The HIPAA Security Rule (NPRM): Overview

By D'Arcy Guerin Gue, Executive Vice President, Phoenix Health Systems

Automation of healthcare information management has created increasing governmental and healthcare industry concerns about the security of computerized healthcare data. As the industry has incorporated electronic medical records, data repositories, networking, Internet access and other new technologies into its delivery processes, its progress in adopting corresponding information security measures has been slow and uneven. In 1997, the National Research Council reported widespread weaknesses in healthcare security measures such as user authentication, access controls, audit trails, controls of external communication links and access, physical security, systems back up, and disaster recovery.

The American public began to register serious concerns about the privacy and security of health records in the early 1990's. Breaches of health privacy, such as press disclosures of individuals' HIV status, network hacking incidents, and misdirected patient E-mails fueled this concern. At the same time, healthcare industry and federal agencies working towards HIPAA "administrative simplification" and increased automation of health information, realized that their initiatives would be unsuccessful without incorporating more effective information security measures. When HIPAA was passed in 1996, it included a mandate for standards that would ensure the security and integrity of health information that is maintained or transmitted electronically. A proposed Security Rule (NPRM) was published by DHHS on August 12, 1998.

Security vs. Privacy vs. Confidentiality

The word "security" should not be confused either with "privacy" or "confidentiality." Privacy refers to the right of an individual to control his personal information and to not have it divulged or used by others against his wishes. "Confidentiality" only becomes an issue once an individual's personal information has been received by another entity. Confidentiality is a means of protecting that information, usually by safeguarding it from unauthorized disclosure. Security applies to the spectrum of physical, technical and administrative safeguards that are put in place to protect the integrity, availability and confidentiality of information.

Applicability and Scope

The Security standards apply to all individually identifiable health information that is in electronic form, whether it is being stored or transmitted. This includes all administrative and financial healthcare transactions covered by the HIPAA Transactions Standards Rule, including internal transmissions. Health information that is on paper or oral is not covered. All healthcare providers, health plans, or clearinghouses that electronically store or transmit individual health information must comply.

Security Threats

The Security Rule focuses both on external and internal security threats and vulnerabilities. Threats from "outsiders" include breaking through network firewalls, e-mail attacks through interception or viruses, compromise of passwords, posing as organization "insiders,"computer viruses, and modem number prefix scanning. These activities can result in denial of service, such as the disruption of information flow by "crashing" or overloading critical computer servers. The outsider may steal and misuse proprietary information, including individual health information. Attacks can also affect the integrity of information, by corrupting data that is being transmitted.

Internal threats are of equal concern, and are far more likely to occur according to many security experts. Organizations must protect against careless staff or others who are unaware of security issues, and curious or malicious insiders who deliberately take advantage of system vulnerabilities to access and misuse personal health information.

Overall Approach to HIPAA Security

HIPAA Security standards have been designed to be "scaleable." The standards are technology-independent in order to address the individual circumstances of healthcare entities, and to allow for inevitable changes in technology.

The Rule is intended to set a minimum level or "floor" of security. Organizations may choose to implement safeguards that exceed the HIPAA standards - and, in fact, may find that their business strategies require stronger protections.

Covered entities are required to:

- Assess potential risks and vulnerabilities
- Protect against threats to information security or integrity, and against unauthorized use or disclosure
- Implement and maintain security measures that are appropriate to their needs, capabilities and circumstances
- Ensure compliance with these safeguards by all staff

Central to HIPAA security is the tenet that information security must be comprehensive. No single policy, practice or tool can ensure effective overall security. Cultural and organizational issues must be addressed, as well as technological and physical concerns. The safeguards that comprise HIPAA-mandated security focus on protecting "data integrity, confidentiality and availability" of individually identifiable health information through the following:

- Administrative Procedures - documented, formal practices to manage the selection and execution of security measures
- Physical Safeguards - protection of computer systems and related buildings and

equipment from hazards and intrusion

- Technical Security Services - processes that protect and monitor information access
- Technical Security Mechanisms - processes that prevent unauthorized access to data that is transmitted over a network

Administrative Procedures

Administrative procedures are intended to limit information access to appropriate parties and guard information from all others. There are twelve areas in which policies and procedures must be implemented and maintained:

Certification - technical evaluation of the compliance of data systems through a "pre-specified set of security requirements."

Chain of Trust Partner Agreements - an agreement between a covered entity and all other entities with whom health information is shared, to "protect the integrity and confidentiality" of the data they exchange.

Contingency Plan - a documented plan to maintain continuity of operations in an emergency or disaster, and to enable recovery of data following disaster.

Formal Mechanism for Processing Records - policies and procedures for the receipt, handling and disposal of health information.

Information Access Control - policies and procedures for allowing different levels of access to health information.

Internal Audit - regular review of systems access patterns.

Personnel Security - policies, procedures such as security clearances, access record maintenance, and staff training.

Security Configuration Management - procedures that coordinate overall enterprise security.

Security Incident Procedures - measures for reporting and responding to security incidents.

Security Management Process - establishing a process to "ensure the prevention, detection, containment and correction" of security breaches.

Termination Procedures - procedures used when terminating employees or users to prevent continued access to health information.

Training - security awareness training for all personnel, and specific training of users on system security protocols.

Physical Safeguards

This category of security standards is focused on preventing unauthorized individuals from gaining access to electronic information. Five areas of physical safeguards include:

Assigned Security Responsibility - officially assigning responsibility for information security.

Media Controls - setting up formal procedures for controlling and tracking the handling of hardware and software, and for data backup, storage and disposal.

Physical Access Controls - developing a facility security plan, and setting up disaster recovery, emergency modes, and other access and handling controls.

Work Station Use - policies and procedures to prevent unauthorized access to protected information on workstations and terminals.

Security Awareness Training - awareness training for all employees and others with physical access to protected health information.

Technical Security Services

Technology security services are often governed by the particular technologies and data systems in use. Covered entities are expected to balance the need for timely access to needed health information with the need to protect its confidentiality and integrity. The Rule provides for five areas of technical security services:

1. Access Control - providing controls limiting access to health information to those with valid needs and authorization.
2. Audit Controls - setting up system mechanisms that record and monitor activity
3. Authorization Control -obtaining and tracking the consents of patients for use and disclosure of their health information.
4. Data Authentication - ensuring that data is not altered, destroyed or inappropriately processed
5. Entity Authentication - employing mechanisms such as automatic logoff, passwords, PINs and biometrics, which identify authorized users and deny access to unauthorized users.

Technical Security Mechanisms

Organizations that transmit health information over open networks must keep it from being easily intercepted by third parties via external entry points. Communications and network controls include:

Integrity Controls - internal verification that data that is being stored or transmitted is valid.

Message Authentication - assurance that the messages sent and received are the same messages.

Either Access Controls - such as dedicated, secure communications lines -- or Encryption - transforming text into unintelligible ciphers thru use of special algorithm processes.

If using a network, protections must also include Alarms, Audit Trails, Entity Authentication and Event Reporting.

Current Status of Security Rule

According to DHHS, the final Security Rule will be published before the end of 2001, and should become effective 60 days later. Compliance with the rule will be required 24 months from its effective date. The proposed rule overall is comprised of widely accepted information practices that are followed in other industries such as banking and manufacturing, and endorsed by many standards organizations. As a result, DHHS has indicated that the final rule will not differ substantially from the proposed rule. Any modifications are expected to focus on reducing redundancies and providing needed clarifications.