

# Halfway There? Check to See If You Are Six of 11 Health Insurance Portability and Accountability Act Rules Are Set

*Joan M. Kiel, PhD, CHPS*

The Health Insurance Portability and Accountability Act contains 11 rules, 6 of which have been released to date. Within each of the rules are numerous actions to be implemented. This article reviews those actions and provides health care managers with what exactly needs to be done to be in compliance with the Health Insurance Portability and Accountability Act effectively and efficiently. Key words: *compliance, HIPAA, privacy, security*

WITH 6 OF 11 sections of the Health Insurance Portability and Accountability Act (HIPAA) disseminated to covered entities, it is a good time to perform an organizational checklist to assess what you “should have done” and what you will need to do to be compliant. The 6 sections are the following:

- a. Transactions and Code Sets
- b. Privacy
- c. Security
- d. Standard Unique Employer Identifier
- e. National Provider Identifier (NPI)
- f. Enforcement

First and foremost, ensure that your organization is familiar with the 6 HIPAA parts. If you are looking at the above list and asking “when did this part come out?” or “what is this?” you will need training and, perhaps, assistance to implement those sections. Be cautious on where to seek help, though. Select those who have *implemented* the HIPAA parts that you need assistance with. These people are health management systems professional with cre-

dentials such as Certified Healthcare Privacy and Security (CHPS), Certified Healthcare Security (CHS), Certified Healthcare Privacy (CHP). If you are knowledgeable of the 6 parts, then you are most likely in the implementation phase and moving toward full compliance. Check to see how your organization is doing.

- Be knowledgeable of the 6 parts of HIPAA.

## TRANSACTIONS AND CODE SETS

The Transaction and Code Set Rule compliance date was October 16, 2002, or October 16, 2003, if one filed an extension. Be sure that your compliance documentation from those with whom you perform transactions is on file. This is the strongest way to be assured that you are compliant. If you do not have the documentation and are having doubts about your compliance status, assess the number of failed transactions. How many recipients are involved? Contact those recipients and explore whose side the issue lies on, but note that it may be on both sides. Maintain a log of system updates and be sure to include all of the backup paperwork with appropriate contact information. Check to see how your organization is doing.

- Have documentation on file
- Have you investigated failed transactions?

---

*From the University HIPAA Compliance, Duquesne University, Pittsburgh, Pa.*

*Corresponding author: Joan M. Kiel, PhD, CHPS, University HIPAA Compliance, Duquesne University, Pittsburgh, PA 15282 (e-mail: Kiel@duq.edu).*

- Is your log system current?
- Is the backup paperwork for updates on file?

## PRIVACY

The Privacy Rule compliance date was April 14, 2003. With this rule, paperwork, information technology (IT), business operations, and employee training experienced changes. This rule was also the HIPAA area that was most visible to patients as they had to sign forms and authorize individuals to see their patient health information (PHI). Now that the rule has been in place for 3 years, practices need to ensure that they are diligently compliant.

Every covered entity must have a privacy officer. That individual must have a job description reflecting the privacy officer position. In addition, all employees, business associates, and workforce members, in general, must be knowledgeable of this person. If the Officer of Civil Rights were to visit, this person could randomly ask any employee who the privacy officer is. It is the covered entity's responsibility to convey to all the privacy officer's identity, location, telephone extension, and duties. The covered entity might put the privacy officer's business card in their orientation packet for new employees or make the business card as a payroll stuffer for all employees.

Some patients have said that they are "tired of being asked about the Notice of Health Information Practices," but the reality is that the Notice must be offered to all patients only on their first encounter after April 14, 2003. The covered entity, though, should develop a manual or electronic system to track those who have acknowledged the Notice so that individuals are not offered it again from the same covered entity. Is the Notice posted in the covered entity, and if the covered entity has an Internet site, is the Notice posted clearly on the site?

Additional forms that must be in place include the Authorization to Release PHI, Accounting of Disclosures, and Request to Amend Records. Is the process for the request for record amendment effective and efficient,

especially if the judgment was a denial? What is the appeal process and has it been satisfactorily accepted by all parties involved? Along with the appeal process, covered entities must have a general HIPAA complaint process. Here, a confidential telephone number or access point to reach an individual to file the complaint confidentially must be established.

To ensure privacy of PHI, documents being faxed must be protected. Here, cover sheets and a policy to ensure that the sender and receiver do not breach privacy must be put in place. Second, the facsimile machines should not be in a publicly accessible area such as a hallway or a workroom that is open to patients walking by. Not only facsimile machines but also bins that hold PHI to be shredded should be in private areas. Many covered entities have a routine whereby during the day, records to be shredded are simply placed in a bin. But if these bins are in a publicly accessible area, information can be lifted. Patient health information that must be destroyed must also be protected until it is destroyed.

From destruction of information to retention of information, HIPAA documents must be saved for 6 years. Ensure that everyone in the covered entity knows of this so that nothing is inadvertently discarded. A file system is to be set up to ready reference the HIPAA documents.

Patient health information used by external constituents such as researchers or vendors must be protected. Research protocols fall under the jurisdiction of an institutional review board. When PHI is being used for a research protocol, a data-use agreement must be completed. Depending on the nature of the research (blind study, human subjects at risk, deidentified PHI or not), other forms will be required. Business associate agreements are needed for those who conduct business with the covered entity and use PHI. Business associate agreements are not needed by everyone that the covered entity has contract with. The difference lies in knowing exactly how the external constituent works with the covered entity and how PHI is used. Simply having a contract with the covered

entity does not make one a business associate. An example of this is a college or university who may send students to the covered entity as trainees.

Applicants for employment and employees must be considered under the HIPAA Privacy Rule. For protection of the covered entity, applicants can be asked if they have ever breached HIPAA. In addition, a general discussion of HIPAA and the covered entity's commitment to it should ensue. The applicant who becomes an employee must then undergo training, which must be documented. Here, a database can be created to keep current on training and retraining dates, any actions taken, and training subjects. It is important that the retraining date(s) be close to the incident date(s). All employees, given their roles and responsibilities, must know their access limit to PHI given the minimum necessary and need-to-know principles. Only in an emergency can employees go beyond their access limit.

The HIPAA Privacy Rule must be operationalized into standard business practices. To help ensure this, covered entities must conduct an awareness campaign and perform audits. One of the reasons for requiring each covered entity to have a compliance/privacy officer is so that the law would not be "forgotten" once it was implemented. Rather, the makers wanted the law to direct the way covered entities perform their work. To be successful, covered entities must constantly keep employees cognizant of HIPAA through an awareness campaign. It is not enough to discuss it at orientation and then never mention it again. Rather, HIPAA must be an ongoing program that is in the forefront of employees' minds. Posted signs, newsletter blurbs, payroll stuffers, and discussion at staff meetings are important methods to keep people aware of HIPAA. In addition to having personnel aware of HIPAA, covered entities must be assured that the rule is being applied properly. Audits are the mechanisms to ensure this. Audits are conducted by the compliance/privacy officer, and their results must be retained for 6 years. The Privacy Rule is not only meant to protect PHI but also

to instill in covered entities best practices. Check to see how your organization is doing.

- Is a privacy officer employed?
- Is a Notice verification system in place?
- Is the Notice posted both in the entity and if needed, on the Web site?
- Is the Authorization to Release PHI, Accounting of Disclosures, and Request to Amend Records form set?
- Is the complaint process established?
- Is the facsimile machine in a private area?
- Is PHI properly destroyed?
- Are HIPAA documents being saved for 6 years?
- Is a policy in place for PHI use by researchers?
- Are business associate agreements signed?
- Are applicants made aware of HIPAA?
- Are new employees trained and is that training documented?
- Are employees aware of their information access limits given the need to know and minimum necessary principles?
- Is an awareness campaign in place?
- Are audits being completed?<sup>1</sup>

## SECURITY

The Security Rule compliance date was April 21, 2005. With this rule, paperwork, computer systems, business operations, and employee training needed review. This rule does not deal only with information systems but more so with administrative, physical, and technical security. Administrative security concerns itself with the policies and procedures that ensure that PHI is secure. Physical security concerns itself with tangible, physical barriers to secure PHI, such as locked doors. Technical security concerns itself with "electronic" barriers to protect PHI, such as firewalls and computer passwords. All 3 types of security must be operational in the covered entity.

Just as with the Privacy Rule, all covered entities must have a security officer. This individual must have a job description reflecting the security officer functions and responsibilities. In addition, all employees, business associates, and workforce members, in general, must be knowledgeable of this person.

If the Officer of Civil Rights were to visit, this person could randomly ask any employee for the name and location of the security officer. It is the covered entity's responsibility to advise all employees of this person's location, telephone extension, and duties.

The security officer is to work with the IT Department to develop, if not already done, or refine as necessary the Security Disaster Manual and Emergency Mode Operation Plan. If the manuals are nonexistent, a small committee consisting of information management and IT people should be formed to develop them. Not only should these manuals be in print, but they should also be put in practice with security drills. The results are to be documented and retained for 6 years.

Just as with the Privacy Rule, training is a vital part of the Security Rule. Here, all employees must be educated on the Security Rule. The training must be measured and documented. In addition to the training, awareness via reminders must be incorporated into normal business practices. Training and awareness must be integrated with authentication methods to ensure that those without legitimate access to PHI do not hear it or see it. Authentication ranges from retinal scans to token rings to passwords and involves assigning each user a unique identifier. The key is to have the identifier not be able to be reconfigured. For example, passwords should not be the individual's first initial and last name; with this configuration, everyone in the covered entity can enter under another employee's name. Passwords must also be changed as needed, ensuring that when employees are terminated, so are their passwords, thus, keeping patient health information secure.

The security officer can assess authentication and computer use with access control audits. Here, assessing patterns of computer use, the security officer can recognize when individuals are using a computer different from their normal patterns and assess whether this use is legitimate. Covered entities are protected by having a log-in audit warning telling employees that the computers will be monitored. Something as simple as "XYZ (covered entity) audits the use of this computer" is sufficient.

Another technical security feature is the automatic log-off. Here, the computer can be set for a specified time of computer inactivity, at which point the user is logged off. This is most helpful if a user walks away from the computer or starts a new task not involving the computer without logging off. The log-off time should be balanced between logging someone off who may be a slow typist and stopping an intruder from getting into the system.

Even with administrative, physical, and technical security measures, a security incident policy must be developed. The security officer, in collaboration with the Human Resources Office, will develop sanction and discipline policies and procedures. Given that HIPAA violations can lead to civil and criminal penalties, the policies and procedures should mirror the seriousness of the violation. When there is an incident that results in an employee termination, the termination of access to PHI of that employee should follow immediately. The security officer, the IT Department, the Human Resources Department, and the employee's immediate supervisor must all be involved immediately to prevent any destruction or theft of data. In cases where data are destroyed, a covered entity can resort to its backups. Data backups must be accomplished consistently and stored both on-site and off-site to be most secure. Although one hopes to not have to resort to backups, when it is necessary, it shows just how important a procedure it is.

Covered entities must ensure that only the minimum necessary data are shared with business associates. Business associate agreements must be signed and managed such that any security violations by external constituents are managed properly. Discuss with your business associates the specific administrative, technical, and physical security they use. Ensure that as changes ensue, your covered entity is updated.

Keep these and all HIPAA Security Rule records for 6 years. Check to see how your organization is doing.

- Are administrative, physical, and technical security measures in place?
- Is a security officer employed?
- Does the Disaster Manual include HIPAA?

- Does the Emergency Mode Operation Plan include HIPAA?
- Are all employees current with training?
- Is a Security Rule awareness campaign implemented?
- Are authentication methods in place?
- Is there a password management program?
- Are access control audits being done?
- Is there a log-in audit warning on each computer?
- Is an automatic log-off process implemented?
- Is a security incident policy implemented?
- Is a termination of access process developed and communicated?
- Are data being backed up consistently and stored securely?
- Are business associate agreements signed and current?
- Is a record retention system developed?

### **STANDARD UNIQUE EMPLOYER IDENTIFIER**

The Standard Unique Employer Identifier Rule compliance date was July 30, 2004. Many covered entities are already compliant, as this rule specifies that employers use their employer identification number (also called the federal tax identification number) as their standard unique identifier. Just as a Social Security number routinely identifies an individual, so too an employer identification number identifies a company/organization. If, for some reason, a covered entity does not have an employer identification number, it needs to file for one immediately. Check to see how your organization is doing.

- Has the covered entity instituted the employer identification number as its standard unique identifier?<sup>1</sup>

### **NATIONAL PROVIDER IDENTIFIER**

The National Provider Identifier Rule (Standard Unique Health Identifier for Health Care

Providers) compliance date is May 23, 2007. This 10-digit number will be assigned to health care providers who apply to the National Provider System for the number. The application process began May 23, 2005. The NPI number will be used to track the provider in all health care transactions.

Check to see how your organization is doing.

- Has the covered entity assigned someone to apply for the number in 2005?
- Has the covered entity applied for their NPI numbers?
- Has the covered entity followed up on the application for or received their NPIs?
- Has the covered entity talked to its IT vendors about its transition to the NPI?

### **ENFORCEMENT**

The Enforcement Rule compliance date was February 16, 2006. Covered entities should have been familiar with this rule because the interim Enforcement Rule was in effect for a period of time. This rule concerns itself with the procedures and penalties for HIPAA violations. Check to see how your organization is doing.

- Has the covered entity developed or obtained the policies and procedures for the Enforcement Rule?
- Is the covered entity complying with HIPAA to avoid having to implement the Enforcement Rule?

### **THE EFFECTIVE MANAGER**

With 6 parts of HIPAA completed, covered entities need to assess where they are in the process and decide what further resources need to be dedicated. The key is to integrate HIPAA implementation into the mission and operations of the organization. Over time, it should become a standard practice of doing business.

### **REFERENCE**

- 
1. 45 CFR Parts 160, 162, and 164, Code of Federal Regulation 1996.