Chapter 13
Getting Started with HIPAA Security Compliance

Kevin Beaver

OVERVIEW OF THE HIPAA SECURITY RULE

It's All about Best Practices

In August 1998, the U.S. Department of Health and Human Services (HHS) published the Security and Electronic Signature Standards; Proposed Rule (Security Rule). The Security Rule covers all healthcare information that is electronically maintained or used in electronic transmissions. It is defined by HHS as a set of requirements with implementation features that providers, plans, and clearinghouses must include in their operations to assure that electronic health information pertaining to an individual remains secure.[1] The Security Rule is merely a set of common best practices that is intended to be comprehensive, technology neutral, and scalable for different-sized organizations. It is a high-level information security framework that documents what needs to be done to secure healthcare information systems. At the same time, and much to widespread chagrin, the Security Rule is not a set of how-to instructions outlining the exact steps for securing healthcare information systems.

When the Security Rule was originally developed in the late 1990s, there were limited information security standards upon which a comprehensive information security framework for the healthcare industry could be developed. In fact, it is documented in the proposed Security Rule that no single standards development organization (SDO) is addressing all aspects of healthcare information security and confidentiality; and specifically, no SDO is developing standards that cover every category of the security framework.[1] Enter the Security Rule. Since 1998, several standards have evolved, such as the ISO/IEC 17799 Information Technology — Code of Practice for Information Security Management, among others. It is

0-8493-1498-4/03/$0.00+$1.50

not currently known whether the final Security Rule will be based on any well-known standards, but healthcare organizations can benefit from utilizing these standard guidelines nonetheless.

Covered Entities

As with the other HIPAA rules, the covered entities that are required to comply with the Security Rule are as follows:

- *Healthcare Providers.* These include hospitals, clinics, nursing facilities, laboratories, physicians, pharmacies, and most other entities that provide healthcare services.
- *Health plans.* Generally speaking, these are any individual or group plans that provide or pay for medical care. Examples include private and governmental issuers of health insurance, HMOs, PPOs, Medicare and Medicaid programs, and certain employer-sponsored health plans.
- *Healthcare clearinghouses.* These include entities that process or facilitate the processing of nonstandard data elements of health information into a standard format for electronic transactions.
- *Business associates.* A person or organization that performs, on behalf of a covered entity, an activity involving the use or disclosure of individually identifiable health information. Examples include financial advisors, accountants, auditors, lawyers, and consultants.

The list above basically boils down to any entity involved in accessing, electronically transmitting, or storing individually identifiable health information.

Value Created by the Security Rule

Staying out of hot water in civil and criminal actions and protecting critical business assets is reason enough to secure information for some, but not all. The Security Rule, like information security in general, is often viewed as a cost center and a barrier to providing effective healthcare. Many doctors, clinicians, and nurses find that information security policies and procedures are an impediment to getting their jobs done. This is accurate when information security is poorly implemented. In fact, when implemented and managed with business processes in mind, information security can have quite the opposite effect. The Security Rule actually provides business value that can be leveraged to lower healthcare costs, increase the efficiency of healthcare operations, and help build long-term customer loyalty.

The Security Rule provides ways for healthcare organizations to leverage information technology in order to offer services that were not previously possible. For example, certain healthcare providers can allow patients to access and administer their private healthcare information via the Internet, knowing all along that their information is being protected from unauthorized use. In addition, wireless technologies that were traditionally insecure

can be leveraged to make physicians' jobs easier and more efficient while protecting them from various liabilities. Secure wireless infrastructures will allow these users to rest assured that the health information on their PDAs (personal digital assistants) is stored, administered, and transmitted securely via access controls and encryption. In addition, information security that is managed properly can create value by giving patients life-long confidence that their private healthcare information is being managed securely and responsibly.

The Security Rule's Relationship with the HIPAA Privacy Rule

The Security Rule has a close relationship with the HIPAA Privacy Rule, in which covered entities are required to comply with by April 14, 2003. In fact, a significant portion of the privacy requirements relies on a solid information security infrastructure in order to be implemented properly. The Privacy Rule mandates that appropriate administrative, technical, and physical safeguards be in place to protect the privacy of health information. That is, information security technology, policies, and procedures must be in place in order to comply with the privacy requirements. The bottom line is that one cannot have privacy without security. Perhaps the original rule makers at HHS did not think about this when they established the privacy requirements long before the security requirements were finalized, much less enforced. Regardless, it would behoove all covered entities to start studying the Security Rule, or at least some published information security best practices (e.g., ISO/IEC 17799). They then must make certain minimal efforts to deploy the policies, procedures, and technologies required for a basic information security infrastructure in order to be fully compliant with the Privacy Rule in 2003.

INSIGHT INTO THE SECURITY RULE

Like any well-designed information security system, the focus of the Security Rule requirements revolves around the confidentiality, integrity, and availability (CIA) of electronic data. At the time of this writing, the proposed Security Rule is divided into four different categories:

1. Administrative Procedures
2. Physical Safeguards
3. Technical Security Services
4. Technical Security Mechanisms

Each category has a corresponding set of requirements that covers all aspects of the business and technical systems that make up an overall information security infrastructure. In the current version, there is a fair amount of overlap between the four different categories, which may cause confusion. In addition, it has become public knowledge that the electronic signature requirement in the proposed Security Rule is going to be

dropped in the final version. Given that these categories are based on various best practices and information security standards, it is most likely that they will not change much in the final Security Rule. Either way, perhaps the final version will be clearer and illustrate that the requirements do not have to be quite as confusing or complicated as initially thought.

There is nothing new or magical about the Security Rule requirements. In fact, even if slight modifications are made in the final version, the proposed rule, if followed and implemented properly, consists of the majority of all information security best practices. That is, covered entities can use the information currently available to get started on their security initiatives now and be well on their way to full Security Rule compliance once the deadline is reached and the rule is enforced.

To ensure the CIA of healthcare information, the Security Rule outlines various technologies, policies, and procedures that must be implemented. From a high-level perspective, these policies and procedures include the following:

- Assigned security responsibility
- Instructions and procedures for secure computer usage
- Formal mechanism for processing and handling data
- Procedures for handling and controlling various media
- Incident response plan
- Disaster recovery plan
- Security configuration management
- Security awareness training
- Personnel termination procedure
- Ongoing security management

In addition, technology-based systems include:

- Logical access controls
- Physical access controls
- User authentication controls
- Authorization controls
- Audit controls
- Data encryption mechanisms

Given the technology-neutral stance of the Security Rule, there are no detailed requirements for specific technologies such as firewalls, authentication systems, or even encryption methods that must be deployed. However, their use is implied because technologies such as these must be used to enforce and support certain policy and procedure requirements.

Because information security is not a specific product or one-time event, care must be taken to ensure that ongoing risks are properly managed. The growing complexity of information systems leads to a multitude of unknowns. If one combines poorly written software, a general lack of

consequences and liability, and security expertise that is difficult to find, then effective information security management is quite difficult to achieve — but it is not impossible. The keys to effective security management are ongoing information risk assessments and audits, regular security training for staff members, and consistent system maintenance and monitoring. It is the combination of these that make up the backbone of a solid information security infrastructure and also make good business sense.

MOVING FORWARD

Forming the Team

The first step toward Security Rule compliance requires the assignment of security responsibility — a Security Officer. The Security Officer can be an individual or an external organization that leads Security Rule efforts and is responsible for ongoing security management within the organization. To maximize the success of this Security Officer role, this person or organization must have authority and decision-making power, be able to provide guidance on security initiatives, and ultimately take full responsibility for Security Rule compliance. Credibility and sound judgment are very important, and upper management support for this position is absolutely essential.

Once this security responsibility has been established, it is essential to form a team of individuals to assist with compliance efforts. Because Security Rule compliance is not just an IT issue, it is important to bring in individuals from all departments who have a stake in this — legal, HR, operations, IT, etc. At some point, this team will likely include representatives from the entire organization. The team can be comprised of members external to the organization, but there must still be points of contact from within in order to accurately gather information on current business processes and systems.

Keep in mind that there are pros and cons to forming an in-house compliance team versus outsourcing the compliance efforts. An in-house team requires specific technical and business-related security expertise that may not exist in the current staff or that may require costly ongoing training. In addition, an in-house team may require that employees are regularly pulled away from their normal daily tasks to handle information security issues, and this may not make good business sense. On the other hand, an internal staff tends to know much more about the organization's information systems, which can help to streamline the implementation. It may also be easier to trust in-house personnel than outsiders, because the relationship has already been established.

In choosing to outsource Security Rule compliance efforts, there are four main things to consider. First, it is essential to find firms that specialize in information security, and specifically HIPAA security compliance. You

will need highly skilled experts, not IT generalists. Firms that specialize are where the experts work. Second, you get what you pay for — within reason. If you search around, you can find expertise in smaller firms that will suit you just fine without having to pay the higher overhead costs associated with larger firms. Third, external experts have less exposure to internal politics. They can stay away from — for the most part — departmental bias and can provide fresh and impartial insight into what really needs to be done. Fourth, watch out for conflicts of interest that could possibly occur if you deal with vendors that try to push specific security products without considering the whole picture or your best interests.

Assessing the Gaps and Risks

Once the Security Rule regulations and information security best practices have been studied and are well understood by the entire compliance team, the next step will be to perform a gap analysis and an information risk assessment. From a high-level perspective, this should help you understand where you are now with your information security initiatives compared to where you need to be according to the Security Rule requirements. In addition, it will help identify current information risks as they relate to the Security Rule. This analysis will help determine the impact the Security Rule has on your the organization. It will also help you understand the scope of your upcoming compliance efforts. Some key steps involved in this process are:

- Interviewing key personnel to gather facts
- Documenting existing information flows within the organization
- Taking an inventory and classifying all electronic health information
- Determining which assets you need to protect
- Assessing the threats and vulnerabilities you are trying to protect against
- Evaluating existing security policies and procedures
- Determining and documenting what technologies and processes are currently in place to protect your information systems
- Reviewing and documenting all electronic information that is shared with business associates

Once this information is gathered, you will be able to identify and prioritize your gaps and information risks in order to get started on creating the compliance plan.

Creating and Implementing the Plan

Once the security gaps and information risks are identified, management should be briefed and a budget created. The next step is to create a compliance plan. It is essential that this plan contain documented roles and responsibilities, along with a prioritization of specific needs, a timeline, and a

list of all deliverables involved. It may be difficult to estimate and secure these resources initially, but not to worry; this can be fine-tuned over time once the team becomes more accustomed to the workload. It is important, however, that everyone on the team, including the Security Officer, buys into and completely understands the plan.

One recurring requirement in the proposed Security Rule, and a general best practice, is to document everything involved with the compliance plan. This plan cannot exist only in the minds of the stakeholders. It must be written clearly and regularly updated. It is also a good idea to keep a backup copy of the plan offsite for disaster recovery purposes. This is not going to be a document that you will want to recreate from scratch! The documented plan will not only prove to be a valuable source for future reference, but will also be used to hold people accountable and serve as proof that the organization is working toward Security Rule compliance.

When the plan is in place and the time is right, the compliance initiatives can commence. Keep in mind that there is no need for perfection initially. All that can be expected is for you to create a good plan and show that you are working on it. Depending on the size and complexity of the organization and current information systems infrastructure, the implementation process could range from being fairly straightforward and simple, to being quite complicated and resource intensive. Either way, a project such as this can be made less daunting with proper planning, execution, and management.

CONCLUSION

Complying with the HIPAA Security Rule is similar to any other compliance program. It revolves around designation of the responsibilities, establishing the appropriate policies and procedures, and maintaining these initiatives from a risk management perspective on an ongoing basis. Preparing for the Security Rule requirements does not have to be that complicated, especially if covered entities start early and certain information security best practices are already in place. The sooner that HIPAA covered entities start on their Security Rule initiatives, the cheaper and easier it will be. Some covered entities will have to overhaul their current information security infrastructure. Others that have a fairly simple IT infrastructure may have to start from scratch. Either way, organizations can save time, effort, and money by integrating information security and Security Rule compliance with current IT and HIPAA Privacy Rule initiatives.

By laying a solid information security foundation now, instead of layering it on top later when resources are slim and expertise is difficult to find, covered entities will be in a much better position to manage Security Rule compliance more effectively and minimize their costs. The key is to go into this with the attitude that the Security Rule, and HIPAA in general, make

good business sense. Moving forward, remember to document everything to support your decisions. This documentation will prove very valuable in the future when it is needed.

References

DEPARTMENT OF HEALTH AND HUMAN SERVICES, OFFICE OF THE SECRETARY, *Security and Electronic Signature Standards; proposed rule*. Federal Register document 45 CFR part 142, 1998.