

# The ABC's of HIPAA Security

By Annette Miller, J.D.

HIPAAAnswers™

Vice President of Compliance Services/Corporate Counsel

Many healthcare providers, healthcare clearinghouses and employer sponsored health plans are facing HIPAA security compliance by April 21, 2005. This article addresses the basic concepts the covered entity must understand in order to begin their security compliance program.

## Overview of Security

The Security Regulation requires the covered entity to implement appropriate security measures to ensure the confidentiality, integrity and availability of electronic protected health information (EPHI) that is created, received, maintained or transmitted by the covered entity.

## Flexibility of Approach

When implementing the security requirements, the covered entity may use any security measures that reasonably and appropriately implement the administrative, physical and technical safeguards. Contrary to popular belief, the Security Regulation does not require any purchases of any new technology, hardware or software to implement any of the security requirements. However, the covered entity is required to consider the following factors when addressing their security measures:

- Its size, complexity and capabilities
- Its technical infrastructure, hardware and software capabilities
- Its cost of security measures
- Its probability and criticality of potential risks to electronic PHI

## Implementing the Safeguards

There are three major categories of safeguards that a covered entity must implement under the Security Regulation.

1. Administrative Safeguards. Under this category, covered entities are required to create policies and procedures for managing the selection, development, implementation and maintenance of security measures and the conduct and access of workforce members to this information, and the selection, development, and use of security controls. This category makes up the majority of the Security Regulation.

HIPAAAnswers™, 8941 Aztec Drive, Eden Prairie, MN 55347

866.326.6785

[www.HIPAAAnswers.com](http://www.HIPAAAnswers.com)

Examples of the administrative standards the covered entity will need to become familiar with include:

- Security Management process
- Naming a Security Official
- Workforce Security
- Information Access Information
- Security awareness and training
- Security incident procedures
- Contingency Plan
- Evaluation

2. Physical Safeguards. The Physical safeguards are the actual physical measures (locks, sign-in sheets, etc...), the policies and procedures to protect a covered entity's electronic information systems (hardware and software) and related buildings and equipment, from natural and environmental hazards and unauthorized intrusions.

Examples of the physical standards the covered entity will need to implement include:

- Facility access controls
- Workstation use
- Workstation security
- Device and media controls

3. Technical Safeguards. The Technical Safeguards address the technology the covered entity uses and the policy and procedures for its use that protect electronic health information and control access to the technology.

Examples of the technical standards include:

- Integrity of Information (PHI and access)
- Person or Entity Authentication
- Transmission Security
- Access control
- Audit controls

As the covered entity begins to implement the security standards there are some general rules that must be kept in mind.

### **Required v. Addressable**

Under the three major safeguard categories, there are 24 standards. The standards describe what the covered entity must do. Eighteen of the standards have specific implementation specifications. The implementation specifications

describe how things are to be done. There are 36 implementations that the covered entity must do. The implementation specifications are divided into two categories – required and addressable. The required implementations are critical and must be implemented by the covered entity. Examples include conducting a risk analysis, having a sanction policy, disaster recovery plan and a data backup plan.

The addressable implementations allow for a covered entity to implement an alternative measure as long as the covered entity can show that the security standard is being met. The covered entity has three options when working through the addressable implementations.

- Implement, if reasonable and appropriate;
- Implement an equivalent measure, if reasonable and appropriate;
- Not implement.

Addressable does not mean that it is optional. All addressable items must be addressed by the covered entity. All actions made by the covered entity must be based on sound documented reasoning. The documentation should address the following questions:

- Why it would not be reasonable and appropriate to implement the implementation specification;
- The decision not to implement the addressable specification, if applicable;
- How the standard is being met.

Cost is not the sole factor in determining whether or not the covered entity should implement the security measure. Whatever security measure the covered entity decides to implement, it is imperative that the covered entity's reasoning is documented.

### **Penalties for Non-Compliance**

Covered Entities that do not comply with the Security Regulation 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 jail. Covered Entities could find themselves facing other unfavorable consequences as well. Examples of other consequences include: exposure to state lawsuits for breach of confidentiality, loss of accreditation, audits by Centers for Medicare and Medicaid Services, damages to business interests and reputation, and loss of patients or clients. Therefore, HIPAA compliance should be taken seriously by every organization.

## Conclusion

There is an abundance of work that will need to be completed prior to the April 21, 2005 deadline date. The security challenge can be overwhelming for many covered entities that try to go it alone. One approach that makes sense for any covered entity is to use a service such as that offered by HIPAAAnswers™. HIPAAAnswers™ offers sample policies and procedures, checklists and forms to assist the covered entity in complying with the security standards. Check us out at [www.HIPAAAnswers.com](http://www.HIPAAAnswers.com).

Annette Miller is the Vice President of Compliance Services/Corporate Counsel for HIPAAAnswers™. She has over 15 years experience in the health insurance industry. Annette graduated from William Mitchell College of Law, cum laude and holds a masters degree in public administration with a minor in health care administration from Drake University. She can be reached at [Annette\\_Miller@hipaanswers.com](mailto:Annette_Miller@hipaanswers.com) or 952-400-1100.

© 2004 Hard Lakes Solutions, Inc.