Regulatory Advisory

AHA
Advancing Health
in America

AHA's Regulatory Advisories, a service to members, are produced whenever there is a significant development that affects the job you do in your community.
(If you did not receive all 11 pages of this advisory, visit "What's New" at http://www.hospitalconnect.com/aha/key_issues/hipaa/index.html.)

The Final HIPAA Security Rule: Making Progress in Implementation

A Message to AHA Members:

On February 20, the Department of Health and Human Services (HHS) published the final Health Insurance Portability and Accountability Act (HIPAA) security rule in the *Federal Register*. The rule established April 21, 2005 – the date for compliance with the security rule – as the latest deadline that hospitals must consider as they move ahead with their HIPAA implementation efforts. April 14 and October 16 mark the compliance deadlines for the medical privacy and the transactions and code set standards rules, respectively. The AHA described some significant aspects of the security rule in the February 27 *Hospital Highlights* (available at www.aha.org by clicking on "HIPAA" under the Key Issues section).

The final security rule is a welcome improvement over the proposed rule. Now, the rule is more compatible with the HIPAA medical privacy rule, and several administrative requirements in the proposed rule that were duplicative or confusing in light of the medical privacy rule have been simplified or eliminated. Hospitals will need to engage in an ongoing process of re-evaluation and assessment to ensure that security measures remain reasonable and appropriate in light of changing security threats and evolving technological capabilities, and maintain compliance with the security rule's requirements.

With the long awaited February publication of the final HIPAA security regulation, hospitals are finally in a position to accelerate their efforts to address the security of their information systems. To support hospitals' progress in implementing the final rule's requirements, the AHA joined with **Ernst & Young** to develop this *Regulatory Advisory*. It describes the rule's core requirements that hospitals must implement, highlights significant differences between the final and proposed rules, suggests how hospitals can jump start their security efforts by leveraging medical privacy rule compliance information and resources, identifies the key challenges that hospitals face in implementing the rule, and recommends how hospitals can avoid these potential pitfalls.

To ensure that you are better prepared to address the security rule's requirements, check off the following items from your to-do list:

✓ Share the attached advisory with your chief information officer, or information security officer if one already has been designated, legal counsel, and the staff team involved in planning and implementing the HIPAA information security program.

- ✓ Get your organization's information security efforts organized and moving ahead without delay to allow sufficient time to identify and adequately address security needs before the April 21, 2005 compliance deadline.
- ✓ Arrange to receive regular reports on your organization's efforts to ensure its steady progress toward full compliance with the rule's requirements.
- ✓ Commit time and resources within your hospital to establish the ongoing process of re-evaluation and assessment of the security program that will be necessary to ensure continued compliance with the security rule's requirements.

The AHA is concerned that the long delay in issuing the final security rule unnecessarily strains hospitals' already scarce resources. Hospitals and health systems were forced to wait more than two years for HHS to release the final security rule. During that time, in order to meet their HIPAA medical privacy rule obligations, hospitals implemented specific administrative, technical and physical safeguards to protect the confidentiality of protected health information. Forced to adopt these measures without the benefit of a final security regulation, hospitals now face needless added costs to modify these "reasonable safeguards" to ensure that they comply with the final security rule. Additionally, the final security rule requires hospitals to perform a number of tasks that clearly mirror and even duplicate tasks already performed as part of their efforts to comply with the medical privacy rule. For hospitals, these tasks certainly could have been performed more efficiently and cost effectively as part of a comprehensive compliance effort focused simultaneously on both privacy and security concerns.

The Office of HIPAA Standards, the division within HHS responsible for enforcement of the security rule, has indicated that it intends to issue guidance and clarification of the rule generally through written documents and postings on its Web site. For updates on these developments and other information and resources related to the HIPAA security requirements, contact the AHA at (800) 424-4301, or visit our HIPAA Web site, www.aha.org.

Rick Pollack
Executive Vice President

August 22, 2003

ERNST & YOUNG
Quality In Everything We Do

AHA
Advancing Health in America

Regulatory Advisory

August 22, 2003

The Final HIPAA Security Rule: Making Progress in Implementation

Background

The Department of Health and Human Services (HHS) published the final HIPAA security rule in the February 20 *Federal Register*. Hospitals have until April 21, 2005 to become compliant with the rule. The AHA described some significant aspects of the security rule for hospitals in February 27 *Hospital Highlights* (available at **www.aha.org** by clicking on "HIPAA" under the Key Issues section).

The AHA is pleased that the final security rule simplifies or eliminates several administrative requirements that were duplicative or confusing in light of the privacy rule and that the privacy and security rules are now more compatible. However, we are disappointed that the long delay in issuing the final security rule unnecessarily strains hospitals' scarce resources. For example, the final security rule requires hospitals to perform a number of tasks that clearly mirror and even duplicate tasks already performed as part of their efforts to comply with the medical privacy rule. Hospitals certainly could have performed these tasks more efficiently and cost effectively as part of a comprehensive compliance effort focused simultaneously on both privacy and security concerns.

The publication of the final HIPAA security regulation means that hospitals are now in a position to refine their efforts to address the security of their information systems. Hospitals are encouraged to move ahead without delay on their information security efforts to ensure that there is sufficient time to address security rule compliance concerns before the April 21, 2005 deadline. Hospitals also will need to engage in an ongoing process of re-evaluation and assessment to ensure that security measures remain reasonable and appropriate in light of changing security threats and evolving technological capabilities and to remain in compliance with the security rule's requirements.

To support hospitals' progress in implementing the final security rule's requirements, the AHA joined with Ernst & Young to develop this *Regulatory Advisory*. It describes the core requirements of the rule that hospitals must implement, highlights significant differences between the final and proposed rules, suggests how hospitals can jump start their security efforts by leveraging medical privacy rule compliance information and resources, identifies the key challenges that hospitals face in implementing the rule and recommends how hospitals can avoid these potential pitfalls.

Hospitals also are encouraged to contact the AHA at (800) 424-4301, or visit our HIPAA Web site, www.aha.org for updates on any guidance and clarification of the rule from the federal regulators as well as other information and resources related to implementation of the HIPAA information security requirements.

Overview of the Rule

As currently written, the final security rule applies only to protected health information (PHI) that is stored or transmitted electronically, whether or not it involves one of the HIPAA standard transactions. Electronic medical record systems and order entry systems, for example, are subject to the security standards. The rule also indicates that fax-back and voice response systems will generally require security measures by one of the parties involved.

The security rule, however, does not cover information in oral, paper or other non-electronic format. Moreover, the preamble to the security rule makes clear that paper-to-paper faxes, person-to-person telephone calls, video teleconferencing, and voice-mail messages, where information is in non-electronic form before transmission, are not subject to the security rule. Also, copy machines, fax machines and telephones, even if they contain memory and can produce multiple copies, are not considered electronic media subject to the security rule.

Core Requirements of the Final Rule

For hospitals, the core of the security rule lies in the requirements specified in §164.306(a). Specifically, hospitals must:

- Ensure the confidentiality, integrity and availability of all electronic PHI they create, receive, maintain or transmit.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the privacy rule.
- Ensure compliance with the security rule by their workforces.

Hospitals will meet these requirements by complying with the standards set forth in the rule. The standards (referred to as “requirements” in the proposed security rule) are organized into three major HIPAA security categories — administrative, physical, and technical safeguards — as well as two smaller categories of standards that were added in the final rule, organizational requirements, and policies, procedures and documentation.

Associated with the standards are implementation specifications that can be generally viewed as security functions. Some of these implementation specifications are “required” and others are “addressable.” As the label implies, *required* implementation specifications must be implemented by all hospitals. Hospitals do not necessarily need to implement *addressable* implementation specifications. Addressable specifications that are “reasonable and appropriate” should be implemented. For those addressable specifications that are not “reasonable and appropriate,” however, hospitals should document their explanations of why implementation of the specification is not reasonable and they may substitute other “reasonable and appropriate” alternatives for these specifications. In all cases, the covered entities must meet the controls required by the standards.

A brief description of the five security categories and the standards they contain is presented below:

Administrative Safeguards contains the majority of the security standards and implementation specifications. The nine standards in this category outline the process infrastructure that needs to be in place for effective security of electronic PHI. The standards address security management, assigned security responsibility, workforce security, information access, security awareness and training, security incidents, contingency plans (for emergencies and disasters), evaluation of security effectiveness, and business associate contracts (or other arrangements) with hospital business partners.

Physical Safeguards outlines the physical infrastructure that needs to be in place for the security of electronic PHI. The four standards in this category address facility access controls, workstation use, workstation security, and device and media controls. Although there are fewer standards in this category than in administrative safeguards, they are an integral part of any sound security strategy.

Technical Safeguards outlines the technical infrastructure that needs to be in place for the security of electronic PHI. The four standards in this category address access control, audit controls, integrity (of electronic PHI), person or entity authentication and transmission security. It is important to note that although the title of this category is "Technical Safeguards," technology-specific requirements (e.g., technical encryption/decryption protocols for Internet transmissions) are not provided. This is intentional because HHS wrote the final rule to be technology neutral.

Organization Requirements outlines the standards for the security aspects of business associate contracts and group health plans.

Policies, Procedures and Documentation outlines the standards for security policies/procedures and other due diligence documentation (e.g., risk analysis results) that need to be developed, retained, made available to persons responsible for implementing the procedures to which the documentation pertains, and updated as changes occur.

Differences Between the Proposed and Final Security Rule

Some key differences between the proposed and final rules include:

- The final rule is more limited in scope than the proposed rule and only covers electronic PHI. *This is a contrast with the privacy rule, which covers PHI in any form, not just electronic.* In the proposed rule, safeguards had to be applied to electronic health information of individuals.
- The concept of required and addressable implementation specifications has been introduced in the final rule. The proposed rule only had required implementation specifications.
- The final rule describes standards or principles with which entities need to comply, but it softens the descriptions of how to comply through addressable implementation specifications. The proposed rule had more details on how to comply.
- The final rule underscores that a risk analysis forms the basis for determining the methods

for complying with the rule. The proposed rule was not as emphatic on this point.

- Scalability, flexibility, cost and security capabilities are key criteria for making security decisions and determining how to comply. The proposed rule did not underscore these points as heavily.
- Documentation requirements for policies/procedures, risk analysis results, security decisions, and their supporting justifications are stressed heavily in the final rule. Documentation must be retained for six years. The proposed rule did not focus on documentation nearly as much, and did not have a retention period requirement.
- The certification standard for technical systems and software in the proposed security rule has been replaced in the final rule with an evaluation standard that applies to the technical and non-technical components of security.
- In the final rule, business associate agreements are the basis for extending the security of electronic PHI to hospital business partners. The proposed rule had a separate contract vehicle called a "chain of trust agreement" for this purpose.
- A separate "Organizational Requirements" section (§164.314), detailing the requirements for business associate agreements and group health plans, has been added to the final rule. This section did not exist in the proposed rule.
- There is a greater alignment of the security concepts with the terms, definitions and standards for privacy in the final security rule. The proposed security rule had a number of inconsistencies with the privacy rule.

The Impact on Large vs. Small Hospitals

The final rule was purposely written to apply to small rural hospitals as well as to large-scale hospital systems. It sets out a process for making decisions about security concerns rather than recommending any specific technologies or required solutions to address security needs.

Compliance efforts are to be proportional to the size and complexity of the organization. If a hospital is small and less complex, the implementation requirements should be less complex. If the hospital is large and more complex, the implementation requirements will likely be more involved and complex. For example, to comply with the "assigned security responsibility" standard, a small outpatient clinic may determine that is it reasonable and appropriate to assign this responsibility to its existing office manager, who would administer the security function at the clinic, in addition to fulfilling existing responsibilities. A multi-location, large-scale hospital system, on the other hand, may have to comply with this standard in a more involved fashion. This organization might hire a full-time security official along with a dedicated staff of security professionals. As part of a new security department, the team would be responsible for managing the security function across the hospital system.

The risk analysis is the key for determining, documenting and defending decisions regarding methods of compliance.

Getting Started

To comply with the final security rule, hospitals should first conduct a thorough security risk analysis that focuses on threats to electronic PHI. A risk analysis must identify the exposure of electronic PHI to unauthorized access, corruption or outages. For the risk analysis to be thorough, it must address all instances of electronic PHI and associated threats in hospital facilities, computer applications, systems and networks.

The privacy gap assessment and PHI data flows that should have been prepared for privacy compliance are key sources of information for getting started. The electronic PHI needs to be mapped to the hospital facilities, computer applications, systems, and networks in which they reside and traverse to provide the necessary framework for conducting the risk analysis. The results of the risk analysis and the completion of a HIPAA security gap assessment will form the basis for selecting reasonable and scalable security solutions and beginning the process of compliance.

Completing a security gap assessment requires a firm understanding of the intent and substance of the security regulations and its relationship to the privacy regulations. A project team of clinical, operations, IT and security personnel should be assembled to perform the gap assessment. The project team should develop and use a questionnaire based on the security standards and implementation specifications as the basis for interviewing departments and personnel within the hospital who are familiar with current practices. Additional supporting documentation, such as policies, configuration standards, and contingency plans, should be gathered, reviewed and validated by the project team. All of this information needs to be analyzed to determine the gaps between current practices and what is required by each of the security standards. A rating system should be used to indicate the severity of each gap, e.g., high, medium or low. The results could then be summarized into a gap assessment report that provides the organization with a clear understanding of its HIPAA security gaps.

The security gap analysis and the privacy compliance plan are the major ingredients for developing a hospital's security strategy. A plan to address the security gaps in priority of their risk should form the backbone of the security strategy. The privacy plan may already have introduced controls to address any number of identified security gaps. If this is the case, these controls should be considered and incorporated into the specific security strategy.

Once a security strategy is developed, the next step is execution. Something to consider early on is the designation of a security official who would have overall responsibility for security. The security official should be the owner of the security strategy and its implementation. The qualifications and positioning of the security official were discussed earlier and are dependent on the results of the risk analysis. In fact, in a small hospital, it may even be appropriate for the privacy and security official to be the same person. As the organization's size and complexity increases, the experience and skills of the security official will be greater and this should be reflected in the reporting relationship. The security official's overriding responsibility is the management and administration of the security program that will achieve and maintain HIPAA security compliance.

Although compliance with the final security rule is not required until April 21, 2005, its affect on privacy may be immediate and should be considered; hence, a sense of urgency in getting started is prudent. Finally, as part of an ongoing risk management program, the risk analysis and gap assessment should be repeated periodically to identify new security threats and gaps.

Issues for Hospitals to Consider in Complying with the Final Rule

Hospitals may be more challenged to implement some of the standards in the security rule than others. The size and complexity of hospitals and their operations will have a direct bearing on the degree of difficulty they may encounter in complying with the standards in the final rule. The following challenges and recommendations may help hospitals avoid potential pitfalls.

Challenge: Security Management Process

Many hospital security officers are clinicians who became systems analysts and may lack the experience and knowledge in performing IT risk analysis and risk management. This problem is compounded when there is a lack of qualified resources and funding necessary to perform a thorough risk analysis.

In addition, some hospitals may prefer to do the minimum necessary when it comes to security, especially with respect to "addressable" implementation specifications. Hospitals may also find it difficult to establish and enforce sanctions due to the nursing shortage and the overall difficulty with sanctioning physicians.

Recommendations to Consider

- Allocate sufficient funding and resources to perform a thorough risk analysis.
- Develop or obtain a structured and an appropriate risk analysis methodology or services through peer groups, professional associations and services firms. Peer groups may be other health care facilities in the community or hospitals of similar size and function located around the country.
- Perform appropriate IT risk analysis and risk management tasks.
- Develop a business case and consensus to implement more than minimal or superficial security technology and procedures, especially with respect to "addressable" implementation specifications.
- Educate executives and allocate sufficient resources to address sanction requirements.

Challenge: Information Access Management

Hospitals typically have multiple information systems with several different system administrators. Some systems may not support strong authentication, with shared IDs and passwords being commonplace in these hospital environments. Adding to this challenge is the fact that many hospital applications are not easily integrated with simplified sign-on solutions.

The hospital workforce includes many non-employees making it difficult to establish an effective termination process across the workforce. Frequent hospital employee inter-departmental transfers also create difficulties for maintaining appropriate user access rights.

Recommendations to Consider

- Avoid solving the same challenge multiple times by coordinating and leveraging solutions across multiple systems and administrators. For example, entities may establish committees comprised of representatives from mainframe, midrange, networking, and other technology areas that exhibit risks. The committees may work together to co-develop standard processes that are platform independent and to identify technology solutions that apply across technology platforms. There are numerous vendors offering cross platform solutions that address single sign-on, user administration, access control, logging and reporting functions.

- Develop or obtain supplemental technologies to support authentication and access controls where they do not exist in existing systems. Currently, there are products available on the market that allow system administrators to manage login controls for many applications on multiple technology platforms (mainframes, servers, PCs, etc.) through a single application. Technology companies also provide solutions that address a wide range of technology issues for encryption, logging, monitoring, and reporting.
- Eliminate the practice of sharing IDs and passwords by establishing and enforcing supporting policies, educating users to the related risks, and providing alternative solutions. These alternative solutions should include sign-on or token-based authentication to technically enable appropriate controls. (A security token is a physical device, such as a smart card or key fob, which is combined with a PIN to authorize access to a computer system or network.)
- Develop or obtain procedures and technologies to address access controls for the large non-employee workforce in hospitals. Using business associate agreements, contracts, revocable tokens and frequent authorization log review procedures increases the likelihood that people with expired access are identified and removed from the system.

Challenge: Contingency Planning

Many hospitals lack the experience and skills necessary for developing and maintaining comprehensive Disaster Recovery and Business Contingency Planning (DRP/BCP) programs. There is a perceived high cost and elusive return on investment with respect to these programs. In addition, organizations must deal with rapidly changing environments (e.g., the introduction of clinical care systems). These circumstances mean that ongoing maintenance of DRP/BCP programs will be required to keep them current.

Recommendations to Consider

- Ensure availability of appropriate expertise and understanding in developing comprehensive disaster recovery and contingency planning programs.
- Develop or obtain appropriate approaches through peer groups, professional associations of information systems and technology professionals, and services firms. Peer groups may be other health care facilities in the community or hospitals of similar size and function located around the country.
- Perform sufficient research and analysis to develop a business case for appropriate DRP/BCP plans and controls. A Web search provides many sources of information. Many professional associations for information systems and technology professionals also have information on leading service providers and advisors. A business impact analysis (referred to as a “BIA”, which is a standard analysis activity and the initial step in developing DRP/BCP plan) would determine the recoverability requirements of key operational processes that interact with electronic PHI. Although this level of analysis is more involved, it would provide the necessary information to determine and support the business case for developing appropriate DRP/BCP plans.
- Address emerging technologies such as clinical care systems and hand held devices by identifying associated risks and taking measures to mitigate related exposures. Utilizing legacy or trusted technologies to replicate or mirror emerging technology operations increases the likelihood that information will be available when needed.

Challenge: Facility Access Controls

Hospitals are designed to provide access to patients, visitors and employees as a critical component of the services they provide. Systems are logically placed in accessible locations to facilitate services. The accessibility of facilities and systems exposes them and the information that resides on them to risk of theft or unintended information disclosure.

The risk can be significantly higher when there are multiple buildings/facilities present at one or more hospital campuses. The challenge of controlling physical access to electronic PHI, monitoring the entrances and exits, as well as appropriately safeguarding PHI becomes more difficult as the number of buildings/facilities goes up, and the traffic through them increases.

Recommendations to Consider

- Increase the difficulty of removing systems and media by providing anchors and locked storage and implementing clean desk practices.
- Implement human and technical surveillance to increase the perception of theft detection.
- Develop or obtain mechanisms to obscure and secure information in commonly accessible areas such as password protected screen savers and blinders that obscure the views of screens from side angles.
- Improve logical access controls and data protection at the system level through encryption, robust passwords or tokens to reduce risk of loss if facility controls are breached.

Challenge: Transmission Security

The Internet is being leveraged to increase communications with patients and the non-employee workforce (physicians), but Internet-based email is generally sent in an unencrypted format. This clearly increases the security risk to electronic PHI. The situation is further exacerbated by the introduction of unsecured wireless technology that is being rapidly rolled out within hospital environments.

Recommendations to Consider

- Research and identify appropriate methods to encrypt PHI transmissions in email and other electronic forms. A Web search provides many sources of information. Many professional associations for information systems and technology professionals also have information on leading service providers and advisors. Solutions should mitigate the exposures identified in the risk analysis.
- Address exposures in wireless networks through access controls and encryption. A prevalent risk is interception of unencrypted information and “sniffing” – electronic eavesdropping. Many encryption packages that would address this concern are currently available at various costs. The challenge is in providing passwords to recipients. Where recipients are “repeat receivers,” it is relatively easy to exchange and establish encryption “keys” or certificates. Where recipients have no established certificates, Web-based email programs that rely on browser-based encryption are gaining growing acceptance.