Summary Analysis: The Final HIPAA Security Rule

By Tom Grove, Vice President, Phoenix Health Systems
February 2003

On February 13, 2003, HHS Secretary Tommy Thompson announced the adoption of the HIPAA Security Final Rule. The final standards were published in the February 20 Federal Register with an effective date of April 21, 2003. Most covered entities will have two full years -- until April 21, 2005 -- to comply with the standards.

The final HIPAA Security Rule has been in development for well over four years, since HHS published its draft version in August 1998. Did the lengthy period of comment, controversy and revision lead to very different final provisions?

Yes... and no. Certainly, an element-by-element comparison shows that most of the controls described in the draft rule have analogues in the final rule. However, a closer examination indicates that the rule is significantly reorganized and revised, reflecting a substantial move away from the specifics of technology implementation, in favor of emphasizing security management principles and broad management controls as the primary vehicles for protecting patient health information.

Increased Privacy/Security Synergy

HHS' initial drafts of the HIPAA Security and Privacy Rules were published within a few months of each other, but close timing did not ensure that the two rules were aligned either in terminology or approach. The publication and later modification of the final Privacy Rule only served to widen the gap. A stated goal of the final Security rule (and a reason given for its publication delays) was to create greater coordination between the two -- a clear acknowledgement that the concepts of security and privacy are inextricably linked.

The most dramatic change in this realignment is a change in scope of the final Security Rule. The proposed Rule broadly proposed to cover all electronic health information pertaining to individuals. The final rule is more consistent with the Privacy Rule in that it covers "protected health information" (PHI) and, in fact, limits its scope only to PHI that is in electronic form. However, note that this refinement doesn't eliminate the requirement for security on non-electronic PHI, since the HIPAA Privacy Rule (164.530(c)) still requires appropriate security for all PHI, regardless of its format.

Other significant changes that improve the compatibility of the Security and Privacy Rules are refinements in terminology. The new Security rule adopts many definitions used in the Privacy rule, thereby eliminating confusing inconsistencies of the past. At least six terms were removed from the Privacy-specific Sections 164.501 and 164.504 and placed in a new Section 164.103 that applies to both final rules: "Plan Sponsor," "Protected Health Information," "Common Control," "Common Ownership," "Health Care Component," and "Hybrid Entity." Covered entities that have cross-referenced the definitions by rule section as part of their HIPAA implementation efforts will need to update references to these terms.

A Workable, Management-Based Approach

When HHS published the proposed Security Rule, it solicited comments regarding the level of detail expressed in the rule. Numerous commenters noted that the Security standards should not be overly prescriptive because the speed with which technology is evolving could make specific requirements obsolete and deter technological progress. HHS responded by stating that standards should be defined in generic terms and should be scalable, flexible, and generally addressable through various approaches or technologies. The result is that the final rule offers more high-level guidance, providing

what is essentially a model for information security, with less specific guidance on how to implement the model. HHS has promised more specifics in future guidance documents, but has left the rule "focused more on what needs to be done and less on how it should be accomplished."

In keeping with this results-based approach, the rule has heightened emphasis on internal risk analysis and risk management as the core elements of the security management process. In addition, cost of security measures has been included as a significant factor to be considered in security decisions. This emphasis will be of particular benefit to small and rural providers, but comes with a significant caution; HHS makes clear in the preamble that cost factors may not be used to free covered entities from the responsibility of implementing adequate security.

Further evidence of the transition toward a broader, management-based rule is seen in HHS' approach to implementation specifications. The majority of the Security standards incorporate implementation specifications, to better describe the actions that should be taken to ensure compliance with the standards. Only 13 of these implementation specifications are required; the majority of the specifications are termed "addressable." Addressable specifications represent approaches to meeting specific standards, any of which may not be relevant to the covered entity's environment. For example, the Rule requires training on security issues for the workforce, but identifies training in password management as an "addressable" specification. In an environment where biometric technology is used to control system access, password training would be irrelevant, and not required.

The decision about the reasonable and appropriate nature of an addressable specification rests on the covered entity and is based on its overall technical environment and security framework. This decision may rely on a variety of factors, including the results of a risk analysis, measures already in place, and the cost of implementing new measures. Based on the results of this decision process, the covered entity may choose one of three options:

1. implement the specification;
2. implement an alternative security measure to accomplish the purposes of the standard; or
3. not implement anything if the specification is not reasonable and appropriate AND the standard can still be met.

General Rule Provisions

Section 164.306, the statement of the general Rule, requires covered entities to:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information (EPHI) the covered entity creates, receives, maintains, or transmits;
- 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 by the Privacy Rule; and
- Ensure compliance by its workforce.

The balance of Section 164.306 expands upon the relationships, as summarized above, between these essential standards and addressable and required implementation specifications.

The remainder of the final Security Rule contains the standards and specifications required to implement the general rule.

Administrative Safeguards

Reinforcing the Security Rule's central focus on security management, the detailed sections of the rule begin with Section 164.308, Administrative Safeguards. Section 164.308 focuses on the security management process - the policies and procedures designed to prevent, detect, contain, and correct security violations. This standard contains four required implementation specifications: risk analysis,

risk management, sanction policy, and information system activity review. The requirement to assign security responsibility has been moved to this section from Physical Security (where it resided in the draft rule); the preamble now clarifies that a single individual must bear this responsibility. This section also includes:

- Several workforce security provisions, including addressable specifications for authorization and/or supervision, workforce clearance procedures, and termination procedures.
- Clarification of requirements and restrictions on the workforce and other users of EPHI by requiring information access management controls, including addressable standards for access authorization, establishment and modification.
- The required specification that clearinghouses that are part of larger organizations must implement policies and procedures to protect the clearinghouse's EPHI from unauthorized access by the larger organization.
- Security training and awareness requirements for the workforce, including addressable specifications to address security reminders, malicious software procedures, user monitoring of log-in attempts, and password management.
- Two additional standards which focus on the organization's planning and response to undesired events. They are:
    1. A requirement for policies and procedures that address security incidents, including the required specification, response and reporting. This specification calls for covered entities to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes, and
    2. A requirement that covered entities protect the availability of EPHI by establishing a contingency plan. Required implementation specifications for the contingency plan include the presence of a data backup plan, a disaster recovery plan, and an emergency mode operation plan. Testing and revision procedures and applications and data criticality analysis are included as addressable specifications.
- Periodic technical and non-technical evaluation of the organization's compliance with the Security rule. The term "evaluation" in the final rule replaces "certification" required in the draft Security Rule. HHS responded to criticisms of this original requirement by replacing it with a mandate to "periodically conduct an evaluation...to demonstrate and document...compliance with the entity's security policy and the [Security Rule] requirements. Covered entities must assess the need for a new evaluation based on changes to their security environment since their last evaluation."
- Language permitting the use of business associates to create, receive, maintain, or transmit EPHI on the covered entity's behalf with the appropriate contractual language described later in the Rule.

Physical Safeguards

Like the draft rule, Section 164.310 of the final Rule requires Physical Safeguards to protect EPHI from unauthorized disclosure, modification, or destruction. This section includes standards for:

- Facility access controls, with addressable specifications that clarify that the standard applies to both normal and contingency operations. They further provide for access control and validation procedures (staff and visitors) and for the collection of appropriate maintenance records for the physical components of a facility that are related to security (such as hardware, walls, doors, and locks).
- Standards for proper workstation use and physical security of workstations that access EPHI.
- Standards for device and media controls -- policies and procedures that control receipt, movement, and removal of hardware and electronic media that contain EPHI. Required

elements include disposal policies and procedures to address the final disposition of EPHI, and/or the hardware or electronic media on which it is stored, and media re-use procedures to remove EPHI before the reuse of media. Addressable aspects of this standard include accountability (a record of the movements of hardware and electronic media and any person responsible), and data backup and storage.

Technical Safeguards

Section 164.312, Technical Safeguards, contains provisions extracted from two sections of the proposed rule: Technical Security Services and Technical Security Mechanisms. Covered entities must implement:

- Technical policies and procedures for access control on systems that maintain EPHI. These systems must allow for unique user identification and include an emergency access procedure for obtaining necessary EPHI during an emergency. Addressable specifications include automatic logoff and encryption and decryption, which is defined as a mechanism to encrypt and decrypt EPHI.

- Transmission security, including two addressable specifications:

    1. Integrity controls -- security measures to ensure that electronically-transmitted PHI is not improperly modified without detection until disposed of, and

    2. Encryption. Designation of encryption as an addressable specification is a key departure from the proposed rule, which explicitly required encryption when using open networks. Covered entities now must determine how to protect EPHI "in a manner commensurate with the associated risk." Covered entities are encouraged in the Rule's preamble to consider use of encryption technology for transmitting EPHI, particularly over the Internet. The key reasons cited by HHS for this change are the cost burden for small providers and the current lack of a simple and interoperable solution for email encryption.

- Hardware, software, and/or procedural methods for providing audit controls.

- Policies and procedures to protect EPHI from improper alteration or destruction to ensure data integrity. This integrity standard is coupled with one addressable implementation specification for a mechanism to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.

- Person or entity authentication, which requires the covered entity to implement procedures that verify that a person or entity seeking access to EPHI is the one claimed to be doing so.

Business Associate Contracts

The proposed Security Rule required a "chain of trust partner agreement" between parties exchanging data electronically. In keeping with the goal of aligning Privacy and Security requirements, Section 164.314 of the final Security Rule requires a Business Associate agreement, which is already required by the Privacy Rule. For relationships where a third party is used to create, receive, maintain or transmit EPHI on the covered entity's behalf, the Security Rule requires the business associate to:

- Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the covered entity's EPHI;

- Ensure that its agents and subcontractors to whom it provides EPHI meet the same standard;

- Report to the covered entity any security incident of which it becomes aware; and

- Ensure that the contract authorizes termination if the business associate has violated a material term.

The Security Rule adopts the Privacy Rule's exceptions to the agreement requirement for disclosures

to providers for treatment, exchanges of information between government entities, and exchanges between group health plans and their sponsors. However, it does not adopt the Privacy Rule's exception for covered entities participating in an organized health care arrangement (OHCA). It is not clear if this is a deliberate or inadvertent omission.

This section also applies the Security Rule provisions to affiliated entities, hybrid entities and group health plans, again increasing the new Rule's compatibility with Privacy Rule provisions for these entities.

Policies, Procedures and Documentation

Section 164.316 requires covered entities to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule. A covered entity may change its policies and procedures at any time. The section also requires covered entities to maintain the policies and procedures and any other required action, activity or assessment in written form (which may be electronic). Three required implementation specifications complete this standard, requiring that the covered entity must:

1. Maintain the documentation for six years from the date of its creation or the date when it last was in effect, whichever
   is later;

2. Make the documentation available to those persons responsible for implementing the procedures to which the documentation pertains; and

3. Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

The Bottom Line

The final Security Rule is, overall, a welcome revision to the proposed provisions. It clearly outlines a realistic model for security management that is broadly flexible across the healthcare industry. However, covered entities should not take the flexibility provisions of the rule as a reason to ignore the technological side of security. HHS has clearly stated its position that this flexibility does not extend to non-compliance; appropriate technical measures will be needed to implement many of the Rule's provisions. The standard requiring periodic evaluation stresses that technical measures must be included part of the mandated evaluation.

A further caution: covered entities would be wise not to underestimate the effort involved in complying with the improved Security requirements, or their liability for security results or lack thereof. The new Rule replaces a relatively "black and white" menu of specified actions with results-based expectations requiring enterprise-wide vigilance and judicious decisions about security through constantly changing circumstances. Implementation of a security management methodology where none has previously existed is a significant process that may require a period of one to two years to conceptualize and implement, followed by continuous monitoring and indefinite updating. Further, each covered entity's security program will be subject to federal scrutiny of the entity's well-documented rationale.

The first step in implementing the final Security Rule is to become familiar with each of its provisions, as written in the official text. **Begin now.**

Tom Grove, Vice President, Phoenix Health Systems, has extensive experience managing HIPAA security and privacy projects for both for large, multi-entity healthcare systems and smaller provider organizations. Tom has published numerous papers on HIPAA compliance, has testified on HIPAA issues at NCVHS hearings, and is a frequent speaker at industry conferences. Tom is a senior member of Phoenix Health Systems' HIPAA Solutions Team. www.phoenixhealth.com

Go to TOP
