Keeping Data Safe

AN IN-DEPTH LOOK AT THE NEW HIPAA SECURITY RULE

By Clayton Fast, CHBME

THE HIPAA SECURITY RULE BECOMES effective April 21, 2005, for the following entities: healthcare providers who electronically transmit any protected health information, healthcare clearinghouses, and health plans (jointly referred to as "Covered Entities"). Most billing services are considered clearinghouses under the HIPAA provisions and are therefore Covered Entities.

The other primary components of HIPAA are "Electronic Transactions/Transaction Code Sets," which took effect October 15, 2003, and the Privacy Rule, which took effect April 14, 2004. Much of the information in this article came from the Workgroup for Electronic Data Interchange (WEDI) Web site.

Security should not be confused with privacy or confidentiality. Security applies to administrative, physical, and technical safeguards that are implemented to protect the integrity, availability, and confidentiality of protected health information (PHI) that is in electronic form. PHI that is oral or on paper is not covered by the Security Rule. Some of the Security Rule standards have already been addressed by your existing HIPAA Privacy Plan.

(Whoops, I'm not sure I heard you correctly! What do you mean, "What Privacy Plan?" I am sure that, as a conscientious billing company, you have in place a HIPAA Privacy Plan!)

The Security Rule has been designed to be scaleable and technology independent. Covered Entities must appoint a "security official" and implement safeguards that are reasonable for their individual circumstances and that apply to the technology they have in place. The safeguards must be comprehensive enough to address cultural and organizational as well as technological and physical concerns and must protect against both internal and external threats. It should be noted that internal threats are probably more likely to occur than external threats. Covered Entities must also conduct thorough and accurate risk analysis on an ongoing basis.

In addition, business-associate agreements will have to be modified to satisfy the specific Security Rule standards for protecting electronic PHI. These agreements must require the business associate to:

- Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of the Covered Entity
- Ensure that its agents and/or subcontractors who receive electronic PHI agree to implement reasonable and appropriate safeguards to protect such information
- Report to the Covered Entity any security incident of which it becomes aware
- Authorize termination of the contract by the Covered Entity if the Covered Entity determines that the business associate has violated a material term of the agreement.

Covered Entities must appoint a "security official" and implement safeguards that are reasonable for their individual circumstances and that apply to the technology they have in place.

Covered Entities that do not comply with the Security Rule requirements are subject to a number of penalties. Civil penalties are $100 per violation, up to $25,000 per year for each requirement violated. Criminal penalties range from $50,000 in fines and one year in prison up to $250,000 in fines and 10 years in prison. There may be other unfavorable consequences, such as negative publicity, civil liability, loss of customers, and/or loss of business associates.

The Security Rule provides a number of "standards" and "implementation specifications." These are divided into three categories: administrative safeguards, physical safeguards, and technical safeguards.

A "standard" is a general requirement that must be complied with by the Covered Entity—for example, contingency planning. Not all standards have implementation specifications. An implementation specification is a more detailed and specific description of the method a Covered Entity can use to comply with a particular standard. For example, under contingency planning, there are five implementation specifications that provide specific direction. They are: a data back-up plan, a disaster-recovery plan, an emergency-mode operations plan, testing and revision procedures, and applications and data criticality analysis.

(continued on page 11)

HIPAA SECURITY

(Keeping Data Safe continued from page 9)

Some implementation specifications are "required" and some are "addressable." The Covered Entity must take action to implement required specifications, but does not necessarily need to take action to implement addressable specifications. However, the Covered Entity must assess whether the addressable specification is reasonable and appropriate, and if so, then the Covered Entity must implement the specification. If it is not reasonable and appropriate, then the Covered Entity must document the fact and implement "an equivalent alternative measure" if reasonable and appropriate.

The following information is a very high level discussion of the Security Rule requirements. Detailed information is available in a WEDI document entitled "Small Practice Security Implementation White Paper." The web link is: http://www.wedi.org/snip/public/articles/dis_viewArticle.cfm?ID=221&wpType=2.

Administrative Safeguards. The administrative safeguards relate primarily to the Covered Entity's "workforce" and the way its staff is educated and expected to carry out the security requirements. The administrative safeguards require documented policies and procedures that are intended to limit information access to appropriate parties and guard information access or disruption from all others. **Table 1** shows the standards and implementation specifications defined by the Security Rule as Administrative Safeguards.

Physical Safeguards. The physical safeguards protect computer systems and electronic PHI from unauthorized access, unavailability, and physical damage. **Table 2** shows the standards and implementation specifications defined by the Security Rule as Physical Safeguards.

Technical Safeguards. Technical safeguards are designed to prevent

Table 1. Administrative Safeguards.

Standards	Implementation Specifications	Required	Addressable
Security Management Process	Risk Analysis	X	
	Risk Management	X	
	Sanction Policy	X	
	Information System Activity Review	X	
Assigned Security Responsibility		X	
Workforce Security	Authorization and/or Supervision		X
	Workforce Clearance Procedure		X
	Termination Procedures		X
Information Access Management	Isolating Healthcare Clearinghouse Function	X	
	Access Authorization		X
	Access Establishment and Modification		X
	Security Reminders		X
Security Awareness and Training	Protection from Malicious Software		X
	Log-in Monitoring		X
	Password Management		X
Security Incident Procedures	Response and Reporting	X	
Contingency Plan	Data Backup Plan	X	
	Disaster Recovery Plan	X	
	Emergency Mode Operation Plan	X	
	Testing and Revision Procedure		X
	Applications and Data Criticality Analysis		X
Evaluation		X	
Business Associate Contracts and Other Arrangements	Written Contract or Other Arrangement	X	

Table 2. Physical Safeguards.

Standards	Implementation Specifications	Required	Addressable
Facility Access Controls	Contingency Plan		X
	Facility Security Plan		X
	Access Control and Validation Procedures		X
	Maintenance Records		X
Workstation Use		X	
Workstation Security		X	
Device and Media Controls	Disposal	X	
	Media Re-use	X	
	Accountability		X
	Data Backup and Storage		X

Table 3. Technical Safeguards.

Standards	Implementation Specifications	Required	Addressable
Access Controls	Unique User Identification	X	
	Emergency Access Procedure	X	
	Automatic Logoff		X
	Encryption and Decryption		X
Audit Controls			
Integrity	Mechanism to Authenticate Electronic	X	
	Protected Health Information		X
Person or Entity Authentication		X	
Transmission Security	Integrity Controls		X
	Encryption		X

unauthorized access to information transmitted over communications networks and to protect, control, and monitor access to information. **Table 3** shows the standards and implementation specifications defined by the Security Rule as Technical Safeguards.

How to Develop a Security Compliance Plan

Development and implementation of a Security Compliance Plan requires these nine steps:

1. Appoint a Security Official. It is important to appoint a security official who is heavily involved in the development of the security plan. The security official may be the existing privacy officer, if so desired. As with the privacy officer position, there is no requirement that this be a full time position. However, the individual must have unfettered access to senior management and the authority to enforce the adopted policies and procedures.

2. Enlist Senior Management Support. Compliance can require significant time, effort, and resources. It is imperative to educate senior management about the Security Rule and esnure that management makes a clear and unambiguous statement of support for compliance before compliance efforts begin. As compliance efforts progress, senior management must be kept informed and up-to-date on the project.

3. Develop and Implement Security Policies. The Security Rule requires certain formal, documented security policies. It is important to define what high-level security policies are required for the particular circumstances of the organization. Security policies will provide a framework to help ensure the security measures are consistent and integrated.

4. Identify Your Electronic Protected Health Information Inventory. The confidentiality, integrity, and availability of electronic PHI must be insured. Regularly identify and document the location of your organization's electronic PHI. Document the flow of electronic PHI within the organization, as well as outside the organization. Identify information exchanged with business associates, information sent over the internet, and information exchanged between computer systems within the organization.

5. Analyze Risk. Risk analysis identifies potential threats, their likelihood of occurrence, and the potential consequences. Conduct a systematic analysis that identifies potential risks and provides recommendations to reduce them to a level that is reasonable and appropriate for the organization. Resources can then be allocated appropriately to neutralize the identified risks.

6. Consider Cultural Issues. Compliance with the Security Rule will undoubtedly require changes in the way the staff members do their job, such as limiting access to electronic PHI and the imposition of monitoring and auditing activities. These changes can cause fear, confusion, and resistance among the staff.

To minimize the impact of these issues, educate staff about the requirements of the Security Rule, why it's important, and the steps the organization will take to comply with the Security Rule. It may also help to involve the staff by requesting feedback on the proposed policies and procedures. People are more likely to cooperate when they have been involved in the development of the compliance plans.

7. Determine What is Appropriate and Reasonable. The organization is not expected to protect against every conceivable risk regardless of cost. The requirement is that the organization implements security measures against risks that can be reasonably anticipated.

Requesting feedback from the staff will help ensure that security measures are reasonable and do not adversely affect the core organizational mission.

8. Create Documentation. It is vitally important that policies and procedures be formally documented and approved by senior management. The Security Rule requires the organization to document its policies, procedures, and decisions. It is equally important that regular reviews and revisions to policies and procedures be done as necessary. The actual day-to-day business practices should conform to documented policies and procedures.

Documented policies and procedures must be made available to the staff members responsible for implementation. Documentation must be maintained for a period of six years from the date it was last in effect.

9. Prepare for Ongoing Compliance. Risks to electronic PHI will likely change over time. To maintain compliance, the organization must regularly review and revise its policies and procedures as dictated by changes in rules and regulations and by changes in the environment. It is also important to regularly monitor the Security Rule for changes.

Many organizations already have excellent security measures in place. There is nothing in the rule that requires costly changes unless they are reasonable and appropriate to the organization; nor does the rule require security measures that will hinder the ability of the organization to perform its functions efficiently and cost-effectively. However, electronic PHI must be reasonably and appropriately protected from loss, damage, or inadvertent disclosure. That is the intent of HIPAA security regulations and of billing companies. ■

Clayton Fast, CHBME, is president of Compass Billing Service Corporation in Greenwood Village, Colorado. He can be reached at cfast@compassbilling.com.
For more information and a variety of articles and papers specific to HIPAA Security, go to www.wedi.org/snip/public/articles/dis_publicDisplay.cfm?docType=6&wptype=2