Global Information Assurance Certification Paper

Online Group: GSEC, LevelOne Security Essentials
User ID: msato001
Practical Version: 1.2b

HIPAA Security Policy Development: A Collaborative Approach

Miles M. Sato
April 30, 2001

Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), enacted on August 21, 1996 as Public Law 104-191, authorized the Secretary of Health and Human Services (HHS) to develop security standards to prevent inadvertent or intentional unauthorized use or disclosure of any health information that is electronically maintained or used in an electronic transmission. This law affects several titles in the United States Code.

On August 12, 1998, HHS released 45 CFR Part 142, the Notice of Proposed Rule Making (NPRM) for the HIPAA security rule [1]. At this time, the final HIPAA security rule has not yet been issued. Requirements presented in this NPRM are not clearly written, and are open to a wide range of interpretation. However, at Title 42 of the United States Code, civil and criminal penalties already exist under HIPAA for unauthorized use or disclosure of individually identifiable health information (42 USC 1320d-5 and 42 USC 1320d-6).

On April 14, 2001, the final HIPAA privacy rule, 45 CFR Parts 160 and 164, became effective [2]. In §164.530(c)(1) a mini HIPAA security is created within the privacy rule:

> "A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."

This language is similar to that of §1320d-2 (d)(2) from Title 42 of the United States Code:

> "Each person described in section 1320d-1(a) of this title who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards…"

The point is that although the final HIPAA security rule has not yet been released by HHS, there are ample regulatory reasons for healthcare organizations to begin the process of developing HIPAA specific security policies.

Proposed HIPAA Security Rule

The proposed HIPAA security rule is divided into four broad categories:

1. Administrative procedures to guard data integrity, confidentiality, and availability: intends to ensure that organizations provide for a structure in which an information security program can be developed and implemented – §142.308(a).

2. Physical safeguards to guard data integrity, confidentiality, and availability: intends to ensure the protection of computer systems and related physical structures in which these systems are housed from fire, other natural and environmental hazards, and intrusion. These safeguards also include the use of locks, keys, and administrative measures used to control access to computer systems and facilities – §142.308(b).

3. Technical security services to guard data integrity, confidentiality, and availability: intends to protect, control, and monitor information access – §142.308(c).

4. Technical security mechanisms to guard against unauthorized access to data that is transmitted over a communications network: intends to protect health information that are electronically transmitted over open networks against interception or interpretation by parties other than the intended recipient. These mechanisms are also intended to protect information systems from intruders who attempt to gain access through external communication points – §142.308(d).

Sandra Fuller, VP of practice leadership for the American Health Information Management Association (AHIMA), in 1999, stated that at least 19 separate health information security policies are required to comply with the requirements of the proposed security rule [3]. Since development of new policies or modification of existing policies to address the proposed HIPAA security requirements would be a formidable and expensive task for many healthcare organizations, a collaborative approach to developing these required policies for HIPAA security rule compliance would provide substantial economic benefit, as well as a baseline community standard for the participants of such a collaborative effort.

Hawaii HIPAA Readiness Collaborative

This paper outlines the methodology and initial products of the collaborative policy development effort currently in progress in the State of Hawaii. In 2000, the HIPAA Readiness Collaborative (HRC) was formed under the leadership of the Hawaii Health Information Corporation (HHIC) [4]. The HRC is composed of major private sector hospitals, major health insurers, and the State hospital system. It receives its direction from key CIOs and CFOs. The HRC's stated goal is to reduce the administrative costs of HIPAA implementation for participating organizations, and to improve interoperability between facilities in the community through the use of standard technologies.

Other statewide HIPAA collaborative efforts include those sponsored by the Idaho Department of Health & Welfare [5], the Minnesota Center for Healthcare Electronic Commerce (MCHEC) [6], the Nebraska Association of Hospitals and Health Systems (NAHHS) [7], and the North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA) [8].

The Hawaii HIPAA collaborative is unique due to its ongoing effort to collaboratively develop security policies and guidelines to meet HIPAA standards based on a statewide understanding of the HIPAA security rule, which will be shared among its participating members. Each of the

participating members of the collaborative can then customize these policies to fit their individual organizational needs.

Hawaii HIPAA Readiness Collaborative Policy Development Methodology

HIPAA security policies are being developed by the HRC's Security Policy Subcommittee. This subcommittee is one of several working groups, which includes the EDI/Administrative Simplification, the Privacy, the Security Awareness Training, the Technical Security, and the Transactions & Code Set Subcommittees.

The Security Policy Subcommittee is composed of ten individuals who represent seven different healthcare organizations (three major private sector general service hospitals, a private sector psychiatric hospital, the Hawaii State hospital system, a major health insurer, and HHIC). Committee members each take on the responsibility for the developing specific HIPAA required security policies. Currently, HRC has released five pilot policies to the general public [9]:

- Confidentiality and Non-disclosure
- Data Classification
- E-mail
- Information Stewardship
- Information Systems Access

Based on experience gained during the development of these pilot policies, it is estimated that each subsequent policy being developed by the HRC will require an average of 45 hours to complete. If one person were tasked to develop the minimum 19 policies required to fulfill the proposed HIPAA security requirements, it would take that person approximately 855 hours to complete. Development of this same set of 19 policies would be completed in approximately 85.5 hours by the HRC Security Policy Subcommittee, since the workload would be distributed among its 10 committee members.

Policy development is a time consuming process. Each policy developed by the HRC Security Policy Subcommittee passes through the following steps:

1. The relevant proposed HIPAA security standard is assessed. In many cases, the actual industry standards that HHS used in creating proposed HIPAA security requirements are consulted for clarification.

2. Key references relevant to a particular policy topic are reviewed, and relevant policies and procedures from committee member organizations are assessed. Additional industry best practices are then studied. Best practice references include the HIPAA Security Summit Guidelines [10], the CPRI Toolkit [11], and the British Standards [12,13]. Policies developed by the HRC are intended to reflect industry best standards. They are also intended to reflect a "community norm."

3. An outline of the proposed security policy is then created and submitted for committee review.

4. Based on committee feedback, the policy outline is revised and a first draft of the policy is written. Sometimes policy templates from sources such as Baseline Software [14] and the SANS.org [15] are used.

5. The draft policy is then reviewed by the committee to ensure that it conforms to accepted policy creation standards. It is checked to ensure that it contains most of the common elements of good policies such as:

    - Purpose
    - Scope
    - Policy statement
    - Responsibility
    - Action
    - References

    The committee understands that good policies generally establish only what must be done and why it must be done, but not how to do it. However, it was decided that HRC developed policies would also include procedural guidelines. The committee felt that the HRC policies should be developed with the intent of providing for scalability, such that its policies can be used not only by large healthcare organizations, but also by single physician offices. The committee understands that scalability is an inherent tenet of the proposed HIPAA security rule.

6. The draft policy then goes through an iterative process of internal validation checks with the proposed HIPAA security rule requirements, and consistency checks against all other policies that are being developed.

7. After internal committee reviews, the draft policy is then released for stakeholder review by executive management and legal representatives within the committee members' respective organizations.

8. Modifications are then made based upon stakeholder feedback.

9. The draft policy then goes through another iteration of internal committee reviews.

10. Finally, after these reviews have been completed, the policy is then released to the general Collaborative membership.

Multiple security policies are now being concurrently developed through this HRC security policy development process. The next set of HRC policies that are expected to be released include:

- Security Incident
- Contingency Planning
- Risk Management

- Risk Analysis
- Configuration Management
- Personnel Security
- Termination

All of the policies being developed by the HRC are understood to be living documents. When the final HIPAA security rule is released, necessary changes will then be made to align them with whatever changes are contained in the final rule. Also, these policies are meant to be used by the Collaborative members as industry best practices template policies to be customized for use within their respective organizations. The HRC policies are designed to be scalable, and to reflect a community normative standard that each member organization can ascribe to, so as to benefit from the concept of safety in numbers.

Sources

[1] Federal Register, 45 CFR Part 142, Security and Electronic Signature Standards; Proposed Rule, 08/12/1998. URL: http://aspe.os.dhhs.gov/admnsimp/nprm/seclist.htm

[2] Federal Register, 45 CFR Parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information; Final Rule, 12/28/2000.
URL: http://aspe.os.dhhs.gov/admnsimp/nprm/pvclist.htm

[3] Fuller, Sandra. Journal of AHIMA, "Implementing HIPAA Security Standards," October 1999. URL: http://www.ahima.org/journal/features/feature.9910.1.html

[4] Hawaii Health Information Corporation. URL: http://www.hhic.org

[5] Idaho Department of Health & Welfare.
URL: http://www2.state.id.us/dhw/hipaa/home.htm

[6] Minnesota Center for Healthcare Electronic Commerce.
URL: http://www.mhdi.org/mchec/hipaa/index.html

[7] Nebraska Association of Hospitals and Health Systems.
URL: http://nahhsnet.org/html/HIPAA.htm

[8] North Carolina Healthcare Information and Communications Alliance, Inc.
URL: http://www.nchica.org/HIPAA/HIPAA_intro.html

[9] Pilot policies released to the general public by the Hawaii HIPAA Readiness Collaborative.
URL: http://www.hhic.org/hipaa/pilots.html

[10] HIPAA Security Summit. URL: http://www.wedi.org/public/articles/HSSGuidelines.doc

[11] CPRI Toolkit. URL: http://www.cpri.org/resource/toolkit/toolkit.html

[12] British Standard, Information security management – Part 1: Code of practice for information security management, BS 7799-1:1999, published by BSI, 1999.

[13] British Standard, Information security management – Part 2: Specification for information security management systems, BS 7799-2:1999, published by BSI, 1999.

[14] Charles Cresson Wood. Information Security Policies Made Easy, Version 7. Baseline Software, Inc., 1999.

[15] SANS.org policy templates.
URL: http://www.sans.org/newlook/resources/policies/policies.htm