enacted in part to protect the privacy, security, and confidentiality of patient health information. It also ensures secure transactions and assigns identifiers for providers, insurers, and patients to ease administrative transactions. HIPAA exists for both for the patient and the healthcare delivery system so that confidential information is utilized as it should be for the care of the patient and so that administrative transactions can be completed effectively and efficiently.

HIPAA, or Public Law 104-191, contains five titles addressing various areas of responsibility:

1. Healthcare Access, Portability, and Renewability
2. A. Preventing Healthcare Fraud and Abuse
   B. Medical Liability Reform
   C. Administrative Simplification
3. Tax-Related Health Provision
4. Group Health Plan Requirements
5. Revenue Offsets

Contained within the Administrative Simplification section of Title II are the three main areas that are pertinent to most healthcare managers: electronic data

interchange, which includes transactions, identifiers, and code sets; privacy; and security. To further delineate these three main areas, HIPAA is divided into 11 rules. It is from these rules that healthcare managers then develop policies and procedures to ensure compliance with the law.

The 11 Rules of HIPAA

The first portion of HIPAA, Transactions and Code Sets, was scheduled for compliance by October 16, 2002. As of October 16, 2009, just 6 of the 11 rules of HIPAA had been released for implementation with compliance dates. Thus, for healthcare managers, HIPAA implementation will be an ongoing process for some time to come. The 11 rules are as follows:

1. The **Claims Attachment Standards Rule** establishes national standards for the format and content of electronic claims attachment transactions (proposed in the September 23, 2005 Federal Register).
2. The **Clinical Data Rules/Electronic Signature Standard** establishes national standards for clinical data and data transmission.
3. The **Data Security Rule** establishes physical, technical, and administrative protocols for the security and integrity of electronic health data (April 20, 2005).
4. The **Enforcement Rule** establishes rules for how the government intends to enforce HIPAA (February 15, 2006).
5. The **Standard Transaction for First Report of Injury Rule** establishes national standards for the format and content of electronic first-report-of-injury transactions used in Workers' Compensation cases.
6. The **Standard Unique Identifier for Employers Rule** establishes the federal tax identification number as an employer's national unique identifier (July 30, 2004).
7. The **Unique Identifier for Individuals Rule** mandates a single patient identifier for all of an individual's patient health information.
8. The **Standard Unique National Health Plan/Payer Identifier Rule** establishes a national identifier for each health insurer.
9. The **Standard Unique Healthcare Provider Identifier Rule** establishes a national identifier for each provider (May 23, 2007).
10. The **Privacy Rule** establishes guidelines for the use and disclosure of patient health information (April 14, 2003).
11. The **Transactions and Code Sets Rule** establishes standard formats and coding of electronic claims and related transactions (October 16, 2002 or 2003).[1]

A Manager's Guide to the HIPAA Rules

As healthcare managers had just passed beyond the Y2K flurry of activity, the first rule of HIPAA, Transactions and Code Sets, was being released for implementation. The required implementation date was October 16, 2002, although covered entities were able to request a 1-year extension. As part of HIPAA's mission to ease electronic transactions, this rule focused on the development of standardized formats for electronic claims and their related transactions. HIPAA also specified what a HIPAA transaction was.

1. Healthcare claims or equivalent transactions
2. Healthcare payment and remittance advice
3. Coordination of benefits
4. Healthcare claim status
5. Enrollment and disenrollment in a health plan
6. Eligibility for a health plan
7. Health plan premium payments
8. Referral certification and authorization
9. First report of injury
10. Health claims attachments
11. Other transactions that the secretary may prescribe by regulation[2]

Healthcare managers need to be aware that as the revised *International Classification of Diseases (ICD-10)* is introduced (projected for Fall 2011), these transactions may undergo some changes. But all have the common objective of facilitating more accurate and efficient transactions.

The next rule to be implemented came with much fanfare (as opposed to the Transactions and Code Sets, which arrived quietly), as it impacted patients directly. With Transactions and Code Sets, patients do not know how their medical diagnoses are being coded, nor is it a great concern to them (as long as the bill is paid by the insurer). With the Privacy Rule, however, patients have forms to sign and new policies to adhere to with regard to accessing their health information.

The covered entity must employ an individual designated as a privacy officer. This person can be full time or part time, but must be intimately knowledgeable of HIPAA. It is certainly not a position to be given to someone in title only. This person is responsible for understanding and implementing the Privacy Rule. Although no specific background is required of the privacy officer, the person must have an understanding of health information, information technology, regulatory compliance, and management.

The first big change for both the staff and the patients was the introduction of the Notice of Health Information Privacy Practice, simply called the Notice. Employees of the covered entity have been required to provide the Notice once to every patient seen on or after April 14, 2003. On February 17, 2009, the Health Information

Technology for Economic and Clinical Health Act (HITECH) made changes to the Notice; thus on and after February 17, 2010, the revised Notice must be provided to all patients once. This is to be remembered concerning the HIPAA Privacy Rule: Whenever the Notice is revised by any legislation, it must again be provided to all patients.[3] It is necessary to have a process in place, whether paper or electronic, to keep track of who has been given the Notice and who has not. For example, if a long-standing patient does not present at the office again until 2012, the system must indicate that this patient has not been in since before February 17, 2010 and thus must receive the revised Notice. On the other hand, one should not wish to waste time and money or irritate the patients by repeatedly giving them the Notice. The Notice must also be changed on the provider's website and in any postings within the facility. Managers must also budget for the costs of keeping the Notice current.

Patients will also see new forms when they request copies of their medical information. The Privacy Rule has altered the standard Release of Information Form, although it remains unchanged in its essential contents. Patients also have the opportunity to request to amend their medical records, and forms must be completed for this purpose. Once completed, forms are reviewed by the author of the medical record notes or perhaps others if the original writer is not available. The privacy officer must be able to lead this process and ensure that all HIPAA documents are retained for 6 years. This in itself takes planning as one must decide whether records will be stored on-site or off-site, and electronically or on paper. A sample request form is shown in Exhibit 2-1.

Not all information is to be retained. Material that is not to be kept must be disposed of in a manner that ensures it cannot reasonably be reproduced. For paper, the most popular disposal method is shredding. For electronic data, the most popular way is degaussing. For either method, however, the covered entity must have a policy in place. If an external firm is used for disposal, it must provide the covered entity with certificates of destruction stating that they did in fact destroy the data and did not retain it or pass it on to others. A certificate of external destruction is shown in Exhibit 2-2.

A significant requirement that encompasses the entire covered entity involves the knowledge and awareness of HIPAA by all workforce members. All must be trained about HIPAA, and that training must be documented. In addition to training, HIPAA awareness must be routinely reinforced. This provision was put in place so that HIPAA is not forgotten, but rather remains a part of standard operating procedures. At every staff meeting the healthcare manager can simply have HIPAA on the agenda and review its status and implementation. The manager can review with the privacy officer how processes and procedures are being carried out and what their apparent effects are on the entity.

Employees must also be aware of their limits on access to information. Based on one's role, employees will be allowed to have access to only the information they need to fulfill their roles and nothing more. The need to know and minimum necessary standards apply such that employees do not acquire patient health information over and above what is needed to complete the task at hand.

Exhibit 2-1

Request for Amendment of Health Information

Patient name: _____

Medical record number: _____

Birth date: _____

Address: _____

Date of information to be amended: _____

Type of information to be amended: _____

Why is the information inaccurate or incomplete? _____

_____

_____

What should the information say? _____

_____

_____

If the request is agreed upon, where else should the amended information go?

Name: _____

Address: _____

_____ _____

Signature of patient Date

To Be Completed by the Healthcare Provider:

Date received: _____

By whom: _____

Request for amendment has been: ACCEPTED DENIED

If denied, state reason: _____

_____

Information is accurate and complete

Healthcare provider's reason: _____

_____

_____

_____

_____

_____ _____

Signature of healthcare provider Date

Exhibit 2-2

Destruction of Patient Health Information by an External Entity

Name of facility and address: _____

Vendor name and address: _____

Description of information, and time period of the information: _____

Pick-up date of material: _____

Quantity of information destroyed: _____

Date of destruction: _____

Method of destruction: _____

Name of person doing destruction: _____

Signature: _____ Date: _____

As stated in the Notice of Health Information Privacy Practices, a patient has the right to file a HIPAA compliant with the covered entity, usually directly with the privacy officer. The first duty of the privacy officer—and this is where that official really needs to know HIPAA thoroughly—is to determine whether the complaint is truly HIPAA related. The patient cannot use the HIPAA complaint process, for example, to complain about waiting too long to see a physician. The covered entity must have a complaint process in place directing where and how patients can file complaints to how these are to be investigated and processed. If a complaint is warranted, sanctions must be assessed against the involved employees.

Not only do complaints warrant follow-up, but routine HIPAA audits may also reveal something that is not HIPAA compliant. Although the HIPAA Privacy Rule does not specify how often audits are to be performed, the healthcare manager can base HIPAA audit frequency on the timing of other audits such as those for billing and quality assurance. Areas in which issues arise are of course audited more frequently. It is necessary to document the audits and their findings; any adverse findings must be addressed via a documented action plan with subsequent follow-up on results.

Healthcare managers need to work with their privacy officer in relation to two external groups: business associates and researchers. Business associates are external constituents who see the covered entities personal health information but are not part of the organization's workforce (e.g., a computer vendor or an outside billing company). With such associates there must be a signed business-associate agreement calling for compliance with all HIPAA regulations. Under HITECH, implemented February 17, 2010, business associates must adhere to all of the HIPAA Security policies and not simply provide reasonable assurance that they are keeping patient health information private, secure, and confidential. The covered entity must also remain in communication with business associates to ensure that any noncompliance is corrected immediately and is not as a result of malice.

Persons conducting research in your organization and using personal health information also must be compliant with HIPAA. Data used for research cannot compromise the privacy, security, and confidentiality of patient health information.

The healthcare manager, in concert with the HIPAA privacy officer, must be proactive in protecting patient health information. Whether involving house staff, patients, themselves, business associates, or researchers, there is always much to be attended to and monitored under the HIPAA Privacy Rule.

Following the Privacy Rule is the HIPAA Security Rule, implemented April 20, 2005. The Security Rule is unique in including both required and addressable policies, thus it is entity dependent. Covered entities must follow the implementation specifications for the required policies. With the addressable policies, a covered entity must assess whether each implementation specification is reasonable and appropriate for protecting its patient health information.[3] The policies are then further divided into the three categories of technical, administrative, and physical aspects of security.

Just as the Privacy Rule calls for a privacy officer, a security officer is required for the Security Rule. This can be the same person as the privacy officer, as long as the individual has the time and expertise to cover both roles. Employees must be trained in security measures and this training must be documented. Security awareness among employees must also be stressed throughout the organization.

Documentation is vital concerning the Security Rule. Just as with privacy documentation, all HIPAA security documentation must be retained for 6 years. The Security Rule also necessitates a disaster manual documenting procedures to follow in the event of a disaster during which health information could be in jeopardy. This manual should exist in concert with the emergency-mode-operation plan intended to keep the organization functioning to the best of its ability in any compromised situation. The security officer, often the primary author of the manual, must be thoroughly conversant with its contents at all times. The security officer will most likely also be the person who implements the security incident policy. Table 2-1 lists the necessary security policies.

Table 2-1 *Areas of Necessary Security Policy Coverage*

Security Policies	Administrative	Physical	Technical
Required	1. Risk Analysis/Assessment 2. Risk Management 3. Sanction Policy/Disciplinary System 4. IS Activity Review 5. Assigned Security Responsibility (Security Officer) 6. Workforce/Personnel Security 7. Clearinghouse Functions/ Hybrid Entity 8. Response and Reporting 9. Data Backup Plan 10. Security Plan 11. Critical Business Processes/ Contingency Plan 12. Business Associates 13. Evaluation	1. Workstation Security 2. Device and Media Controls 3. Disposal of Computers 4. Media Reuse	1. Unique User Identification 2. Emergency Access 3. Audit Trails 4. Person or Entity Authentication
Addressable	1. Authorization and/or Supervision of Access to personal health information Personal Health Information (PHI) 2. Access to Data/Workforce Clearance 3. Terminating Access 4. Granting Access/Access Control 5. Access Establishment and Modification/Personnel Security 6. Security Reminders/Awareness 7. Malicious Software 8. Log-in Monitoring 9. Password Management 10. Testing and Revision 11. Applications and Data Criticality	1. Disaster Recovery/ Restore Lost Data 2. Physical Safeguards 3. Access Control & Validation 4. Maintenance Records/Logs 5. Accountability/ Transfer of Media & 6. Copy electronic personal health information.	1. Automatic Log Off 2. Encryption and Decryption Mechanism 3. Authentication of Electronic PHI 4. Integrity Controls 5. Encryption of Transmitted PHI

The security officer must be the person who implements and monitors policy compliance. The HIPAA Rule does not prescribe specific security measures, but rather provides blanket mandates and allows the organization to decide how these will be met. For example, the organization must have authentication methods in place, but whether these include passwords, thumbprints, or retinal scans is the organization's decision.[3]

Since access to patient health information is role-based, access-control audits must be completed. Employees who do not need access to information to perform their jobs will be identified on an audit if they violate access rights. With electronic records violations are readily detectable as one can look at the computer history, but with paper records there is more reliance on one's word that another was seen with the record. Computers should clearly record that electronic records are audited when one logs in. The computer should also have an automatic log-off process in the event of an emergency. Employees should never share their passwords except in a true emergency, nor should they store their passwords in obvious places.

When an employee leaves the organization either voluntarily or involuntarily, access must be terminated. It is particularly important when an employee is terminated involuntarily, as time is of the essence to prevent the terminated employee from saving any files for personal use or destroying files. If at all possible, a terminated employee's computer should be examined for any such activity before the person's departure. Thus another function of the security officer or designee is to have all files backed up as a precaution against loss.

In the same manner as the privacy officer, the security officer needs to manage the business-associate agreements. The same method used with the Privacy Rule can be used here.

Although the Security Rule is fairly extensive, its presence it is not nearly as evident to the patient as is the Privacy Rule.

The final three rules, the Standard Unique Employer Identifier Rule, the National Provider Identifier Rule, and the Enforcement Rule are not as extensive as the Privacy and Security Rules but they are just as important from a managerial perspective. The Standard Unique Employer Identifier Rule was implemented July 30, 2004. This rule calls for the organization to use its employer identification number (EIN) as its standard identifier. Many organizations were already doing this before HIPAA, so compliance was not an issue. For those who were not doing so, it was a matter of replacing what they had been previously using with the EIN.

The National Provider Identifier Rule was implemented May 23, 2007. This rule required healthcare providers to use a 10-digit unique identifier. The covered entities had to apply for the numbers and ensure they were used in all transactions. Computer fields, as well as forms, and policies needed to be updated. Inventorying the locations where the numbers are used is itself a large task.

The Enforcement Rule was implemented on February 16, 2006. As its name indicates, this rule mandates enforcement of HIPAA. Healthcare managers had to develop appropriate policies and procedures. This rule specifies what happens if there is a violation of HIPAA; it describes the issues of evidence and trial situations. Mangers need to understand this rule in the unlikely event of ever being a defendant or a plaintiff or involved in some other way in a legal debate.

These six rules of HIPAA currently set the stage for the remaining five rules. The healthcare manager will utilize the same skills and processes in implementing the remaining five as applied in the implementation of the first six. Most importantly, managers must come to view HIPAA as a part of standard operating procedures.

What Organizations Need to Do for All Six Implemented Parts

With 6 of the 11 rules of HIPAA released and 5 more to go, healthcare managers need to see HIPAA as an essential part of general operations. If its inevitability is recognized and it is incorporated into how one regularly does business, it will not feel like a legal albatross. Its integration into standard operating procedure requires putting some specific things in place.

First, as stated for the Privacy and Security Rules, a covered entity must employ a privacy officer and a security officer. Once in place, this person or persons can then, in concert with the healthcare manager, implement and manage HIPAA. A sample job description for a privacy officer appears in Exhibit 2-3.

The privacy and security officer is supported by a HIPAA committee. The HIPAA committee is comprised of people from information technology, health information management, administration, human resources, finance, and research if applicable. All of the parts of HIPAA must be represented on the HIPAA committee and thus a wide variety is needed in the committee's membership.

The third and most time-consuming responsibility is the development of the policies and procedures needed for all of the HIPAA rules. These policies are best developed from the law itself rather than from secondary sources. In this manner, the organization will be using the most precise policy language. Also, as with the Security Rule's addressable policies, all organizations will not be the same in size and scope so it is preferable to avoid using policies from other organizations. Each HIPAA rule should be covered by a policy manual or at least a separate manual section for easy reference. In drafting one's own, the organization will also be able to include consideration of implementation and changes to business operations. The HIPAA committee can be most helpful in drafting polices. In addition, many organizations have a policy committee that can also assist.

The fourth responsibility requires the covered entity to provide a training and awareness program for all workforce members. Not only as each part of HIPAA is unveiled must there be training, but this training must also be ingrained into the fabric of the organization. It cannot be a do-it-once and forget-about-it event. Training can be done in-house or outsourced; it can be done face-to-face, via computer, or by distance education. In the majority of small- to medium-sized organizations, it is the role of the privacy and security officers to perform this task. In larger organizations, online training is used or is outsourced to trainers so that it will not take up all of the time

Exhibit 2-3

Sample Job Description, Privacy Officer

Title: Privacy Officer
Division: Corporate Administration
Reports to: Chief Executive Officer of the covered entity
Position purpose: The privacy officer is responsible and accountable for all activities related to the development, implementation, evaluation, and modification of activities concerning the privacy of and access to patient health information as designated by HIPAA.

Position responsibilities:

- Identify, implement, and maintain organizational patient health information privacy policies and procedures.
- Work with the security officer, compliance committee, management, and staff in ensuring that privacy and security policies and procedures are maintained.
- Is responsible and accountable for all activities related to the privacy of and access to patient health information.
- Perform health information privacy risk assessments.
- Perform ongoing compliance monitoring activities and works with management to operationalize these monitoring activities into the daily functions.
- Develop and implement compliance related forms.
- Develop and maintain initial and ongoing training for all workforce members of the organization on HIPAA and HITECH.
- Review and bring into compliance all business associate agreements in regards to HIPAA and HITECH.
- Establish and implement a system to track assess to patient health information.
- Establish and implement a process allowing patients the right to inspect and request to amend their health information.
- Establish a program whereby complaints can be received, documented, tracked, and investigated.
- Develop a disciplinary system of sanctions for failure to comply with HIPAA for employees and constituents of the organization.
- Promote an ongoing culture of information privacy awareness and compliance to all related policies and laws.
- Develop policies and procedures for release of information and access to information.

- Maintain current knowledge of applicable federal, state, local, and organizational privacy laws and regulations.
- Work with all facilities and departments to standardize policies and procedures in regards to the privacy of patient health information.
- Lead the compliance committee and amend it as needed.
- Communicate as often as necessary due to changing regulations and compliance issues.
- Perform other activities as assigned.

Position qualifications:

- Bachelor's degree in a healthcare-related field is required.
- Certification in Healthcare Privacy and Security is recommended.
- Three years of management experience in health care.
- Knowledge of information privacy laws and issues related to access to health information, release of information, and patient rights.

of the privacy and security officers. All of the training must be documented and the documentation must be retained for 6 years. Some more thoughtful managers simply put it in the employee files and keep it beyond 6 years as long as the person remains employed. Training is done as changes occur to HIPAA, but sustained awareness must to be a regular business practice. Simply having a discussion at a staff meeting on HIPAA may constitute awareness; therefore, this activity need not be extensive to be effective. Of course if there is a violation, training must address that in the correction plan. Training is never ending, as HIPAA itself must be regarded as never ending.

The fifth responsibility concerns the development of a document retention system to retain all HIPAA materials for a minimum of 6 years. At the onset, many thought that this would be easy: Simply save everything. But doing so eventually becomes overwhelming in the face of the need to retrieve a specific record, thus the need for an organized method of retention.

HIPAA materials that must be retained include the forms that patients, employees, and business associates complete, policies that are revised, employee records such as for training and sanctions, audits and updates, and any material that contains patient health information that may not exist in the formal medical record (e.g., research forms). As a first step, a documentation retention subcommittee of the HIPAA committee can be formed. It is this group's responsibility to determine what needs to be retained and who has it, and then determine the quantity of information to save and whether its form be paper, electronic, or audio. Multiply that effort by 6 years and then determine how and where the material can be saved. For example, can paper be scanned? Or will the paper be saved in hard copy but perhaps off-site? Here budgetary considerations emerge. Initially many managers did not consider processing and retention costs; the

amount of material that must be saved can be large. Also, if one contracts with an off-site storage organization, it is necessary to reckon with the cost of retrieval. How much per piece? How much per retrieval trip? Retention is not simply saving items; it necessarily includes an understanding of the process of doing business.

The sixth responsibility concerns development and implementation of an audit system. This was much more prominent when the Enforcement Rule was implemented. The basic assumption is that if it is not documented, it was not done. Unfortunately, one's word is never good enough when the healthcare manager must respond to a HIPAA complaint. Making audits a part of standard operating procedures shows that the organization is serious about it, and that, in itself, helps create a culture of caring and competency. A sample audit report form is shown in Exhibit 2-4.

Exhibit 2-4

Sample Audit Report Form

Date of audit: _____

Audit performed by: _____

Subject of audit: **Please circle subject of audit**

- Computer log-ins
- Medical record documentation
- Coding and billing (claim denials)
- Adherence to confidentiality policies
- Adherence to security policies
- Update of employee files
- HIPAA training of employees
- Review of violations/operational issues
- Review of personnel access to patient health information
- Number of breach of confidentiality issues
- Claim denials
- Other: _____

Department audit took place in: _____

Sample of employees surveyed: Number: _____ Type: _____

Adherence percentage: _____

Nonadherence percentage: _____

Report rationale: _____

Action plan:

_____

_____

The next responsibility calls for development and posting of a complaint process. Any patient has the right to file a HIPAA complaint if he or she believes that something that occurred is not consistent with HIPAA requirements. This must be clearly stated in the notice, which must also delineate the process for filing a complaint both internally and with the federal government. The healthcare manager must take every complaint seriously and ensure it is investigated. The manager, along with the HIPAA privacy officer, must first determine if a complaint is actually HIPAA related. If so, the privacy officer will further investigate and also call in the security officer if the complaint involves security issues. If not HIPAA related, the complaint goes back to the manager for follow-up as a general personnel issue. Complaints must be tracked such that employee follow-up occurs, it is determined that office procedures are altered to prevent further complaints as necessary, and training is reinforced in common complaint areas.

The final major responsibility, the sanction process, functions in concert with the complaint process. Although HIPAA does not specify the nature of the sanctions, the organization must apply reasonable sanctions that are consistent with the seriousness of the violations. It must be noted, however, that a violation of HIPAA can also provoke civil and criminal penalties; therefore, all violations and sanctions must be taken seriously. Sanctions can include termination of an offending employee and additional penalties. It is absolutely necessary that the manager retain documentation establishing that the employee was trained and did attend awareness meetings. It is unreasonable to expect the employees to observe HIPAA regulations if they have not been adequately trained. A sample of a form for documenting training appears as Exhibit 2-5.

In many organizations, HIPAA training documentation is kept with general employee training records and is maintained by the HR department. No matter who maintains the records, however, the HIPAA privacy and security officers remain accountable for training employees on the HIPAA Privacy and Security Rules.

Exhibit 2-5

HIPAA Training Record

Name: _____

Employee identification number: _____

Department: _____

Employment start date: _____

Date	Training Topic	Comments
_____	_____	_____
_____	_____	_____
_____	_____	_____

Keeping Up with HIPAA

With six of the eleven rules of HIPAA implemented, healthcare managers have much to do. As seen with HITECH and its influence the HIPAA Privacy and Security Rules, while managers await the next five rules, they must also remain current with the original six. When HIPAA is essentially up and running in the organization, this task of keeping up to date becomes less daunting. Managers are encouraged to attend conferences, join professional associations, read the literature, and foster awareness of HIPAA throughout their organizations.

Questions for Review and Discussion

1. Under HIPAA are patients allowed to alter their health information records? If so, how must this be done?
2. Why is documentation of HIPAA training necessary?
3. Define the term "business associate" and describe how and by whom the activities of such associates are controlled.
4. What are the circumstances that primarily govern anyone's access to a patient's personal medical information?
5. What is the purpose of the Health Information Technology Economic and Clinical Health Act (HITECH) implemented February 17, 2010?
6. What do you believe have been the biggest objections to HIPAA voiced by managers and administrators?
7. So far, what seem to have been the greatest visible effects of HIPAA?
8. Describe the form or forms in which a covered organization must maintain its HIPAA records.
9. What do you consider to be the primary reasons for the enactment of HIPAA?
10. What is the general legal attitude toward the absence of documentation needed to resolve a complaint or respond to a challenge?

References

1. Mossman, V. S. (2006). Recap of HIPAA information sessions and guidelines. *Action Newsletter, American College Health Association, 46*(1).
2. 45 CFR 160.103. Standards for Privacy of Individually Identifiable Health Information. US Department of Health and Human Services, Office for Civil Rights. (2000, December 28).
3. 45 CFR 164.520(b)(3). Health Insurance Reform: Security Standards, Final Rule. US Department of Health and Human Services, Office for Civil Rights. (2003, February 20).