Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

HIPAA Security Compliance Project - Identification of Logging and Auditing Requirements

The purpose of the Final Health Insurance Portability and Accountability Act (HIPAA) Security Rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. This discussion will outline a project "plan of attack" for a covered entity to identify and address the electronic logging and auditing requirements within the Final HIPAA Security Rule. Compliance projects can be frustrating, particularly in large, diverse organizations. B...

Copyright SANS Institute
Author Retains Full Rights

AD

HIPAA Security Compliance Project – Identification of Logging and Auditing Requirements

Kurt Patti, CPCU, CLU
August 27, 2003
GSEC Practical Assignment
Version 1.4b Option 1

Abstract

The Final Health Insurance Portability and Accountability Act (HIPAA) Security Rule became effective on April 21, 2003. Covered entities must comply with the requirements by April 21, 2005. Small health plans have until April 21, 2006. The purpose of this final rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. [2]

This discussion will outline a project "plan of attack" for a covered entity to identify and address the electronic logging and auditing requirements within the Final HIPAA Security Rule. Compliance projects can be frustrating, particularly in large, diverse organizations. By identifying and utilizing the proper resources, planning carefully, and staying organized, a project team can meet the challenges successfully. A project team for a fictitious covered entity has been charged with identifying and making recommendations for reconciling the gaps between the company's logging and auditing policies and practices, and the requirements of the Final HIPAA Security Rule. The study will follow the steps taken by the project team and will examine some of the challenges in organizing and carrying out such a project in a large financial services organization. It will suggest potential solutions and some alternative approaches. In the final analysis, it should be a useful reference document for any covered entity faced with the task of evaluating and ensuring compliance with the administrative and technical logging and auditing standards set forth in the Final Security Rule.

Background

The Final HIPAA Security Rule contains the following broad requirement areas that must be addressed by covered entities:

- Administrative Safeguards to protect data integrity, confidentiality and availability of electronic protected health information (PHI).

- Physical Safeguards to protect data integrity, confidentiality and availability of electronic protected health information.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Technical Safeguards to protect data integrity, confidentiality and availability of electronic protected health information. [2]

The regulation is written at a relatively high level. It is neutral with regard to the technology to be used, and leaves a good deal of room for interpretation. This approach makes sense due to the rapidly changing world of technology, and to the diversity in covered entity organizational size, types of operations, levels of risk, and available resources. The Final Rule covers more of the “what to do” in terms of items to be addressed and implemented, and not so much the “how to do it”.

• HIPAA Security - Administrative Safeguards Related to Logging and Auditing

Included among the Administrative Safeguards section of the rule, is a requirement to conduct an "Information system activity review”. This is the terminology selected to replace the terms "internal audit" as required in the proposed regulations. The "information system activity review’’ is a required implementation specification under the Security Management Process Standard in the final ruling. The “intent for this requirement was to promote the periodic review of an entity's internal security controls, for example, logs, access reports, and incident tracking. The extent, frequency, and nature of the reviews would be determined by the covered entity's security environment.” [2]

The Administrative Safeguards section also contains a Security Awareness and Training Standard that includes an addressable implementation specification termed “log-in monitoring.” “Log-in monitoring,” points to creating procedures for monitoring log-in attempts to applications and systems containing PHI, and for reporting discrepancies. [2]

> Although covered entities must implement all 18 of the Standards and the Required Implementation Specifications, they must only assess the Addressable Implementation Specifications to see if they are reasonable and appropriate in their environment. When analyzed as to their contribution to protecting electronic PHI, covered entities must implement them if reasonable and appropriate. If implementing an Addressable Implementation Specification is not reasonable and appropriate, the covered entity must document why it would not be reasonable and appropriate to implement, and implement an equivalent alternative measure if that is reasonable and appropriate. [7, p.2]

A third standard within the Administrative Safeguards section of The Final Rule, related to logging and auditing of electronic PHI is the Evaluation Standard. This is a required standard that stands on its own, with no associated lower-level implementation specifications. This standard requires a covered entity to periodically evaluate itself both technically and non-technically, with regard to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

how it measures up to the standards implemented under the Final HIPAA Security Rule. [2]

• HIPAA Security - Technical Safeguards Related to Logging and Auditing

The Technical Safeguards section calls out an "Audit Controls" standard. The Audit Controls standard requires the capability to record and examine system activity in information systems containing, or using electronic protected health information. “Entities have flexibility to implement the standard in a manner appropriate to their needs as deemed necessary by their own risk analyses.” [2]

HIPAA Compliance Project – Identify Logging and Auditing Requirements

Hippo Incorporated is a large financial services organization, and a “covered entity” as defined by the HIPAA regulations. It runs a bank and also sells many lines of insurance, including health insurance. In addition, Hippo offers employee group health coverage, and medical expense flexible spending accounts to its employees. Hippo has a very large and very specialized Information Technology (IT) department, broken down into many separate functions and units. Therefore, the knowledge and understanding of systems requirements and their interrelationships is widely dispersed throughout the organization. Like most large companies, Hippo also struggles with the effective communication and understanding required between business area subject matter experts, and the IT professionals designated to work on projects. This is primarily due to the business partners’ lack of technical savvy, and the IT professionals’ lack of day-to-day business operations knowledge.

Hippo’s Information Security Officer formed a HIPAA compliance group to examine and address HIPAA Privacy and Security from a broad, enterprise-wide perspective. The compliance group elected to approach Hippo’s HIPAA compliance efforts by grouping the work into smaller, more manageable pieces. Each of these pieces was to become a project. This compliance group was responsible for analyzing the HIPAA Privacy Rule, and the Proposed (at the time) Security Rule, to determine what the company’s “HIPAA projects” would encompass, and how the work would be segregated.

The compliance group determined that one of the HIPAA projects would be responsible for identifying and analyzing the logging and auditing requirements called out in the Final Security Rule under the Administrative and Technical Safeguards sections. Any logging or auditing requirements called for in the Physical Safeguards section would be analyzed and addressed by a separate project. The project team was expected to analyze the current state of the enterprise with regard to logging and auditing, compare it to the legislative requirements, and make recommendations for situations the project team identified as non-compliant with the regulations.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Unlike the HIPAA Privacy Rule, which applies to PHI in all forms, The Security Rule applies only to PHI in electronic form. Therefore, the project team was to focus on those systems, applications, and databases that were identified as containing PHI.

Like many covered entities, Hippo had been preparing for the Final HIPAA Security Rule prior to its release, by planning and positioning the organization for compliance based on the proposed legislation. Once The Security Rule was finalized, a review of how The Final Rule differed from the proposed legislation was required.

Hippo Incorporated's Information Technology projects are initiated only after detailed cost/benefit analyses and justification. Upper management must review and bless all initiatives prior to kickoff. Projects designed to address legislative requirements such as HIPAA, always sit at the very top of the priority list, and there was no trouble obtaining approval and funding for the HIPAA logging and auditing project. Several of the earlier identified "HIPAA projects" had already been completed, and the HIPAA logging and auditing project team knew it would have access to the documentation gathered and created by those other efforts. Among those items coming out of the other projects, was a listing of all the applications determined to contain protected health information. There were 17 separate applications, some used by many different units within the company.

Challenge: Determining what resources should be assigned to the project team.

Approach: Hippo assigned a project sponsor from its Compliance area, and a project manager with experience implementing legislative compliance projects. Two business analysts were selected from the IT Support area of the Health Insurance applications, along with two data security project analysts and a data security support analyst familiar with the HIPAA legislation due to their participation in some of the earlier HIPAA projects. In addition to these core team members, a health insurance systems analyst, and a mainframe database analyst were assigned responsibility to monitor the progress in case their services were needed. Hippo also had the support of a representative from the corporate legal department in case legal questions, concerns, and interpretation needs arose.

Alternatives: Many organizations faced with HIPAA Security compliance are smaller than Hippo and will not have these types and numbers of resources available to them for a similar project. No matter the situation, or the size of the covered entity involved, it is important to have the business operations knowledge and the IT/Security expertise represented on the project, as well as the knowledge and understanding of the legislation. In many cases, smaller organizations may have to rely on one or two individuals to drive their compliance efforts. Outside resources, including consulting firms and compliance products

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

are available to aid in understanding and meeting the federal standards if the resources are not available in house. Some of the best places to start for information, help, compliance tools, and support on the road to HIPAA Security compliance, are the Centers for Medicare and Medicaid Services (CMI), SANS, Department of Health and Human Services (DHHS), and the Workgroup for Electronic Data Interchange (WEDI) web-sites.

Challenge: Determining the scope of the project and avoiding "scope creep".

Approach: The team drew up a project charter document, which included the scope of work from a broad perspective, outlining what they were planning to accomplish. The charter and scope were based on the Proposed HIPAA Security Rule, as The Final Rule had not yet been published. By staying abreast of the latest developments, watching and reading industry publications, and the web sites mentioned above, among others, the team knew that The Final Rule was not expected to be substantially different than The Proposed Rule. The charter was reviewed and approved by the project manager and the project sponsor, whom also represented Hippo's HIPAA compliance group. The scope of work was broken down into several milestone objectives to cover the expected logging and auditing requirements identified by the compliance group to be addressed by this project. Staying within the defined scope of a project can be difficult. Some of the other HIPAA projects had already been completed and there was a constant need to ensure no duplication of effort, so as not to waste resources and cycles. Leveraging existing research documentation and findings can save a great deal of time and effort. Frequent checks throughout the life of the project helped to ensure the project team stayed within the project scope limits, and utilized existing research documentation when available. Avoiding "scope creep" was accomplished by verifying that all proposed work could be mapped directly back to at least one of the overall objectives outlined in the charter.

The broad, approved scope objectives based on The Proposed Rule, developed by the project team, were as follows:

- Determine how the expectations of the legislation would apply to Hippo Inc. based on its size, types of operations, and resources.
- Gather and document existing logging and auditing practices and procedures within the organization.
- Identify any gaps between existing practices and procedures and those deemed necessary by the project team, in order to address the legislation.
- Develop and present recommendations to identified responsible areas within the organization.

Alternatives: In large companies, with budgeted, funded projects, any work done outside of scope increases the risk that the project will come in over budget, or

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

not get completed successfully. One of the most important ideals in identifying a project's scope is sticking to it, once it is approved. There are many ways to determine what should and should not be included in the scope of a project. With legislative projects, legal counsel and interpretation are strongly recommended. This will enable the project team to feel relatively comfortable they have addressed at minimum, those items legally required. Smaller entities with more limited resources would still benefit from breaking the work down into smaller chunks, even if their HIPAA compliance efforts all fall under one project umbrella. There should always be an open channel of communication between the compliance project team and the company's Information Security Officer.

Challenge: Project Planning

Approach: During the project kickoff meeting, when all team members were introduced and had the opportunity to hear from the Project Sponsor and Project Manager, a series of planning sessions were scheduled. Over the course of a week, during three planning sessions, lasting two hours each, the project team hammered out a project schedule using the scope objectives as guides. Each objective was broken down into tasks that were sequenced to allow for tracking in a project-scheduling tool. The project plan was presented to the project sponsor and the project manager for comment and eventual approval.

Alternatives: Although a smaller firm may have a "team" of only one or two individuals to address all HIPAA legislation, organized planning is essential to reaching goals and meeting deadlines. Without a detailed task list pointing to specific milestones to meet identified objectives, it is difficult to track progress and identify next steps. Planning is always an iterative process, and there should also be a means of making documented, approved changes if necessary.

Challenge: The Final Rule was just released, now where to start?

Approach: Shortly after the sponsor and manager approved the project plan, the Final HIPAA Security Rule was released. The team came up with the following approach to carry out the project plan:

1. Compare The Final Rule to The Proposed Rule. This comparison would allow the team to identify the differences between anticipated requirements and actual requirements. It also provided an opportunity to make any necessary adjustments to the plan as a result of changes between The Proposed Rule and The Final Rule.

2. Analyze the Final HIPAA Security Regulations to identify and understand the references to logging and auditing standards and implementation specifications.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

3. Gather and understand the existing logging and auditing policies and practices throughout the organization. Special emphasis was to be placed on researching those areas already identified as utilizing systems and data containing PHI.

4. Compare the company's existing logging and auditing practices to those identified as required or addressable, in the analysis of The Final Rule.

5. Make recommendations to responsible areas to address findings that need to be addressed, in order to meet the standards and implementation specifications adopted in The Final Rule.

Alternatives: The current state of awareness and existing knowledge of the HIPAA legislation resident in an organization will determine the starting point of this type of project. Again, the size and available resources of the organization will also have a bearing on what needs to be done first. Assuming a similar level of understanding of the legislation, the objectives above should serve a company of any size well. If there is very little understanding of the law within an organization, HIPAA education and training should occur prior to project planning. The web sites already mentioned are a great place to start the process. Subscribing to the WEDI SNIP Security Workgroup Listserv, as well as the WEDI SNIP Privacy Workgroup Listserv, is a valuable way to ask questions, and share information with other covered entities facing the same challenges.

1. Compare the Final Security Rule to the Proposed Security Rule.

The team had a working knowledge of the proposed legislation and was happy to find that The Final Rule was simplified, more straightforward, and written to more closely mirror the style of the Final Privacy Rule. A particularly useful document found to aid in this comparison analysis was "PricewaterhouseCoopers Interpretation of the Final HIPAA Security Rule". [7]

The broad scope objectives documented in the charter did not require any changes as a result of The Final Rule. However, a few modifications were made to some of the tasks as a result of the team's interpretation of The Final Rule, and due to some legal interpretation following a review of The Rule by the corporate legal representative.

2. Analyze the Final HIPAA Security Regulations to identify and understand the references to logging and auditing standards and implementation specifications.

"PricewaterhouseCoopers Interpretation of the Final HIPAA Security Rule" gives the following well-stated synopsis of The Final Rule:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

> The rule is composed of 18 standards, each of which may have required and addressable implementation specifications. All covered entities must comply with all the standards with respect to electronic protected health information and they must review and modify their security measures as needed to continue reasonable and appropriate protection of electronic PHI. A covered entity must: ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI; protect against any reasonably anticipated uses or disclosures of PHI that are not permitted or required under the privacy rules; and ensure compliance by its workforce. [7 p.1, 2]

The project team's review and analysis identified the following Final HIPAA Security Rule standards and implementation specifications as those to be addressed by the HIPAA logging and auditing project:

A. Standard – Security Management Process – Section 164.308(a)(1)(ii)(D)
   Implementation Specification – Information System Activity Review (Required)
B. Standard – Security Awareness and Training – Section 164.308(a)(5)(ii(C)
   Implementation Specification – Log-in Monitoring (Addressable)
C. Standard – Evaluation (Required) – 164.308(a)(8)
D. Standard – Audit Controls (Required) – 164.312(b) [2]

These standards and implementation specifications are discussed in detail above, in the "Background" section of this document.

3. Gather and understand the existing logging and auditing policies and practices throughout the organization.

Due to Hippo's size, network complexity, system interdependencies, data interrelationships, and specialized IT environment, this was a monumental undertaking if it was to be done thoroughly.

Challenge: Identify and analyze existing company logging and auditing practices within the organization.

Approach: The first step in determining existing practices was to gather all company policies, standards and guidelines applicable to data security and privacy at an enterprise level. The team accomplished this by conducting a thorough search of Hippo's company intranet, and through phone calls, emails, and meetings with contacts in the Information Security Department and the Technical Architecture Department. Hippo Inc. already had a very solid information security awareness program implemented as a result of the Gramm-Leach-Bliley Act of 1999. In addition, an enterprise-wide information security

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

policy, with its associated standards and guidelines was already in place, including best practices logging and auditing standards. The Technical Architecture Unit also owned and published a set of system and network architecture standards and guidelines, which included logging and auditing specifications. The Information Security Department had annual vulnerability assessments conducted by bringing in external consultants to perform penetration testing. All enterprise-wide security, privacy, and information-handling policies, and references to logging and auditing standards uncovered during this step were compiled into a spreadsheet. This spreadsheet would later be utilized to match existing standards against HIPAA required standards for gap analysis.

The next step in this process was to gather departmental and application-specific policies, practices, and procedures from those areas utilizing the systems and applications identified as containing PHI.

The team analyzed all sources of enterprise security policy they had gathered to determine what was already in place with regard to company logging and auditing requirements. It would be more difficult to gain support for recommended changes from affected business areas if company policy did not support the recommendations, despite any interpretation of the federal legislation. From an intra-company political standpoint, full support could require changes to company policy in order to gain management approval for necessary changes called for in the legislation.

After gathering all existing logging and auditing documentation regarding what should be done, the team identified and interviewed representatives from each application support area to attempt to determine what type of logging and auditing practices were actually being carried out. As mentioned earlier, knowledge and understanding of Hippo's systems is very specialized, and widely dispersed. In some instances the initial contacts were able to provide the team with most of the information requested, but in most cases, additional expertise was required. According to a white paper entitled "Security and Privacy Auditing in Health Care Information Technology," developed by the Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC), "The overall goals when constructing an audit trail are to record who did what to which object, when and on which system." [9, p.2] With this in mind, the team developed the following questions, which were sent via electronic mail to additional selected subject matter experts, and system contacts identified during the interviews and beyond:

1. Is information captured showing who and when a user accesses the application?
2. Provide the name of the log or report that captures access information, and indicate where it is stored.
3. Who (Job Title) reviews the access log or report, and how often?

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4. Is information captured on additions, modifications and deletions to data within the application?
5. Provide the name of the log or report, and indicate where it is stored.
6. Who (Job Title) reviews the system activity log or report, and how often?

Responses to the questions often required follow-up, clarification, and additional research in order to gain understanding, and to ensure accurate documentation. After the team compiled the information received from all areas utilizing systems containing PHI, it became apparent that many of the older mainframe applications, particularly those that were homegrown, lacked sufficient transaction-level activity logging. Most of the newer vendor products had the capability built in, and in most of those cases the functionality was being utilized.

As a result of these findings, the team developed a second list of questions that focused on application access controls, for logging and auditing purposes. The rationale here was to confirm that applications containing PHI were restricted to only those employees requiring the access to accomplish their duties. If Hippo did not record all transaction-level activity within systems containing PHI, it was doubly important to ensure that the "minimum necessary" doctrine was in fact being followed, while proper logging and auditing practices could be put in place. The idea behind "minimum necessary," which actually came out in the HIPAA Privacy Rule, is to "limit the use or disclosure of, and requests for protected health information (PHI) to the minimum necessary to accomplish the intended purpose." [10] Again, these questions were sent via electronic mail to the application support area contacts and to the business areas to answer, or to enlist the help of those who could.

1. Who (areas, departments, individuals) has access to the application or associated data?
2. When a user successfully signs on to the application(s) is there a notice displaying the date/time of his/her last successful sign on to the application?
3. Are unsuccessful access attempts logged? Name of report: _____
4. Is the log or report reviewed? How often and by whom (Job Title)?
5. Outline the access controls in place for all users (e.g.):

- How does one go about getting access?
- Who makes sure they should have access?
- Is access limited based on job duties (role-based)?
- How are those who no longer need access "cleaned up"?
- How often are the access lists reviewed and cleaned up?
- If reports or listings of users are generated to review valid access -> name(s) of reports: _____
- How often are they reviewed and by whom (Job Title)?
- If there are no reports, or listings, how is the access review conducted - what tools - by whom?

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Are there documented processes and/or procedures in place to restrict access to only those with a business need?
- Are these areas audited for process/procedure compliance? By whom (Job Title), and how often?
- Are users required to go through Hippo's HIPAA/Privacy training?
- Are there documented operating procedures that outline access controls, and maintenance? Please provide a link _____.

The responses were again compiled through an iterative process, which involved follow-up meetings and additional correspondence. This information was also captured and stored in a spreadsheet for comparison to HIPAA standards during the upcoming gap analysis.

Alternatives: Gathering existing policies and procedures in a large organization can be a daunting task. Typically, silos exist in large organizations and some business units do a better job of documenting policies and procedures than others. Hippo's intranet made the search for enterprise policy somewhat less complicated, but the business and support operations' policies and procedures varied in form, function, and detail from one unit to the next. Smaller organizations may be more uniform in their approach to documented policy and procedure. No matter the size, or the type of organization, the key to finding the right information is diligence, and identifying the proper contacts. It is important to compile all information gathered in a format that is easily accessible, and readily understood.

4. Compare the company's existing logging and auditing practices to those identified as required or addressable, in the analysis of The Final Rule.

Challenge: Determining whether or not there are any gaps.

Approach: Once all the research had been done, and the information had been verified and captured in the spreadsheets, the team began its gap analysis. With the spreadsheets in hand, the team conducted several meetings to go over the relationships between the applicable Final Rule standards and implementation specifications compared to the related company standards and guidelines. The spreadsheets, which mapped each of the four HIPAA standards and implementation specifications to the related company policies and procedures, made the gap analysis much easier to accomplish.

Hippo's enterprise level information security policy, standards and guidelines supported all the applicable Final Rule standards with one exception. Hippo's standards did not include a reference to the addressable "log-in monitoring" implementation specification, under the Security Awareness and Training Standard – Section 164.308(a)(5)(ii(C) of the rule. The project team addressed the standards included in the scope of their project in the following manner.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A. Standard – Security Management Process – Section 164.308(a)(1)(ii)(D) Implementation Specification – Information System Activity Review (Required)

The ongoing third party annual vulnerability assessments along with regular internal audits conducted by the company's internal auditing department, helped to meet this standard. The team drafted a note to the management group in Internal Auditing, outlining recommendations for access control items to be monitored in future audits of PHI-handling departments. The team recommended that the Information Security Department develop a specific section devoted to HIPAA security, in all future vulnerability assessments.

B. Standard – Security Awareness and Training – Section 164.308(a)(5)(ii(C) Implementation Specification – Log-in Monitoring (Addressable)

This is the implementation specification Hippo's policy did not support. Unlike "required" implementation specifications, if an implementation specification is "'addressable,' a covered entity has options: implement it, implement an equivalent measure or do nothing (documenting why it would not be reasonable and appropriate)." [1, p.5] The team's decision was to draft a proposal to the information security unit responsible for maintaining the enterprise information security policy, standards and guidelines, recommending inclusion of log-in monitoring standard at the next quarterly review/revision date. The team felt the specification was "reasonable and appropriate," and despite the fact that it was not covered in policy, log-in monitoring was actually in place for the vast majority of the PHI systems and applications.

C. Standard – Evaluation (Required) – 164.308(a)(8)

This standard was addressed in the same manner as the Information System Activity Review. Future internal audits and vulnerability assessments were to monitor ongoing compliance from a technical and non-technical standpoint, as called for in The Final Rule.

D. Standard – Audit Controls (Required) – 164.312(b)

Enterprise policy, standards and guidelines supported The Final Rule with regard to audit controls, but further analysis was required at the PHI-application level to determine gaps between stated policy versus actual practice.

The next step was to make an application-by-application comparison of specific policies, procedures, logging and auditing practices from the PHI-handling departments, to those called for in The Final Rule. The team again used the spreadsheets compiled during the research phase, which greatly aided the comparison process.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

This portion of the review revealed some gaps, some of which have been mentioned, and led to the bulk of the recommendations coming out of the project.

Alternatives: Effective gap analysis requires a clear understanding of what is expected, compared to what is in place. Any well thought out process that does a thorough job of identifying "where we are," compared to "where we need to be," will be a tremendous aid in identifying the work required for compliance.

5. Make recommendations to responsible areas to address findings that needed to be addressed, in order to meet the standards and implementation specifications adopted in The Final Rule.

The project team separated all findings by application, drafted an executive summary, and attached the findings, along with their associated recommendations. The recommendations were sent to the project sponsor and the project manager for their approval. Once approved, the executive summary and individual recommendations were sent to the application area contacts and their management, along with an invitation to a project recommendations meeting a week later. This gave the affected areas an opportunity to review the recommendations and prepare for the meeting.

While most systems containing PHI, and the departments working with PHI were already found to be tracking "who did what to which object, when and on which system," [9, p.2] the team felt compelled to make the following recommendations to all PHI handling departments, in order to document consistent sharing of information and expectations across the enterprise, from an access control standpoint.

- For each application containing protected health information, create a process with associated documented procedures, or review existing processes and procedures, to ensure the following:

    - Thorough review (annually at minimum) of all those individuals (internals & externals) with access to the application/data - delete access to the application/data for those who no longer require it to do their jobs.
    - This review refers to the logging and auditing of access control lists of users of the application/data.
    - It includes checking for and removal of, duplicate user IDs/accounts, inactive system accounts, suspended IDs (including process to automatically suspend id after predetermined period of inactivity), and system administrator access that is no longer required.
    - Where multiple levels of system access are available, dependent on job responsibilities, (role-based access) review each employee's level of access to confirm it is still appropriate.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Documented management approval of the regular reviews should be maintained and available.

Furthermore, the following recommendations were made to those specific areas utilizing the older mainframe homegrown PHI applications that were found to be lacking in some of the necessary transaction-level activity logging.

- Put in place or supplement current activity-level logging to ensure the ability to track logins, logoffs, unsuccessful logon attempts, and changes, additions, and deletions to all records containing PHI.
- Implement a log-in monitoring screen to be viewed upon gaining access to the application, which indicates to the user the date and time of his/her last successful logon.

Challenge: How to make sure recommendations are carried through?

Approach: Hippo has an Information Technology Security and Compliance Unit responsible for follow-up on compliance assessment/audit findings and resolutions. A representative of this group was given a copy of the executive summary along with all findings and recommendations, and invited to the project recommendations meeting. Following the reading of the executive summary and a question and answer period, the IT Security and Compliance representative shared with the group what they could expect in the way of follow-up. IT Security and Compliance would check on each area's progress in meeting the project recommendations on a quarterly basis. All areas were to be in compliance before April 21, 2005, the compliance date called out in The Final Rule.

Alternatives: The Information Security Officer is ultimately responsible for making sure the company is in compliance with the legislation. The ISO can designate a compliance body to oversee the progress, or personally take on the responsibility. Either way, regular progress checks are a good idea to ensure the work is on track to meet the deadline.

Summary

The HIPAA legislation has placed a tremendous burden on covered entities across the country, and addressing compliance issues can be frustrating and confusing. There is a good deal of assistance and educational material available on the web. For a successful compliance project, it is important to break the work down into manageable pieces, identify and secure the proper resources, develop a systematic approach through careful planning, then stick to the plan.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References:

1. "Strategies For Complying With the Final HIPAA Security Rule." RSA Security Inc. White Paper. March 2003. Page 5. URL: http://www.rsasecurity.com/solutions/health/downloads/HIPAA_WP_0303.pdf (9 August 2003)

2. Federal Register Part II Department of Health and Human Services, Office of the Secretary 45 CFR Parts 160, 162, and 164, "Health Insurance Reform: Security Standards; Final Rule." 20 February 2003. URL: http://aspe.hhs.gov/admnsimp/FINAL/FR03-8334.pdf (9 August 2003)

3. Centers for Medicare and Medicaid Services. URL: http://cms.hhs.gov/hipaa/ (10 August, 2003)

4. Laliberte, Scott. "HIPAA Security." International Association of Privacy Professionals. 14 October 2002. URL: http://www.privacyassociation.org/docs/academy2002/2.05Laliberte.pdf (9 August 2003)

5. Suarez, Walter, M.D. "Security Standards." Strategic National Implementation Process (SNIP). URL: http://www.wedi.org/snip/public/articles/details%7E12.htm (10 August 2003)

6. Workgroup for Electronic Data Interchange (WEDI). URL: http://www.wedi.org/ (10 August 2003)

7. "PricewaterhouseCoopers Interpretation of the Final HIPAA Security Rule." 15 April 2003. Pages 1 & 2. URL: http://www.hhic.org/hipaa/pdf/PWCsecurityrules050503.pdf (13 August 2003)

8. Robinson, Ellen. "Case Study in Implementing Security for HIPAA Privacy Compliance." 21 June 2003. URL: http://www.sans.org/rr/paper.php?id=1184 (26 August 2003)

9. Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC). "Security and Privacy Auditing in Health Care Information Technology." White Paper. November 2001. Pg. 2. URL: http://www.nema.org/docuploads/112153BA-486E-4E55-AEBA50D8CEF2C0C5/Security_and_Privacy_Auditing_In_Health_Care_Information_Technology-November_2001.pdf (22 August 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

10. "Standards for Privacy of Individually Identifiable Health Information." [45 CFR Parts 160 and 164]. Office for Civil Rights. Rev. 6 July 2001. URL: http://www.hin.com/070601guidance.html (25 August 2003)

11. Mezcer, Andrew H., Ph.D. "45 CFR PART 160 –General Administrative Requirements and 45 CFR PART 164 – Security and Privacy." 20 February 2003. URL: http://www.wedi.org/snip/public/articles/45CFR160&164.pdf (23 August 2003)

12. Whiting, Rick. "Sybase Adds Support for HIPAA Standards." 9 July 2002. URL: http://www.informationweek.com/story/IWK20020709S0002 (12 August 2003)

13. Hunt, Drew. "HIPAA Compliance Case Study: Establishing and Implementing a Program to Audit HIPAA Compliance." URL: http://207.44.246.52/~ehcca/presentations/HIPAAWest3/5_07.ppt (23 August 2003)

14. "Three Levels of Employee Access Drive Minimum Necessary PHI." AIS Health.Com. Reprinted from Report on Medicare Compliance. 30 January 2003. URL: http://www.aishealth.com/Compliance/Hipaa/RMCThreeLevels.html (15 August 2003)

15. "Audit Trails Back Up HIPAA 'Minimum Necessary' Rule." AIS Health.Com. Reprinted from Report on Medicare Compliance. 21 November 2002. URL: http://www.aishealth.com/Compliance/Hipaa/RMCAuditTrail.html (15 August 2003)

16. Department of Health and Human Services. URL: http://aspe.hhs.gov/admnsimp/ (9 August 2003)

17. SNIP Security and Privacy Workgroup. "Audit Trail Clarification White Paper, Version 4.0." 1 May 2003. URL: http://www.wedi.org/cmsUploads/pdfUpload/WhitePaper/pub/S-Audit4.0.pdf (24 August 2003)

18. SonicWALL Inc. "Network Security Solutions for Healthcare – HIPAA and Beyond." White Paper. March 2003. URL: https://partners.mysonicwall.com/WhitePaper/DownloadCenter/pdf/WP_HIPAA.pdf (24 August 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 1st, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced