HIPAA Security Redux: A Re-evaluation Process and Recommended Areas to Review

Save to myBoK

by M. Peter Adler, JD, LLM, CISSP, CIPP

Remember the mad scramble to create a compliance plan before the HIPAA security rule deadline? It's time to revisit that plan.

Publication of the HIPAA security rule created a flurry of discussions, debate, and activity as healthcare professionals grappled with how to comply before the regulatory deadlines arrived. Covered entities—those organizations affected by the rule—conducted risk assessments, selected safeguards, drafted policies and procedures, and provided staff training.

The resulting programs have been in place for a year or two now, and covered entities should begin to re-evaluate select components of their HIPAA security compliance program. This article provides a framework for conducting compliance re-evaluation and suggests three areas of focus to ensure that ongoing compliance is demonstrable and effective.

Why Re-evaluate?

The security rule includes methods for implementing an organization-wide program for securing electronic protected health information (PHI) as it is collected, stored, processed, and transmitted.[1,2] The deadline for compliance was April 20, 2005, for most covered entities.[3]

The security rule requires a covered entity to perform periodic technical and nontechnical compliance evaluations based initially upon the administrative, physical, and technical standards implemented under the rule. Subsequent evaluations are made in response to environmental or operational changes affecting the security of electronic PHI and whether policies and procedures continue to meet the requirements of the security rule.[4] The rule further requires review (and modification, as needed) of security measures to provide continuing reasonable and appropriate protection of electronic PHI.[5]

Examples of environmental or operational changes that affect PHI security include:

- **Changes in ownership or organizational structure.** People switch jobs, departments are reorganized, and entities change ownership. Programs should be assessed whenever important organizational changes occur to confirm that the security infrastructure continues to operate appropriately.
- **Modification or replacement of health information systems,** including the networks and applications that run them. Since HIPAA became law, there have been numerous advancements in how electronic PHI is received, stored, processed, and transmitted. This includes an explosion of activities involving electronic health records and the planning of shared networks that will use them. As progress in health information management continues, covered entities must be certain that information security considerations are reviewed whenever a system or application is modified or replaced.
- **Increased internal and external threats.** Security breaches of healthcare organizations have increased from 10 percent of all breaches in 2005 to 16 percent in 2006.[6] The safeguard selected in a HIPAA security compliance program may have to be updated or modified to counter increases in security threats.
- **Legislative changes.** Thirty-nine states have passed notice of breach laws.[7] These laws require organizations to provide notice to potentially affected customers, and in some cases, law enforcement, when certain notice-triggering information is compromised by a security breach. The state laws apply to covered entities in varying degrees. An organization's HIPAA security program may require modifications to comply with the notice of breach laws and other legislative changes.

Organizational Complacency

Another form of change that may necessitate a program assessment is a lack of change. A compliance re-evaluation is an antidote for organizational complacency.

After the privacy, security, and HIPAA administrative simplification provision deadlines passed, many covered entities operated as though no further actions were necessary. As a result, many robust security compliance programs atrophied and are no longer in compliance. Other programs that were not quite complete at the deadline lost momentum and have never reached their goals.

A 2006 report on IT compliance found that only 40 percent of covered entities comply with the security rule, up two points from the previous year.[8] In a survey on HIPAA compliance conducted by AHIMA, approximately one-quarter of respondents reported that their organizations were 95 to 100 percent compliant with the security rule in 2006, and approximately half rated their organizations at 85 to 95 percent compliant.[9] This reflected only modest gains over the previous year.

Top Picks for Re-evaluation

The security rule does not specify the areas that must be reviewed, so covered entities are free to select the components of their plans they will evaluate. These may depend on changes in legislation, available resources, and identification of areas that are incomplete or functioning imperfectly.

Three items commonly meet these descriptions and thus make good candidates for review. Typically they are components of the plan that were not implemented well initially or now require a review due to legislative, environmental, or operational changes. These areas are risk analysis and management; assigned security responsibility; and response and reporting.

Risk Analysis and Management

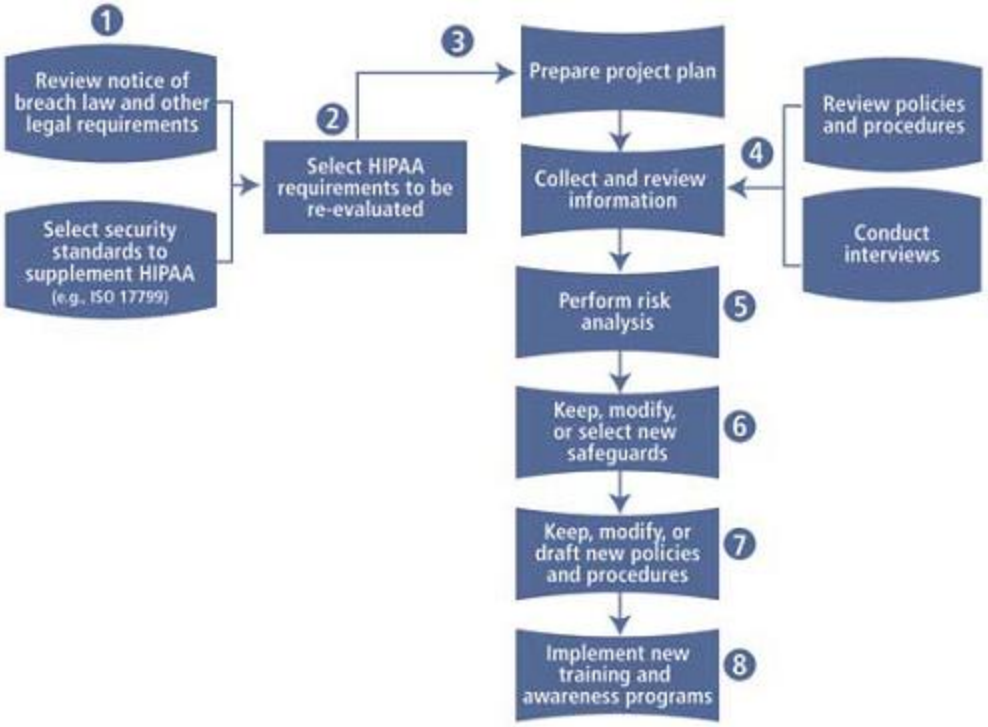
Risk analysis and risk management are two required implementation specifications found under the security management process standard.[10] Together they form the process for identifying threats, vulnerabilities, and risks and selecting safeguards to minimize the risk to electronic PHI.

The risk analysis implementation specification calls for covered entities to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by a covered entity.[11]

The risk management implementation specification requires covered entities to employ security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level in order to comply with the general requirements of HIPAA security regulations.[12]

The Re-evaluation Process

While a re-evaluation can involve an organization's entire HIPAA security program, it is typically a mini-assessment of the covered entity's compliance with specific aspects of the rule. A re-evalutation process is represented in the flow chart shown at right, with a description of each step below.



1. Review Legislative and Legal Developments

In this first step, the covered entity reviews legislative changes that may affect its HIPAA security compliance program. Legislative changes include notice of breach laws. They also include legal requirements such as contractually based compliance standards under the payment card industry data security standard, PCI DSS. Identification of new or pending legislation will help the covered entity select areas to be re-evaluated. It is also helpful to select industry standards and other best practices to supplement those provided by the security rule. Popular standards include ISO 17799:2005 and the National Institute of Standards and Technology (NIST) SP 800 Series.

2. Select HIPAA Requirements to Re-evaluate

The security rule does not specify areas that must be reviewed, so the covered entity is free to define the scope of its re-evaluation. Selection of areas to be re-evaluated may depend on changes in legislation, the resources available for the re-evaluation, and identification of areas that are incomplete or not functioning well. Some organizations may simply choose to start at the top of the list of HIPAA standards and implementation specifications and work their way down over time.

3. Prepare Project Plan

The project plan is used both to organize the re-evaluation and measure its progress and success. It details the areas to be re-evaluated, from whom information will be collected, key areas of inquiry, and the processes used to analyze risk and select safeguards.

4. Collect Preliminary Information

In this step, the organization collects policies and procedures, contracts, training materials, and related documents for review. Interviews are conducted with individuals responsible for the areas being re-evaluated. Documents are reviewed for compliance with the security rule. The analysis may include whether the policies

and procedures adequately cover the HIPAA requirements being reevaluated and whether contracts with business associates are current and complete.

The interviews help determine if key employees appropriately understand the requirements under evaluation and if written policies and procedures continue to accurately reflect current operations.

5. Perform Risk Analysis

A qualitative or quantitative risk analysis is performed on the areas under re-evaluation. The risk analysis is similar to that done for the original HIPAA risk assessment. It can be as simple or as complex as resources permit.

The key question is whether the required standards and implementation specifications are being met with safeguards that are reasonable and appropriate for identified risks; that is, whether the selected safeguard lowers to an acceptable level the probability of a threat exploiting a vulnerability.

The risk analysis also measures whether addressable implementation specifications are reasonable and appropriate for the covered entity and, if not, whether reasonable and appropriate alternative safeguards have been implemented. If no safeguard is implemented for addressable implementation specification, the risk analysis will review whether documentation has been prepared explaining why no measures were put in place.

Environmental and technology changes occurring since the initial assessment may directly affect the measurement of risk and selection of safeguards to counter risk. For instance, encryption of data at rest or during transmission may be more reasonable now than it was two years ago, because encryption technology has become easier to use and less expensive to implement

6. Keep, Modify, or Select New Safeguards

Based on the results of the risk analysis, the covered entity determines reasonable and appropriate safeguards for each area under re-evaluation. Existing safeguards may be kept, modified, or completely replaced. For example, the organization may upgrade software to an existing intrusion detection system, or it may install a new key-card system.

7. Keep, Modify, or Draft New Policies and Procedures

The covered entity reviews existing policies and procedures to determine how well they meet the requirements of the security rule. Existing policies and procedures are left unchanged if found to be adequate; they are modified if changes are required. New policies and procedures are drafted if they are lacking as required by the security rule.

8. Security Awareness and Training

The final step in the re-evaluation process is training staff about any changes made to the program as a result of the re-evaluation process. Training and awareness programs are an important element in demonstrating compliance with the security rule.

Risk analysis and risk management are top picks because they are fundamental processes for evaluating all safeguards selected and managed by the organization. Some questions to consider during the re-evaluation include:

- Does the covered entity have documented policies and procedures on how and when risk analyses are to be conducted?
- Do the policies and procedures specify the roles and responsibilities within the covered entity for ensuring that periodic risk analyses occur?
- Do policies and procedures include schedules for reviewing the effectiveness of selected safeguards?
- Do policies and procedures specify the process for selecting and implementing safeguards following a risk analysis?
- Have periodic risk assessments been conducted since the original HIPAA security compliance program was implemented?

Assigned Security Responsibility

According to the security rule, covered entities must identify a security official responsible for the development and implementation of HIPAA security policies and procedures.[13] The rule does not provide further guidance. Many covered entities appointed an information security officer to prepare and approve information security policies and procedures, assign security roles, and coordinate and review the implementation of security across the organization.

Reviewing this area during a re-evaluation is beneficial because roles and responsibilities are often not adequately established or have changed since the original implementation. Often policies and procedures are not updated to reflect current practices.

When re-evaluating security responsibilities, a covered entity should review how well security management processes function. Questions include:

- Did the covered entity simply name a responsible person as required by the security rule, or did management provide clear direction, support, and resources for the security compliance program?
- Are specific roles and responsibilities for information security clearly assigned across the organization?
- Are the covered entity's information security goals identified, do they meet the organizational requirements, and are they integrated into the organization's operations?
- Do the policies and procedures reflect actual practices?

Response and Reporting

HIPAA requires covered entities to create security incident procedures.[14] The implementation specification also requires covered entities to document "security incidents" and their outcomes. This requirement is broad, because "security incident" is defined to include both attempted and successful unauthorized access, use, disclosure, interference, and similar activities.[15]

The security rule does not require a covered entity to notify persons who may be affected by the breach. However, guidance published by the Centers for Medicare and Medicaid Services suggests that a security response may include reporting to affected individuals as part of the duty to mitigate found in the privacy rule.[16]

Since the California notice of breach legislation became effective in 2003, 39 states have passed similar laws. Four of the state laws provide that compliance with HIPAA will automatically comply with the state law. Nineteen states provide that an entity will be deemed to be in compliance with the state law only if it has an information security program that includes notification procedures consistent with the timing requirements of the state law.

For all 39 states, modifying the HIPAA security response and reporting policies and procedures can result in compliance with notice of breach law.

To re-evaluate compliance with HIPAA response and reporting requirements, a covered entity must confirm that it has developed and implemented appropriate security incident policies and procedures. If it has, it should next confirm that the policies and procedures:

- List possible types of security incidents and the response procedures for each
- Clearly list roles and responsibilities for responding to security incidents

- Include current contact information for persons responsible for reporting and responding to security incidents
- Identify to whom and when security incidents must be reported
- Address changes required by state notice of breach laws that affect the covered entity's incident response policies and procedures
- Include contact information of law enforcement and payment card industry personnel (if credit card information is involved)

The re-evaluation could also test the effectiveness of the security incident policies and procedures by conducting a mock security incident.

Re-evaluation does not have to be cumbersome or complex, but it must provide a systematic method to measure and promote ongoing compliance even after environmental and operational changes. Depending on the organization and its needs, the process can begin with the three areas listed here or other areas selected by the covered entity and proceed periodically with additional areas selected for review.

Notes

1. Electronic protected health information is individually identifiable health information transmitted by electronic media and maintained in electronic media, subject to certain exceptions such as employment records held by a covered entity in its role as employer information covered by Federal Education Records Protection Act. *See* HIPAA, Public Law 104-191, 45 CFR §160.103.
2. HIPAA 45 CFR §§164.302–318.
3. Covered entities are healthcare providers that conduct certain electronic transactions, including health plans and healthcare clearinghouses. 45 CFR §160.103. Small health plans were given until April 2006 to comply with the security rule. 45 CFR §164.318(a)(2).
4. HIPAA 45 CFR §164.308 (a)(8).
5. HIPAA 45 CFR §164.306 (e).
6. Privacy Rights Clearinghouse. "A Chronology of Data Breaches." Available online at www.privacyrights.org/ar/ChronDataBreaches.htm.
7. As of fall 2007, the states with notice of security breach laws are: Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Vermont, Washington, Wisconsin, and Wyoming.
8. Holmes, Allan. "The Global State of Information Security 2006." September 15, 2006. Available online at www.cio.com/article/print/24979.
9. AHIMA. "The State of HIPAA Privacy and Security Compliance 2006." April 2006.
10. HIPAA 45 CFR 308(a)(1)(i).
11. HIPAA 45 CFR §164.308(a)(1)(ii)(A).
12. HIPAA 45 CFR §164.308(a)(1)(ii)(B).
13. HIPAA 45 CFR §164.308(a)(2).
14. HIPAA 45 CFR §164.308(a)(6)(ii).
15. HIPAA 45 CFR §164.304.
16. Centers for Medicare and Medicaid Services. "Security Standards: Administrative Safeguards." HIPAA Security Series, vol. 2, paper 2. Available online at www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsAdministrativeSafeguards.pdf.

M. Peter Adler *(adler@adleripg.com) is president of InfoCounsel, LLC, in Alexandria, VA*

Article citation:
Adler, M. Peter. "HIPAA Security Redux: A Re-evaluation Process and Recommended Areas to Review" *Journal of AHIMA* 78, no.10 (November 2007): 38-42.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.