

Comments on HIPAA Final Security Rule

Stephen Cobb, CISSP & Chey Cobb, CISSP

February, 2003

Background:

Through standardization of payment transaction codes, the Health Insurance Portability and Accountability Act of 1996 encourages electronic billing for healthcare, to reduce costs and increase efficiency and thus offset the expense of extending insurance coverage to workers who change jobs. The framers of the legislation realized that it would inevitably lead to more medical data being computerized and thereby exposed to the risks associated with computer security, in three main areas:

1. Confidentiality: data revealed to people not authorized to see them
2. Integrity: unauthorized changes to data, intentional or otherwise
3. Availability: access to data denied by persons or events

For this reason, the HIPAA legislation required a Privacy Rule to be created, spelling out what was to be considered protected health information (PHI). A Security Rule was also mandated, to spell out how the protection afforded by the Privacy Rule would be assured.

Since congress declined to create any of the rules implementing HIPAA, the task fell to the Department of Health and Human Services. Over the last few years, HHS has gone through the process of issuing draft rules, seeking comments, and producing final rules.

The Privacy Rule became final at the end of 2000, although it was amended quite heavily in the summer of 2002. The deadline for initial compliance with the Privacy Rule is April, 2003 (except for smaller entities, who have another year).

The draft of the Security Rule was published in 1998 and the final version was published February 20, 2003. This means that those organizations to whom it applies must be in compliance by April 21, 2005. However, the effect of the Security Rule is more immediate than this date suggests. That is because the Privacy Rule states:

“A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information...A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.”

Organizations that have been working towards compliance with the HIPAA Privacy Rule have already had to make some decisions about what “appropriate” and “reasonable” safeguards might be. The draft Security Rule has been available since 1998 and the word from HHS has always been that the final version would not be much different from the draft, and so the draft could be used as guidance. Furthermore, it was often stated that the Security Rule is merely a reflection of security best practices, what responsible organizations should already be doing to protect sensitive personal information.

Comments:

As a result of the above, we believe a lot of people expected that the final Security Rule would provide fairly specific guidance as to exactly what constitutes “appropriate” and “reasonable” safeguards. However, the final Security Rule does not provide much specific guidance. Here is the reasoning provided by HHS:

“We received numerous comments expressing the view that the security standards should not be overly prescriptive because the speed with which technology is evolving could make specific requirements obsolete and might in fact deter technological progress. We have accordingly written the final rule to frame the standards in terms that are as generic as possible and which, generally speaking, may be met through various approaches or technologies.”

There is considerable merit in this approach, which is similar to that taken by other agencies promulgating privacy and security rules, such as those for protecting non-public financial information under Gramm-Leach-Bliley. From a technical perspective, we cannot fault the final HIPAA Security Rule. What it describes is a responsible approach to protecting sensitive personal information that could easily be generalized beyond the healthcare field. In that respect it contributes to the emergence of agreed standards for security practices.

However, from a practical perspective, the final HIPAA Security Rule is bound to disappoint. While some health care organizations might have been in favor of less prescriptive rules back in 1998, this overlooks the natural effect of a compliance deadline. The closer such a deadline gets, the more prescriptive the guidance sought by those charged with compliance. We have heard, more than once, at more than one seminar we have given on this topic, words to this effect:

“Just tell us what we have to do to be in compliance.”

If you accept that this is the prevailing sentiment, then the final Security Rule, as published, is clearly a disappointment. In fact, we think this sentiment says a lot about the effect of security through legislation, as opposed to security via self-regulation, which is a topic we look forward to discussing elsewhere. However, the reality is that the legislation is in place, as are the rules, and they will shape the way medical data security develops in America in the foreseeable future.

Consider what was said in the draft of the Security Rule and you can see how expectations for a prescriptive approach might have been raised:

“We are designating a new, comprehensive standard...which defines the security requirements to be fulfilled to preserve health information confidentiality and privacy as defined in the law.”

What we have in the final rule is comprehensive, but it does little to help covered organizations determine the risks to protected health information, or the acceptable level of protection to offset that risk. Here is what is now said in the rule:

Section 164.306, Security Standards: General Rules

Covered entities must do the following:

- (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
- (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
- (4) Ensure compliance with this subpart by its workforce.

These are straightforward. As is the breakdown of the required safeguards and requirements into five main areas: Administrative, Physical, Technical, Organizational, and Policies/Procedures/Documentation.

1. Administrative safeguards

- (A) Security management process
- (B) Assigned security responsibility
- (C) Workforce security
- (D) Information access management
- (E) Security awareness and training
- (F) Security incident procedures
- (G) Contingency plan
- (H) Evaluation

2. Physical Safeguards

- (A) Facility access controls
- (B) Workstation use
- (C) Workstation security.
- (D) Device and media controls

3. Technical Safeguards

- (A) Access control.
- (B) Integrity
- (C) Person or entity authentication
- (D) Transmission security

4. Organizational Requirements

(A) Business associate contracts or other arrangements.

(B) Requirements for group health plans

5. Policies and procedures and documentation requirements

(A) Policies and procedures.

(B) Documentation

When you dig into these sections, they are very demanding. For example, under Administrative safeguards, the security management process requires the implementing of policies and procedures to prevent, detect, contain, and correct security violations. Risk analysis is required. This means organizations must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the CIA of electronic protected health information held by the covered entity.

Risk management is also required to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. Organizations must apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures; and there must be regular review of the records of information system activity, such as audit logs, access reports, and security incident tracking reports.

This is all clearly stated, but what is not clear is how covered entities are going to accurately and thoroughly assess the potential risks and vulnerabilities. This requires detailed and current knowledge of information security. And it cannot be side-stepped. Consider what happens when you dig further into the rule and find that some items are not required but “addressable.”

For example, under “Transmission security” organizations are required to “implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.”

One obvious way to do that is encryption. But encryption is said to be “addressable.” All we are told is to: “Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.”

We think a lot of security professionals are going to have a hard time with “deemed appropriate.” That implies some sophisticated risk assessment. A typical healthcare organization will know a lot about medical risk assessment, but that’s very different from a security risk assessment, which is something you cannot perform without an in-depth knowledge of security risks.

And here is the rub. If a covered entity decides not to encrypt PHI during electronic transmission, and PHI is exposed as a consequence, it will be hard to turn to Security Rule compliance for defense. The argument would presumably be that the organization was not at fault for failing to protect the PHI with encryption during transmission, because it was not “deemed appropriate.” But we cannot imagine any security professional testifying that the risks inherent in transmitting sensitive medical information electronically without encryption were so small as to be acceptable, except in some very narrow circumstances.

Conclusions:

We anticipate that a lot of privacy and compliance professionals will be looking for a lot of answers in the next few months and years. Security professionals will be called upon to help assess risks and specify appropriate risk reduction measures.

A lot of covered entities will be designating a point person for medical data security (required) and training staff in security (required). A lot of lawyers will be waiting to pounce on medical privacy breaches that occur post-April 14, 2003.

And some companies will still be trying to decide whether or not they are covered entities and if so what security measures they need to put in place. The fact is, there are plenty of ways to get sued for violating medical privacy right now, and making anything less than a thorough and conscientious effort to assess and mitigate security risks to sensitive data carries serious risks of its own.