



InetCE

Volume 7

2003

Number 3

George E. MacKinnon III, Ph.D., R.Ph., FASHP
Founding Editor

Linda Swanson
Copy Editor

Internet Continuing Education (*InetCE*) provides free, continuing education to pharmacists and other health care providers 24 hours a day over the Internet at www.InetCE.com. Since 1997, these home study programs have assisted in keeping practitioners apprised of treatment-related topics, general pharmacy, and law in the changing health care environment.

InetCE grew out of a need for relevant, continuing education in health care, and to make it accessible to pharmacy practitioners in various practice settings. This format provides convenient instruction, on-line testing, evaluation, and certification. Continuing education examinations are graded automatically and, if successfully passed, the user can print the statement of credit.

ProCE, Inc. is accredited by the Accreditation Council for Pharmacy Education (ACPE) as a provider of continuing pharmaceutical education. Continuing education programs are developed in accordance with the ACPE's "Criteria for Quality and Interpretive Guidelines." *InetCE* is supported through an unrestricted educational grant provided by Pfizer Inc., U.S. Pharmaceuticals.

HIPAA Security Rule: Administrative Requirements

InetCE 221-146-04-065-H03

Uday O. Ali Pabrai, CHSS, SCNA
Chairman and CEO
HIPAA Academy
2835 Aurora Avenue
Suite 115-342
Naperville, Illinois

PLEASE NOTE: The content of the article was current at the time it was written. The exam for this article is not valid for CE credit after 05/31/2006.

LEARNING OBJECTIVES

1. Identify the motivation for pharmacies to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule's design objectives and core category (domain) areas.
2. Describe key definitions and terminology emphasized in the final HIPAA Security Rule.
3. Examine the full scope of the final HIPAA Security Rule implementation requirements for pharmacies.
4. Analyze the administrative requirements for pharmacies associated with the Privacy Rule.
5. Identify threats to pharmacy communication over open networks such as the Internet.

ABSTRACT: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) security will be a pressing item for all covered entities to address. The compliance date for security is April 21, 2005. Larger organizations, especially those in the pharmaceutical industry, have started to examine the requirements defined in the

final HIPAA Security Rule. This article establishes the core requirements for the final HIPAA Security Rule, as well as addresses the impact of the HIPAA Privacy Rule on security and the threats that enterprises face for electronic communication.

This program is co-sponsored by ProCE, Inc. and Midwestern University College of Pharmacy Glendale. ProCE, Inc. is accredited by The Accreditation Council for Pharmacy Education (ACPE) as a provider of continuing pharmaceutical education. An on-screen statement of credit verifying participation in 0.2 CEUs (2.0 contact hours) will be displayed for printing to participants who successfully complete the examination. This article has been assigned ACPE ID number 221-146-04-065-H03.



HIPAA SECURITY RULE: ADMINISTRATIVE REQUIREMENTS

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is about information efficiency, privacy, and security in the U.S. health care industry. On February 20, 2003, the Department of Health and Human Services (HHS) released the final HIPAA Security Rule. The focus of this article is on the HIPAA Security Rule.

The Security Rule is defined within the Administrative Simplification (AS) portions of HIPAA Title II. It is the Administrative Simplification portion of the HIPAA legislation that is fueling initiatives within organizations to address health care privacy issues in these areas:

- Transactions and Code Sets
- Identifiers
- Privacy
- Security

The final Security Rule requires all covered entities to safeguard electronic Protected Health Information (PHI). A covered entity refers to all health plans, health care clearinghouses, and certain health care providers. The final Security Rule impacts all covered entities that have (even just once) submitted one of the HIPAA-defined transactions electronically.

The health care issues that relate to HIPAA deal with transaction efficiency, as well as the security and privacy of patient and medical records and information. This is very similar to the needs all businesses have to secure information related to employees, customers, and suppliers. Covered entities will also need to work with business associates, agents, and contractors that have access to electronic PHI, for example, application service providers, to ensure the security of all health information in electronic form. Covered entities have to ensure privacy and confidentiality when health information is stored, maintained, or transmitted.

This Rule impacts the pharmacies as most bill insurance companies for their patients. The industry must safeguard all electronic PHI. For most organizations, this will require the deployment of a variety of security technologies that would address areas such as perimeter security, authentication, access control, audit controls, encryption, confidentiality, and integrity.

HIPAA's goal is to bring about national standards for consistent data formats for electronic health care transactions. Besides data format consistency, another purported benefit from HIPAA compliance is the reduction in paper handling costs for health care claims. These costs are likely to be reduced from \$6 to \$8 per claim to less than

\$1. As transactions are increasing when they are conducted electronically, there is a requirement to secure the movement of information between covered entities. However, since pharmacies have handled online adjudication for many years, these cost savings may be tempered.

HIPAA Title II

HIPAA Title II includes the Security Rule. This final Security Rule describes the requirements for security for health care entities to be in compliance with the Administrative Simplification portion of HIPAA Title II. The proposed rule was published on August 12, 1998. The final Security Rule was published in the Federal Register on February 20, 2003. Covered entities, with the exception of small health plans, must comply with the requirements of the final Security Rule by April 21, 2005. Small health plans must comply with the requirements of the final Security Rule by April 21, 2006.

The final Security Rule establishes standards for the security of individual health information and electronic signature use by covered entities (health plans, health care clearinghouses, and health care providers). Covered entities must use the security standards to develop and maintain the security of all electronic individual health information.

The Security Rule is applicable to all health care information electronically maintained or used in an electronic transmission, regardless of format (standard transaction or a proprietary format). The Security Rule makes no distinction between internal corporate entity communication or communication that is external to the corporate entity. The Security Rule was defined in terms of requirements that would allow businesses in the health care industry

to select the technology that best meets their business requirements while still allowing them to comply with the standards.

The Security Rule allows the pharmacy industry, as it does for other covered entities, to ascertain the level of security information that would be needed. The confidentiality level associated with individual data elements concerning health care information would determine the appropriate security application to be used. The Security Rule defines the requirements to be met to achieve the privacy and confidentiality goal, but each business entity, driven by its business requirements, would decide what techniques and controls would provide appropriate and adequate electronic data protection. This would allow data collection and the paperwork burden to be as low as is feasible.

Pharmacies Must Comply with the HIPAA Security Rule

All pharmacies that transmit a HIPAA transaction, even if it just a single transaction, no matter the size, are considered a covered entity under the regulations, and as such, they are required to comply with HIPAA and its regulations. Pharmacies, like any other covered entity, may be fined for noncompliance (civil fines of up to \$25,000 per violation and criminal penalties of up to \$250,000 and 10 years imprisonment). Surprised?

Consider these 2 major incidents—both major infractions of individuals' privacy:

- Kaiser Permanente mistakenly sent e-mail responses to the wrong recipients. The e-mails contained sensitive patient information and affected over 850 members.
- Thousands of patient records containing medical histories, social

security numbers, credit card numbers, and other confidential information have been found in unlocked dumpsters and on the Web.

The HIPAA Privacy Rule from HHS addresses violations such as these and what can be done to protect patients' confidential information.

In the absence of a national legal framework of health information privacy and security protections, consumers are increasingly vulnerable to the exposure of their personal health information. Disclosure of individually identifiable information can occur deliberately or accidentally and can occur within an organization or be the result of an external breach of security.

Examples of violations related to patient information include the following bulleted items:

- A Michigan-based health system accidentally posted the medical records of thousands of patients on the Internet (*The Ann Arbor News*, February 10, 1999).
- A Utah-based pharmaceutical benefits management firm used patient data to solicit business for its owner, a drug store (*Kiplingers*, February 2000).
- An employee of the Tampa, Florida, Health Department took a computer disk containing the names of 4,000 people who had tested positive for HIV, the virus that causes AIDS (*USA Today*, October 10, 1996).
- The health insurance claims forms of thousands of patients blew out of a truck on its way to a recycling center

in East Hartford, Connecticut (*The Hartford Courant*, May 14, 1999).

- A patient in a Boston-area hospital discovered that her medical record had been read by more than 200 of the hospital's employees (*The Boston Globe*, August 1, 2000).
- A Nevada woman who purchased a used computer discovered that the computer still contained the prescription records of the customers of the pharmacy that had previously owned the computer. The pharmacy database included names, addresses, social security numbers, and a list of all the medicines the customers had purchased. (*The New York Times*, April 4, 1997 and April 12, 1997).
- A speculator bid \$4000 for the patient records of a family practice in South Carolina. Among the businessman's uses of the purchased records was selling them back to the former patients. (*New York Times*, August 14, 1991).
- In 1993, the *Boston Globe* reported that Johnson and Johnson marketed a list of 5 million names and addresses of elderly incontinent women. (ACLU Legislative Update, April 1998).
- A few weeks after an Orlando woman had her doctor perform some routine tests, she received a letter from a drug company promoting a treatment for her high cholesterol. (*Orlando Sentinel*, November 30, 1997).
- In Maryland, a banker improperly accessed a medical database to

determine which of its borrowers had been diagnosed with cancer. Once such individuals had been identified, the bank improperly attempted to terminate its lending relationship with them.

- The chain drug store CVS and grocery chain Giant Food conceded that they had disclosed their customers' prescription records to a direct mail company, which then tracked customers and solicited them to consider alternative treatments. After media reports sparked public concern, both companies discontinued this practice.
- A study by the University of Illinois found that 35% of Fortune 500 companies admitted to checking medical records prior to hiring or promoting employees.

As seen from the previous examples, the problem is very serious. In the face of industry evolution, the potential benefits of our changing health care system, and the real risks and occurrences of harm, protection of privacy must be built into the routine operations of our health care system. The issues and implications related to the privacy and security of patient/client health information is very serious.

HIPAA Security Categories (Domains)

The final Security Rule outlines the requirements in 3 major categories, and each will be described further:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

Administrative Safeguards

Administrative safeguards are administrative actions and policies and procedures to

manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of the covered entity's workforce in relation to the

protection of that information. Figure 1 summarizes the 9 standards and implementation specifications defined in the Administrative Safeguards category.

Figure 1: Administrative Safeguards—Standards and Implementation Specifications

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

Administrative safeguards refer to documented practices to manage the selection and execution of security measures to protect data and to manage the conduct of members of the workforce in relation to the

protection of data. As part of the administrative safeguards requirement, for example, an organization must perform a risk analysis and develop a sanctions policy.

The administrative safeguards category forms the foundation on which the other standards depend. Covered entities are required to implement administrative, physical, and technical safeguards. These entities must ensure that data are protected, to the extent that is feasible, from inappropriate access, modification, dissemination, and destruction.

Physical Safeguards

Physical safeguards address the protection of physical computer systems and related

buildings and equipment from fire, other natural and environmental hazards, and intrusion. Physical safeguards include physical security access, card access solutions, paper destruction procedures, and computer room access. The use of locks, keys, and administrative measures used to control access to all computing systems and facilities management is also included. Figure 2 summarizes standards and implementation specifications defined in the Physical Safeguards category.

Figure 2: Physical Safeguards—Standards and Implementation Specifications

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

Physical safeguards are physical measures and policies and procedures to protect a covered entity's electronic information system and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

Technical Safeguards

Technical safeguards refer to the technology and the policy and procedures for its use that protect electronic PHI and control access to it. Figure 3 summarizes standards and implementation specifications defined in the Administrative Safeguards category.

Figure 3: Technical Safeguards—Standards and Implementation Specifications

Standards	Implementation Specifications	R = Required A = Addressable
Access Control	Unique User Identification Emergency Access Procedure Automatic Logoff Encryption and Decryption	R R A A
Audit Controls		R
Integrity	Mechanism to Authenticate Electronic PHI	A
Person or Entity Authentication		R
Transmission Security	Integrity Controls Encryption	A A

The final Security Rule makes no distinction between internal networks and external networks—both need to be secured. Furthermore, the final Security Rule covers electronic PHI at rest (that is in storage) as well as during transmission. Covered entities must protect electronic PHI when they transmit information. The final Security Rule requires protection of the same scope of information as that covered by the Privacy Rule, except that it only covers that information if it is in electronic form. Per the final Security Rule, a covered entity's responsibility to implement security standards extends to the members of its workforce, whether they work at home or on-site. Documentation related to the final Security Rule implementation must be retained for a period of 6 years.

Electronic Signatures/Transactions

The proposed Security Rule did not require the use of an electronic signature, but specifies the standard for an electronic signature that must be followed if such a signature is used. If an entity elects to use an electronic signature, it must comply with the Electronic Signature Standard. However, the final Security Rule adopts

only security standards. The final Rule for electronic signatures will be published at a later date. Hence, only a brief description of the proposed Electronic Signature Rule is provided in this article.

Electronic transmissions would include transactions using all media, even when the information is physically moved from one location to another using magnetic tape, disk, or compact disc (CD) media. Transmissions over the Internet, Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, and private networks are all included.

Electronic Signatures

Electronic signatures are specifically excluded from the final Security Rule. The proposed Security Rule did identify Electronic Signatures as an optional requirement. Covered entities are not required to implement electronic signatures. It is likely that in the near future we may see a final Rule specifically related to Electronic Signatures. Figure 4 summarizes standards and implementation features for Electronic Signatures defined in the Proposed Security Rule.

Figure 4: Electronic Signature—Based on Proposed Security Rule

Electronic Signature Requirement (From Proposed Rule)	Implementation Features (From Proposed Rule)
Digital signature (If digital signature is employed, the following 3 implementation features must be implemented: <ol style="list-style-type: none"> 1. Message integrity 2. Nonrepudiation 3. User authentication Other implementation features are optional.	<ul style="list-style-type: none"> • Message integrity • Nonrepudiation • User authentication • Ability to add attributes • Continuity of signature capability • Counter signatures • Independent verifiability • Interoperability • Multiple signatures • Transportability

The proposed Security Rule contained multiple proposed “requirements” and “implementation features.” In the final Security Rule, the term “requirement” is replaced with “standard” and the term “implementation feature” is replaced with “implementation specification.”

Pharmacy Implications

In the final Security Rule, the implementation specification may either be a required implementation specification or an addressable implementation specification. The concept of addressable implementation specifications is to provide covered entities additional flexibility with respect to compliance with the security standards. A covered entity will do one of the following for addressable implementation specifications:

- Implement one or more of the addressable implementation specifications
- Implement one or more alternative security measures
- Implement a combination of both

- Not implement either an addressable implementation specification or an alternative security measure

After its own risk analysis, risk mitigation strategy, an assessment of what security measures may already be in place and the cost of implementation of the covered entity must decide these issues:

- If a pharmacy determines that a given addressable implementation specification is reasonable and appropriate for its operation, then the pharmacy must implement it.
- If a pharmacy determines that one of the addressable implementation specifications is not inappropriate and/or is an unreasonable security measure, but the standard cannot be met without implementation of an additional security safeguard, the pharmacy may implement an alternate measure that accomplishes the same end as the addressable implementation specification.

An entity that meets a given standard through alternative measures must document the decision to not implement the addressable implementation specification, the rationale behind that decision, and the alternative safeguard implemented to meet the standard. A covered entity may also decide that a given implementation specification is simply not applicable (i.e., neither reasonable nor appropriate) to its situation, and that the standard can be met without implementation of an alternative measure in place of the addressable implementation specification. In this scenario, the covered entity must document the decision not to implement the addressable specification, the rationale behind that decision, and how the standard is being met.

For example, under the information access management standard, an access establishment and modification implementation specification reads, “implement policies and procedures that, based upon the entity’s access authorization policies, establish, document, review, and modify a user’s right of access to a workstation, transaction, program, or process.” It is possible that a small practice, with one or more individuals equally responsible for establishing and maintaining all automated patient records, will not need to establish policies and procedures for granting access to that electronic protected health information because the access rights are equal for all of the individuals.

Approach and Philosophy

These security measures by pharmacies must be documented and kept current. The regulations explicitly recognize that very small organizations will be able to satisfy the requirements with less elaborate approaches than larger, more complex organizations. Keep in mind that the

HIPAA security standards are designed to be the following:

- **Comprehensive**—They cover all aspects of security safeguards, such as:
 - Identification
 - Authentication
 - Access Control
 - Accountability and Nonrepudiation
 - Integrity
 - Communications
 - Administration
- **Technology neutral**—Standards can be implemented using a broad range of off-the-shelf and user-developed technologies and security solutions.
- **Scalable**—The goals of the regulations can be achieved by entities of all sizes from single practitioners to large multi-national health care organizations.

The Security Rule does not address the extent to which a particular entity should implement the standards and implementation specifications. Instead, the Security Rule requires that each covered entity assess its own security needs and risks and devise, implement, and maintain appropriate security to address its business requirements. How individual security requirements would be satisfied and which technology to use would be business decisions that each organization would have to make.

Security Principals

Security of health information is especially important when health information can be directly linked to an individual. For example, confidentiality is threatened not only by the risk of improper access to electronically stored information, but also by

the risk of interception during electronic transmission of the information.

The Security Rule consists of the requirements that a health care entity must address in order to safeguard the confidentiality, integrity, and availability of its electronic data. It also describes the implementation features that must be present in order to satisfy each requirement. The central principals of security are stated below:

- *Confidentiality*
- *Integrity*
- *Availability*

Security-related impairment generally includes, but is not limited to, “damaging disclosure or the asset to unauthorized recipients (*loss of confidentiality*), damage to the asset through unauthorized modification (*loss of integrity*), or unauthorized deprivation of access to the asset (*loss of availability*).”

The Security Rule requires that each health care entity engaged in electronic maintenance or transmission of health information assess potential risks and vulnerabilities to the individual health data in its possession in electronic form; and develop, implement, and maintain appropriate security measures. Most importantly, these measures must be documented and kept current.

Definitions and Security Terminology

In this section some key security terms and definitions emphasized in the final Security Rule are reviewed.

Definitions

Security is minimizing the vulnerability of assets and resources. Security is generally defined as having controls, countermeasures, and procedures in place to ensure the

appropriate protection of information assets and control access to valued resources. Security or security measures encompass all of the administrative, physical, and technical safeguards in an information system.

An asset is defined as anything of value.

Vulnerability is any weakness that could be exploited to violate a system or the information it contains.

A threat is a potential violation of security.

Basic Security Terminology

- Authentication
- Access control
- Confidentiality
- Integrity
- Nonrepudiation
- Availability

Authentication is typically the first step in gaining access to the system. Authentication means the corroboration that a person is the one claimed. Typing a username and a password is an example of authenticating yourself as a user on the system. Kerberos is an example of a network authentication protocol designed to provide strong authentication for client/server applications by using secret-key cryptography. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. Authentication is the process of “proving” your identity. A system needs to authenticate users to a degree appropriate for the level of risk/threat that an authenticated user represents.

Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Access control provides protection against the unauthorized use of resources accessible using network protocols. Permissions for files, directories, and processes relate to the area of access control (i.e., who has access to these resources [objects] on the system). Access control relates to what resources a user or service may access on the system or network.

Access control refers to a method of restricting access to resources, allowing only privileged entities access. Types of access control include, among others:

- Mandatory Access Control
- Discretionary Access Control
- Time of day
- Classification

Confidentiality is about the protection of data from unauthorized disclosure. Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Confidentiality relates to secrecy of data on the system and network. Confidentiality is about protecting your data from passive threats.

Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner. Integrity provides protection against active threats.

Repudiation is defined as the denial by one of the entities involved in a communication of having participated in all or part of the communication.

Availability is the property that data or information is accessible and usable upon demand by an authorized entity or person.

Other Terminology from Final Security Rule

In this section other definitions included in the final Security Rule are summarized.

Administrative safeguards are administrative actions and policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Facility means the physical premises and the interior and exterior of a building(s).

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Malicious software means software, for example, a virus, designed to damage or disrupt a system.

Password means confidential authentication information composed of a string of characters.

Physical safeguards are physical measures and policies and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Technical safeguards mean the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

User means a person or entity with authorized access.

Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

Privacy Rule and Flow of PHI

As a pharmacy entity begins to analyze the requirements for implementation in the Security Rule, it is also imperative that 2 additional areas be addressed prior to the determination of potential solutions in the areas of security policy, procedures, architecture design, and technologies:

- Privacy Rule, with emphasis on the administrative requirements and the flow of PHI—both internal and external
- Threats to the health care infrastructure

Privacy Rule Compliance Requirements

In this section, the administrative requirements associated with the Privacy Rule are analyzed. We examine potential threats to the health care enterprise in the next section.

The key steps that a pharmacy needs to consider to meet HIPAA Privacy Requirements are:

1. Administrative requirements
 - a. Assigned responsibility
 - b. Development of policies and procedures
 - c. Safeguards
 - d. Documentation
 - e. Training
 - f. Complaints
 - g. Sanctions
 - h. Mitigation
 - i. No Intimidation Acts
 - j. No Waiver of Rights
2. Identify and assess organization PHI.
3. Analyze gaps in current policies.
4. Adjust organizational processes.
5. Negotiate Business Associate Contracts.

There are several administrative requirements that relate to the Privacy Rule. These include:

1. Assigned responsibility
 - a. Privacy Official
 - b. Contact person for complaints
2. Development of policies and procedures
 - a. Notice of Privacy Practices
 - b. Consent (optional)
 - c. Authorization
3. Safeguards
 - a. Administrative
 - b. Technical
 - c. Physical
4. Documentation
 - a. Creation
 - b. Maintenance
5. Training
 - a. HIPAA Privacy Requirements: Overview
 - b. HIPAA Security Requirements: Overview
 - c. PHI policies and procedures
6. Complaints
 - a. Process
 - b. Documentation
7. Sanctions
 - a. Policy

- b. Documentation
- 8. Mitigation
- 9. No Intimidation Acts
- 10. No Waiver of Rights

Business Associates

Business associates are entities that act on behalf of the pharmacy in doing one of the pharmacy's acts (tasks). Business associates act as though they are the covered entity. There are a few key steps that a pharmacy must follow to address the Privacy Rule requirements related to business associates. First, the pharmacy needs to identify the entities that are business associates. This is a key responsibility of the Privacy Officer. An example of a business associate is a billing service that submits claims to insurance carriers.

The 2 questions that need to be asked as the Privacy Officer determines which organizations are possibly business associates of the pharmacy are:

- Does the entity provide services on behalf of your pharmacy?
- Do any of those services performed require access to PHI?

Once the list of business associates that meets the criteria defined have been determined, then the next step is to establish appropriate assurances in the written agreement. All business associate contracts must be stored safely, as it may be required for audit or other compliance activities. The Business Associate Contract (BAC) should address the following key points:

- Limit use and disclosures of PHI as permitted by state or federal law.
- Limit the use and disclosure of PHI to terms of the agreement.
- Bind all BAC agents and subcontractors to the agreement.

- Business associate must report all unauthorized uses and disclosures to your pharmacy.
- Your pharmacy must be permitted to take "reasonable steps" to correct any misuse of PHI, including canceling the contract without penalty.
- Must assist the covered entity with patient rights, such as request for patient records and amendments.

The final phase of addressing business associates is to monitor their performance. Your pharmacy needs to be sure that if business associates disclose PHI without proper authorization, then you are positioned to take reasonable steps to correct the misuse. Keep in mind that in determining if a covered entity is properly monitoring business associates HHS will consider if a "reasonable person" should have known of any inappropriate disclosures.

It is the responsibility of the Privacy Officer to determine new relationships with entities that may be business associate relationships and then require them to enter into a business associate agreement. The Privacy Officer must review all business associate agreements. The Security Officer needs to be aware of the business associates, their BACs and use that information within the context of developing the enterprise security policy as well as defining the security architecture.

Threats to Pharmacy Infrastructure

In this section, potential threats to electronic communication and information systems in an enterprise pharmacy infrastructure are described.

Types of Attacks

There are many different types of attacks that may be launched by hackers on the

pharmacy network. Pharmacies are even more vulnerable than other health care entities, as they typically communicate over open networks such as the Internet. These threats to pharmacy networks include:

- Denial of Service (DoS) attacks
- Distributed Denial of Service (DDoS) attacks
- Spoofing or masquerading
- Password cracking applications
- Malicious software attacks

Denial of Service Attacks

Denial of Service (DoS) attacks can be disruptive for any pharmacy organization. In a DoS attack the attacker does not gain unauthorized access to a resource. Instead the hacker's action leads to the loss of access to a resource. The resource may be the network, central processing unit (CPU), memory, or disk. A DoS attack results in a resource being overloaded, such as disk space, network bandwidth, internal tables of memory, or input buffers (buffer overflow). The overload causes the host or particular service to become unavailable for legitimate use. This could be blocking access to a resource all the way up to causing a host to crash. There are numerous DoS attacks, and the solutions to them are not always easy. Some attacks, such as Internet Control Messages Protocol (ICMP)-based attacks, can be blocked with filters. Others can be as simple as turning the particular service off if it is not needed.

Distributed Denial of Service Attacks

Distributed Denial of Service (DDoS) attacks result in hundreds if not thousands of systems being used to launch attacks across many systems in the pharmacy network. Such attacks result in extreme bandwidth use, high router processing use, as well as high system usage by unauthorized software installed on victim sites. Hackers first break

into weakly secured hosts using common security holes in the operating system or network protocols. Once such systems are compromised then the attacker installs DDoS software to launch coordinated attacks on victim sites.

Spoofing or Masquerading

Spoofing is where one host or entity falsely assumes (masquerades as) the identity of another host or entity. The Man-in-the-Middle attack depends upon convincing 2 hosts that the computer in the middle is the other host. This is accomplished with a domain name spoof if the system is using Domain Name System (DNS) to identify the other host or Address Resolution Protocol (ARP) spoofing on the Local Area Network (LAN).

Password Cracker Applications

A password cracker application is any program that compromises password security by revealing passwords that have previously been encrypted. For example, a hacker may encrypt every word in the dictionary (spelled forwards and backwards and other combinations) using the Data Encryption Standard (DES). The encrypted password is then compared with the target password. If there is a match, then there is a very high chance that the password was cracked (over 98% chance). Password cracker applications are very effective in determining poorly selected passwords. Examples of passwords cracker applications include:

- L0phtCrack 2.0 (NT password cracking tool)
- ScanNT, NTCrack, Password NT (other NT password cracker programs)
- Crack (UNIX password cracking program)

- CrackerJack (cracks UNIX passwords)

Each organization needs to define its password policy, and this must require at a minimum:

- Passwords of a minimum length (6 to 8 characters)
- Combinations of alphanumeric characters
- Users to change their password every 30 to 60 days
- Users to not be able to select previously used passwords

Malicious Software

Malicious software refers to viruses, worms, Trojan horses, and backdoor programs. Malicious software either has negative behaviors or is used by attackers to further their goals of attacking enterprise networks and systems. The key difference between the types of malicious software is their means of spreading. The HIPAA Security Rule includes “protection from malicious software” as an addressable implementation specification. It refers to procedures for guarding against, detecting, and reporting malicious software.

Virus

A virus is a program that attaches itself to files on the target system. A virus is a self-replicating program that spreads by infecting other programs. During attachment the virus’s original code is appended to victim files; this is referred to as infection. At this point, when the file is infected it is converted from an ordinary file to a carrier. This infected file can infect other files; this is referred to as replication. The replication of files can spread across to the hard disk leading to systemic infection.

Once the virus attaches itself to an executable file, such as files that end in .exe or .com, each time the file is executed it will infect other files. Macro viruses infect data files such as documents generated in Microsoft Word or PowerPoint. These viruses typically attack your global document templates, ultimately damaging each and every document type opened with the application. Recent examples of viruses include Melissa, Babylonia, and Loveletter. There are basically 3 types of viruses:

- Master boot sector viruses
- Boot sector viruses
- File viruses

File viruses can spread system-wide, while boot sector viruses attack a small portion of the disk. Viruses may also be:

- Stealth viruses
- Polymorphic viruses

Stealth viruses use a number of techniques to conceal that a drive has been infected. Polymorphic viruses are much more complex—these viruses can change, making it extremely difficult to identify. The process of viruses changing is called mutation. In mutation the virus may change its size and composition, thus evading detection by virus detection software. To address this challenge, virus detection software creates scanners that can identify encryption and other patterns.

Virus attacks are significant in that they cause substantial damage and can be costly. Vendors such as Symantec (www.symantec.com), McAfee Security (www.mcafee.com), and Trend Micro (www.antivirus.com) offer products to help businesses defend against virus attacks.

Trojan Horse

Trojan horse programs are another type of malicious code. A Trojan horse is unauthorized code contained within a legitimate program that performs functions unknown to the end user. It may also be a legitimate program that has been altered by the placement of unauthorized code within it and performs functions unknown to the end user. The Trojan horse program does something more than what is expected by the end user, and typically will result in some damage or transmission of information that is sensitive, such as e-mailing the password file. Examples of Trojans include ILOVEYOU, StuffIt 4.5 Trojan (would delete key system files), and AOL Password Trojan (would reveal your AOL username and password).

Worms

A worm is a self-contained program that uses security flaws such as a buffer overflow to remotely compromise a system and then replicate itself to that system. Unlike viruses, worms do not infect other executable programs, but instead install themselves on the victim system as a stand-alone entity that does not require the execution of an infected application. Worms exploit known vulnerabilities in systems and applications. They then spread themselves. To protect against worm attacks, a comprehensive solution that includes anti-virus software, as well as an intrusion detection system (IDS), is required.

Examples of worm attacks include Code Red, Code Red II, and Nimda. The Code Red worm exploited a known vulnerability in Microsoft IIS 4.0 and 5.0. The worm operated by creating a random list of Internet Protocol (IP) addresses, which it then scanned for the IIS vulnerability. If the worm found a target system with the

vulnerability, it executed the buffer overflow exploit, which resulted in the worm's code being loaded onto and executed by the victim system. The worm then began to propagate itself from the just compromised system. After 2 hours, the worm changed the server's Web page.

Significant Threat

Throughout history, business transactions have almost always been face to face. The Internet and e-business applications, in particular, are transforming the fundamentals of trust in business transactions. The identity of the person on the other side of an e-business transaction is hard to determine. It is also not easy to establish the identity of the person on the business side of the transaction. The other threats to all businesses, including industry verticals such as health care, insurance, financial, government, and others include these 3 threats listed below:

- Attackers (black hats) can take down or vandalize your vital systems.
- Attackers can steal your valuable customer information.
- Your enterprise/corporate data can be abused/misused.

Blackhats, also referred to as hackers (crackers), have one mission—to attack, disrupt, and exploit systems within the business infrastructure. As you design the security architecture for your enterprise, it is important to understand the threat from blackhats to sensitive health care data and systems.

Knowing your customer, partner, and employee are becoming vital issues as businesses look to provide more information and engage in payment of medical transactions online.

Strong authentication requires 2 or more of the following forms:

- What you know (password, PIN)
- What you have (smart card, token)
- Who you are (biometrics)

The problem with passwords is serious—passwords are frequently written down and left in insecure places.

Protecting the Pharmacy Infrastructure

In this section, the security technology options that may be considered by pharmacies to meet Security Rule compliance requirements are examined.

Privacy Requirements: Starting Point for Security Implementation

Privacy and security are addressed separately under HIPAA and, therefore, 2 distinct rules were established. In the context of HIPAA, privacy defines who is authorized to access information and includes the right of individuals to keep information about themselves from being disclosed. “Security,” in this context, is the ability to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction, or loss.

Achieving even a base level of this type of security can be harder than one might think. Software, argues John Pescatore, a Gartner (refer to Gartner Group website, www.gartner.com) Research Vice President, “can be made to do whatever any clever programmer wants it to do; however, it is more difficult to prevent software from doing what you don’t want it to do. Even worse, even if you succeed at that, it is nearly impossible to keep someone else from changing the software to do what you don’t want it to do.”

In a HIPAA-compliant environment where certainty, reliability, and carefully proscribed access to information is key, software’s fluidity, relatively weak self-protection, and constant state of flux can make it an inappropriate foundation for protecting your highest-value information assets. Mr. Pescatore concluded that hardware provides “high levels of security by being more difficult to change than software.” For systems that are relatively stable and must resist modification, he states, “Hardware will be required to provide an appropriate level of security.”

Pharmacies and their business associates will be held accountable for inappropriate disclosures of patient information and will be expected to implement administrative changes to protect information. The Privacy Rule covers the policies and procedures that must be in place to ensure that the patients’ health information is protected and their rights are upheld.

The Security Standard is a companion to the Privacy Rule—in order to protect the information, pharmacies will be expected to put in place security safeguards. Complementing the Security Rule, the HIPAA Privacy Rule defines who is authorized to access patient-identifiable information. It also establishes the rights of individuals to keep information about them from being disclosed. The provisions of the Privacy Rule overlap with the Security Rule in some areas, especially with the emphasis in the final Security Rule. Pharmacies will need the assistance of skilled security professionals and architects for a successful implementation of HIPAA-related security assessment, policies, and technologies.

Secure Information Delivery

The HIPAA Administrative Simplification Title is really about secure information

delivery between administrators, patients, and caregivers. It is about the electronic capture, transformation, and delivery across the health care industry entities. The health care industry has traditionally been impeded by:

- Limited technology budgets
- Multiple proprietary systems
- Multiple legacy systems
- Paper-based processes

The mandated HIPAA regulations are the catalyst to improve processes and information flow throughout the pharmaceutical industry.

As a direct consequence of health care transactions, it is becoming much more important to protect patient and medical information. This requires the health care organization to build a secure infrastructure.

Thus, the HIPAA-compliant health care organization is one that would use Electronic Data Interchange (EDI) for transactions, protect patient's medical information with a combination of Notice and Authorization, and secure all electronic medical records and transactions. This is the health care industry implementing e-business.

Security Implementation Considerations

HIPAA is highly likely to result in pharmacies investing in a trust framework for enterprise systems (Internet, intranet, and extranet) and security policies. Why is trust important? It is because a trusted infrastructure can make Internet-based pharmaceutical transactions as secure as face-to-face transactions.

A trusted infrastructure deals with the reality that the inside and outside of an enterprise are becoming one. Building a trusted

infrastructure is the next "infrastructure" challenge for all businesses. It is increasingly becoming a core requirement for a pharmacies' enterprise infrastructure. The HIPAA legislation will result in the establishment of a trusted infrastructure as a priority in the pharmaceutical industry.

The key for HIPAA compliance is to build a secure infrastructure. The key components of a secure infrastructure include technologies in 2 key areas of security: Defense and Trust.

Examples of defense-based security technologies include:

- Firewall systems
- Intrusion Detection Systems (IDS) and detection of malicious software
- Secure Virtual Private Networks (VPNs)

Examples of security technologies that enable trust include:

- Encryption
 - Public Key Infrastructure (PKI)
- Strong Authentication
 - Biometrics
 - Authentication tokens
 - Smart cards

HIPAA's security requirements do not mandate a particular security technology. The rule describes the requirements, and it is up to each individual organization to determine how to best meet these requirements. HIPAA does have specific requirements in the areas of authentication, access control, data integrity, encryption and nonrepudiation.

Summary

The core objective of HIPAA is to protect individuals from the unapproved and

unwarranted release of information related to their personal health. The focus of the HIPAA Privacy Rule is to address the intentional release of health-related information. Its purpose is to restrict the disclosure and use of the information to entities approved in advance by the individual. “Intentional release” is generally defined as outside the bounds of reasonable and diligent attempts to prevent such release.

In this article, we reviewed the objective of HIPAA’s Security Rule to protect the storage and transmission of electronic PHI. The Security Rule addresses the steps that the covered entity must take to prevent the unauthorized disclosure, destruction, and corruption of PHI maintained or transmitted by covered entities. The identification of solutions to meet the requirements of the Security Rule must take into account:

- HIPAA Security Rule standards and implementation specifications that must be supported by the pharmacy enterprise
- Threats to the pharmacy entity
- Requirements related to the Privacy Rule such as flow of PHI and business associates

The final Security Rule consists of the requirements that a pharmacy must address in order to safeguard the confidentiality, integrity, and availability of its electronic data. The recommendations from the Security Rule state that all organizations that handle electronic PHI—regardless of size—should implement and address standards and implementation specifications identified in the categories of administrative, physical, and technical safeguards.

The standard does not address the extent to which a particular entity should implement

the specific features that have been defined. The final Security Rule requires that each health care entity engaged in electronic maintenance or transmission of health information assess potential risks and vulnerabilities to the individual health data in its possession in electronic form. It should then develop, implement, and maintain appropriate security measures.

Most importantly, these measures must be documented and kept current. How individual security requirements are satisfied and which technologies are used are business decisions that each pharmacy organization must make. Pharmacies should view the HIPAA Security Rule as a starting point, not an end point, and should go beyond HIPAA security requirements in defending business assets and information.

References

1. Health Insurance Reform: Security Standards, Final Rule, 45 CFR Parts 160, 162 and 164. Retrieved from <http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-3877.pdf>.
2. Final Privacy Rule Information on Electronic Transactions As It Relates to the Pharmacy Industry. National Council for Prescription Drug Programs. Retrieved from <http://ncpdp.org/PDF/finalrule.pdf>.
3. Health Insurance Portability and Accountability Act. American Medical Association. Retrieved from <http://www.ama-assn.org/ama/pub/category/4234.html>.
4. Health Insurance Portability and Accountability Act of 1996: Title I Statutory Text. Retrieved from <http://cms.hhs.gov/hipaa/hipaa1/content/HIPAASTA.pdf>.

5. Health Insurance Reform: Modifications to Transactions and Code Sets Standards for Electronic Transactions. U.S. Department of Health and Human Services. Office of the Secretary. 45 C.F.R. Part 162.

6. Health Insurance Reform: Standards for Electronic Transactions; National Standard Health Care Provider Identifier; Proposed Rules. U.S. Department of Health and Human Services. Health Care Financing Administration. 45 C.F.R. Part 142. Retrieved from <http://aspe.hhs.gov/admsimp/nprm/txnprm.pdf>.

7. Health Insurance Reform: Standard Unique Employer Identifier. U.S. Department of Health and Human Services. Office of the Secretary. 45 C.F.R. Parts 160, 162. Retrieved from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002_register&docid=02-13616-filed.pdf.

8. Health Insurance Reform: Standards for Electronic Transactions; Announcement of Designated Standard Maintenance Organization; Final Privacy Rule and Notice. U.S. Department of Health and Human Services. Office of the Secretary. 45 C.F.R. Parts 160, 162. Retrieved from <http://aspe.hhs.gov/admsimp/final/txfinal.pdf>.

9. HIPAA Administrative Simplification. Centers for Medicare and Medicaid Services. Retrieved from <http://www.cms.hhs.gov/hipaa/hipaa2/default.asp>.

10. HIPAA Administrative Simplification. U.S. Department of Health and Human Services. Office of the Secretary. 45 C.F.R. Parts 160, 164.

Services. Retrieved from <http://aspe.os.dhhs.gov/admsimp/>.

11. HIPAA Insurance Reform. Centers for Medicare and Medicaid Services. Retrieved from <http://cms.hhs.gov/hipaa/hipaa1/default.asp>.

12. Nondiscrimination in Health Coverage in the Group Market; Interim Final Privacy Rules and Proposed Rules. U.S. Department of Health and Human Services. 45 C.F.R. Part 146. Retrieved from <http://cms.hhs.gov/hipaa/hipaa1/content/nondiscr.pdf>.

13. Privacy of Health Records. Office for Civil Rights. Retrieved from <http://www.hhs.gov/ocr/hipaa/finalreg.html>.

14. Protecting Your Health Insurance Coverage. U.S. Department of Health and Human Services. Retrieved from <http://cms.hhs.gov/hipaa/hipaa1/content/protect.pdf>.

15. Security and Electronic Signature Standards; Proposed Rule. U.S. Department of Health and Human Services. Office of the Secretary. 45 C.F.R. Part 142. Retrieved from <http://aspe.hhs.gov/admsimp/nprm/secnprm.pdf>.

16. Standards for Privacy of Individually Identifiable Health Information; Final Privacy Rule. U.S. Department of Health and Human Services. 45 C.F.R. Parts 160, 164. Retrieved from <http://www.hhs.gov/ocr/hipaa/dates.pdf>.

17. Technical Corrections to the Standards for Privacy of Individually Identifiable Health Information. U.S. Department of Health and Human Services. Retrieved from

<http://www.hhs.gov/ocr/pvcfix01.pdf>.

18. Electronic Health Care Transactions and Code Sets Standards Model Compliance

Plan. U.S. Department of Health and Human Services. Retrieved from

<http://cms.hhs.gov/hipaa/hipaa2/ASCAForm.pdf>.