Privacy & Security Toolkit

Managing Information Privacy & Security in Healthcare

A Primer on Health Information Security

By Greer Stevenson

BACKGROUND

The Security Rule component of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 makes compliance with its requirements mandatory for covered entities (CEs); all health plans, health care clearinghouses, and health care providers who transmit any electronic protected health information (ePHI). The 2013 Omnibus Rule made business associates (BAs) and their subcontractors liable for meeting compliance with the Security Rule as well. The Security Rule requires CEs and BAs to employ reasonable and applicable administrative, physical, and technical safeguards to protect personally identifiable health information that is stored or transmitted electronically from any reasonably foreseeable threats or risks. The statement "any foreseeable threats or risks" covers a magnitude of both internal and external evils and mishaps; yet, the demands of the Security Rule are not overwhelming, indeed they are sound business practices. This is reinforced by the use "employ reasonable" to quantify safeguards.

Below is an overview of security concepts and regulation review. Resources are provided for further details and guidance.

Basic Security Concepts

Information security is achieved by implementing policies and procedures as well as physical and technical measures that deliver CIA.

- Confidentiality is the protection of information from unauthorized access or disclosure.
- Integrity is the protection of information from unauthorized change (deliberate or accidental).
- Availability permits the use of information as intended by ensuring that the information and other required resources are accessible for use whenever needed including during emergencies and disasters. Access is based on the individual's role and is provided on a need-to-know basis.

Additional basic security concepts are:

- Accountability involves the concepts of answerability, responsibility, blameworthiness, liability and other terms associated with the expectation of account-giving.[1]
- Non-repudiation is an information technology service that provides proof that an action took place, can be verified by a third party with high assurance, and can not subsequently be refuted. It most often is applied to authentication or approval but may also involve information integrity, origin, submission, sending, transport, receipt, delivery and knowledge.

[1] http://en.wikipedia.org/wiki/Accountability

BUILDING A STRONG SECURITY FOUNDATION

A security program must protect the confidentiality, integrity, and availability of the data identified by HIPAA, other Federal and State laws and regulations, and/or management. A security program requires the identification of the resources to be protected, along with threats to and vulnerabilities of the resources (risk assessment) and the development of a plan to manage the associated risks (risk management).

A security program has a set of objectives, stated clearly and concisely in policies and standards, based on system functionality, mission requirements, and available resources. The plan provides the foundation of the security architecture and is based on the technology and process that creates, maintains, processes, transmits, and/or stores the information to be protected. The plan is driven by a formal risk assessment that covers the information technology systems and their infrastructure. The essential resources that will be required are people, supporting processes, physical facilities and technology. The methodology used to verify how well the objectives are met consists of testing, review, vigilance, documentation and re-testing (verification). This approach for developing a security program can be used by any organization, regardless of its size.

RISK MANAGEMENT

Health information must be managed in a way that allows healthcare organizations and its business processes to continue unhampered despite the presence of threats and during emergencies. Risk management involves the process of assessing risk and developing strategies to reduce risk to an acceptable level. It depends on a formal process and results in security policies, standards, procedures, business continuity plans, disaster recovery plans, technology, security awareness and training, liability insurance, and acceptance of residual risks. Risk management provides the process for making informed business decisions that assign appropriate resources to mitigate the risks to the organization's information proportional to its value. Each organization needs to determine the level of risk they believe appropriate to their business needs and culture. Some organizations will be more risk averse than others. To find this equilibrium, all business processes must be identified. These will include those processes that cover the access, storage, use, disclosure, and transmission of health and confidential data that are required by law, the health profession, ethics, and/or management to be protected together with the supporting systems and infrastructures.

Risk Assessment

A risk assessment is a fundamental part of risk management. It will identify the information assets of the organization that have value and must be protected. Risk assessments are more complex in larger organizations (HCOs) than in small ones. It requires individuals with skills in security management, and personnel from all of the functional areas who are familiar with the business processes, organizational culture, and laws that affect the particular business area (e.g. financial, clinical, health information management, and third party agreements/contracts). By requiring input from all functional areas, an HCO can achieve consensus and support from all areas and ensure that all available knowledge is utilized to thoroughly protect the entity. Executive support is imperative. Without executive support, the risk assessment will almost certainly be a failure from the start because other departmental responsibilities will take a higher priority.

A risk assessment will help an organization answer the following questions:

1. What assets must the HCO protect?
2. From whom or what do these assets need to be protected?
3. What and how large is the harm that might come from a failure of protection?
4. What and where are the vulnerabilities or weakness of our HCO that might be exploited?
5. What level of protection is required to block these vulnerabilities and threats?
6. How much time, effort, and money should I spend to protect it?

The answers to these questions will provide information to assist with decisions on how much should be spent to protect assets, data, and/or process with technology, physical infrastructure changes, or security policies and training. The asset's value, magnitude of the other costs associated with its loss and the likelihood that it will occur must be considered. For example, the risk analysis can assist management in determining if spending $500,000 to protect a system that has a tangible liability of $250,000 but an intangible liability (due to bad publicity) of $600,000 is justified. If the probability of the threat occurring is high, the expense may be appropriate. The value of an asset should be determined by considering multiple parameters such as cost of acquisition or development, cost to maintain and protect the asset, value to the organization, replacement cost, lost productivity, and liability to the organization. Intangible losses such as the HCO's goodwill or reputation should also be considered.

A thorough risk assessment will, also, provide valuable disaster recovery and business continuity planning information. If the data and/or systems are not available when needed, the goals of the security plan will not have been met. Disaster recovery and business continuity plans require, at a minimum, yearly testing, revision, and updating of documentation. The actual timeline for testing plans may vary by organization based on their assessment of the criticality of the applications.

Additionally, it is important to remember that risks change. Risks should be reassessed as management viewpoints change, processes or any related supporting activity or technologies are modified, and with new or revised legislation and regulations.

PEOPLE

People affect, and are affected by security. People may contribute to better security in many ways such as by recognizing malicious software, reporting incidents, assisting security guards with a vigilant eye, reporting suspicious actions to appropriate authorities, and filling responsible security positions (security officer, department security coordinator, security trainers, etc.). On the other hand, people are often the source of vulnerabilities when they allow others to use their passwords, or access a database for more than "minimum necessary" information.

Security tends to interfere with individual's work lives through extra training requirements, sanctions, and changes in daily workflow. Thus, HCOs should endeavor to implement its security program with good planning, care and effective methods. For example, training given via simple policy review or presentations work for quick basic knowledge but result in poor retention. Many learning management systems now exist to bring basic HIPAA training to an HCO's workforce. Methods for augmenting mandated training include helpful reminders in the form of screen savers or cartoons in an HCO's newsletter. The use of staff meetings to briefly remind everyone not to share their passwords or discuss patient information in the elevator helps avoid two common breaches. People have a tendency to revert back to insecure behaviors unconsciously unless there is continual reinforcement of appropriate behaviors. Vigilance, loyalty, training,

and commitment tend to make security mishaps occur less often and allow them to be spotted more quickly.

Sanctions

The privacy and security rule mandates a policy covering sanctions for violations but sanctions alone do not stop violations. It is important to ensure that all policies are enforced at all levels equally and forcibly. Tolerating policy or procedure violations will undermine a security program, particularly favoritism shown to executives or physicians.

People also play an important role in enhancing security through vigilance in open areas of a facility and around work areas but most of all with new ideas on how to incorporate security measures into the organization. HCOs should solicit these ideas from their staff and regularly offer a reward and recognition for ideas that most enhance security.

POLICIES, PROCEDURES, STANDARD AND GUIDELINES

Policies describe how the organization plans to protect the HCO's tangible and intangible information assets. Policies include generalized requirements approved at the HCO's executive level that indicate a course of action to personnel who must make decisions. Policies should be reviewed on, at least, an annual basis if not more, dependent upon changes in law and/or technology. Standards, procedures, and guidelines supplement these requirements by tailoring policies for specific departments. Standards state specific minimum requirements dictated by an entity's policies; are definitive; and required. Procedures give a method and instructions by which a policy is accomplished. Procedures are normally tailored for applicable departments as not all departments need to meet the requirements of a policy at the same defined level. Guidelines are suggestions for accomplishing a certain task. HIPAA requires documentation for the policies, standards, and procedures as verification that entities are in compliance with the regulation. All the required aspects as defined in the Security Rule must be complied with and the addressable standards must be documented as being analyzed and accepted or replaced or not required with the reason for rejection. This documentation is also used for training and review when changes to processes occur.

Policies

The security officer should work with representatives of departments using the systems and data, management and other functional experts to develop and implement policies. A good model for policy content is:

1. Objective of the policy – What you are trying to achieve by implementing the policy;
2. Purpose of the policy – Why it was adopted and how it will be implemented (broad terms);
3. Audience – To whom the policy applies;
4. Policy statement – Body of the policy (specifics of how it will be implemented) ;
5. Exceptions to the policy; and
6. Definitions (if necessary).
7. Who to contact for questions or interpretation

Processes

An HCO should develop, document and annually review administrative and physical processes. Important processes include how to handle fires, water damage from putting fires out, chemical spills, and acts of

nature emergencies. These occurrences may never happen but when they do they will affect your security posture and systems. Other important processes include those for hiring, approval for data and system access, security training, incidents reporting and investigations, physical access protocols, and termination of employment. Particular attention should be paid to voluntary and involuntary termination of employment to ensure that data and system access is disabled and that keys and identification badges are collected.

Physical Facilities

Protection of access to the physical facilities that house information technology is required by the Security Rule. "Physical access controls should permit entry to individuals with appropriate authorization and deny entry to individuals lacking appropriate authorization. This standard requires limiting physical access both to the general building or business suite and to areas dedicated to the storage and use of computer equipment and media. Four addressable implementation specifications supplement this mandatory requirement, including contingency operations, facility security plan, access control and validation procedures, and maintenance records. These physical controls reinforce both the administrative and technical policies and procedures on information access management required elsewhere in the rule. The administrative, physical, and technical controls collectively protect the confidentiality, integrity and availability of protected health information by permitting only authorized individuals to create, review or modify only information for which they have a "need-to-know"."

Technology

Commonly employed technical measures include: unique user identification, strong passwords, time-based forced time-outs or logoffs, virus protection, firewalls and encryption of data on removable media and laptop computers, wireless transmission, and remote access. However, technology must work with the HCO's culture, people, processes, and systems. Security depends on a multi-level strategy to deter security breaches. Technology should not drive security but support security efforts. Because security affects all areas and processes of the organization, it has become an organizational function rather than the exclusive domain of IT. No department is spared the impact of any technological change. Technology, therefore, should be installed with input from those that will be affected by the installation or modification. At the same time, staff must realize that unauthorized installation of software such as instant messaging (IM) or use of removable media can leave the organization open to malware, hackers, and thus breaches. Security must be monitored via audit logs, network software, and intrusion detection systems (IDS). None of these items can perform the job without people to verify they are working as designed and the necessary profiles are up-to-date. Technology should be able to enhance the overall integrity of the data while it is in transit or sitting on a laptop at a hotel through encryption. Wireless network should be encrypted at all times to prevent loss of confidentiality if data are intercepted. Backing up data and plans to permit its recovery and continue business operations in the advent of a disaster are also part of a security program.

CONCLUSION

Good security requires constant vigilance. Because effective use of deployed technology increases security, an HCO's business processes and culture should drive choices of technology not the reverse. Security reflects an HCO's state of awareness and, thus, changes every day with the behavior and attitude of the people who interact with the systems, processes, and infrastructure that support the personal health information and the organization.

Greene, S.S., 2006. *Security Policies and Procedures: Principles and Practices*. Prentice Hall.
Merkow, M. and Breithaupt, J., 2006.
Information Security: Principles and Practices. Prentice Hall.
Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191, 1996