



## **HHS Issues Final HIPAA Security Rule**

On February 20, 2003, the U.S. Department of Health and Human Services (“HHS”) issued a final version of the HIPAA Security Rule. A proposed version of the Security Rule (the “Proposed Rule”) was published four and a half years ago. While much of the substance of the Proposed Rule remains, the Security Rule has been reorganized for clarification purposes and has been made more compatible with the HIPAA Privacy Rule. The Security Rule has also been revised to provide covered entities with important compliance flexibility in certain areas. Most covered entities will have to come into compliance with the Security Rule by April 20, 2005.

### **Required vs. Addressable Implementation Specifications**

The Security Rule is organized around general “standards,” many of which are divided into more detailed “implementation specifications.” Compliance with all of the standards is mandated. However, the Security Rule draws a distinction between “required” and “addressable” implementation specifications. While covered entities must comply with all required specifications, with respect to addressable specifications, covered entities may:

- Assess whether the specification is reasonable and appropriate given the environment in which the entity is operating;
- If deemed to be reasonable and appropriate, implement the specification;
- If deemed not to be reasonable and appropriate, document the reasons for this determination and implement an equivalent, alternative security measures if that is deemed reasonable and appropriate.

HHS has made certain implementation specifications addressable to provide health care organizations (especially smaller ones) with an opportunity to forego compliance with security obligations that may not be justified from a cost-benefit standpoint. However, it is critical that any determination by a covered entity to adopt an alternative security measure or no measure at all be based on a thorough risk assessment that is adequately documented.

Among the most notable Security Rule provisions that is now “addressable” is the obligation to encrypt protected health information transmitted over open networks. Other

addressable specifications include employee access authorization procedures, security reminders, virus protection, log-in monitoring, password management policies and testing/revision of contingency plans.

### **Integration of “Technical Security Services” and “Technical Security Mechanisms”**

Like the Proposed Rule, the Security Rule contains distinct sections covering administrative safeguards and physical safeguards. However, the Proposed Rule included separate technical requirements for data being stored in a covered entity’s information system (referred to as “technical security services”) and data being transmitted by a covered entity to an outside party (referred to as “technical security mechanisms”). The Security Rule eliminates this distinction and creates a single set of technical safeguard requirements that apply to all electronic protected health information, whether at rest or in motion. The technical safeguards mandated by the Security Rule, which include many but not all of the requirements in the Proposed Rule, include access controls, audit controls, integrity controls, person/entity authentication and transmission security.

### **Coordination of “Chain of Trust” and “Business Associate” Requirements**

Since the issuance of the final HIPAA Privacy Rule, there has been much confusion regarding the interplay between the Privacy Rule’s business associate contract requirements and the obligation under the Proposed Rule to enter into “chain of trust” agreements with parties receiving electronic protected health information. The Security Rule eliminates this confusion by folding the chain of trust requirement into the Privacy Rule’s business associate obligation. As a result, covered entities are not required to enter into contracts under the Security Rule with any entities other than those that qualify as business associates under the Privacy Rule. Business associate agreements, however, must incorporate language regarding electronic data to comply with the Security Rule. Although the Security Rule’s compliance date is in April 2005, to preclude the need for subsequent amendments, covered entities may wish to ensure that the business associate agreements being executed to comply with the Privacy Rule’s April 14, 2003 deadline also satisfy the requirements of the Security Rule.

### **Replacement of Certification Requirement with Evaluation Obligation**

The Proposed Rule contained an ambiguous provision obligating covered entities to “certify” their compliance. This provision has been deleted in the Security Rule. It appears to have been replaced, at least in part, by an “evaluation” standard under which covered entities must “perform a periodic technical and non-technical evaluation” to ensure that they remain in compliance with the Security Rule despite environmental or operational changes.

### **Elimination of “System Configuration” and “Formal Mechanism for Processing Records”**

The Security Rule eliminates the requirement in the Proposed Rule that covered entities adopt policies governing system configuration and a formal mechanism for processing records. These provisions were deemed by HHS to be either unnecessary or redundant.

## **Obligation to Appoint Single Security Official**

The Proposed Rule required covered entities to assign security responsibility but did not specify whether such responsibility had to be vested in an individual as opposed to a committee of other group. The Security Rule eliminates this ambiguity by expressly requiring the appointment of a single security official to oversee compliance.

## **Clearer Definition of “Electronic Protected Health Information”**

To ensure compliance with the Privacy Rule, the Security Rule adopts the same definition of protected health information. However, unlike the Privacy Rule, the Security Rule applies only to “electronic protected health information,” which is protected health information maintained in or transmitted by “electronic media.”

The Security Rule contains a more detailed definition of “electronic media,” which should eliminate some of the confusion as to whether certain modes of transmission are covered by the Security Rule. Among other things, this definition states explicitly that fax and telephone transmissions do not constitute electronic media for purposes of the Security Rule. However, telephone voice response and faxback systems are considered electronic media because they are input and output devices for computers.

## **Guidance on “Scalability” Determinations**

The Proposed Rule emphasized that its obligations were “scalable,” i.e., that they were designed in a flexible manner to permit covered entities of varying sizes to develop reasonable, individually tailored approaches to compliance. The Security Rule expands on the notion of scalability by providing explicit guidance regarding the factors that a covered entity may take into account when selecting particular security measures. The factors include the following:

- The size, complexity and capabilities of the covered entity;
- The covered entity’s technical infrastructure, hardware and software capabilities;
- The cost of security measures; and
- The probability and criticality of potential risks.

It would be prudent for covered entities to consider these factors when making decisions about the reasonableness of particular security measures. Covered entities should also make reference to these factors when documenting their Security Rule compliance determinations.

## **Importance of Risk Analysis**

Risk analysis is given greater prominence in the Security Rule than in the Proposed Rule. As indicated above, a covered entity may elect not to comply with an addressable implementation specification only if this decision is supported by a risk analysis. Indeed, the preamble to the Security Rule states that risk analysis and risk management “forms the foundation on which all of the other standards depend.”

## **Compliance Matrix**

The Security Rule contains a helpful appendix that summarizes the requirements in a matrix form. The matrix is divided into three sections, covering administrative, physical and technical safeguards, respectively. Within each section, the relevant standards are delineated. Next to each standard, any implementation specifications are listed, with a notation as to whether they are required or addressable. The full text of the Security Rule as well as the matrix may be found at 68 Fed. Reg. 8334 (February 20, 2003).

*This material was prepared by Robert Belfort of the law firm of Manatt, Phelps & Phillips, LLP. This material is provided for informational purposes only and should not be construed as legal advice on any subject matter. Any information contained herein is not intended to be a substitute for legal counsel.*