CLIENT ALERT

HHS Issues New HIPAA Security Rule

Feb.23.2003

On Thursday, February 20, 2003, the Secretary of the U.S. Department of Health and Human Services ("HHS") published in the Federal Register final security standards ("Security Rule") under the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191 ("HIPAA").

The Security Rule is designed to supplement existing HIPAA administrative simplification regulations previously issued by HHS, including the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"). The Security Rule applies to the same "covered entities" to which the Privacy Rule applies, namely health plans, health care clearinghouses, and health care providers who transmit HIPAA-covered transactions in electronic form. Most covered entities must be fully compliant with the Security Rule by April 21, 2005.

Framework

The Security Rule adopts "national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information" ("PHI").[1] It is intended to "address all aspects of the security of electronic health information while it is being stored or during the exchange of that information between entities."

The Security Rule sets forth security "standards" and corresponding "implementation specifications" addressing the following areas:

Administrative Safeguards

- Implementation of a security management process that includes risk analysis, risk management, internal sanctions, and information system activity reviews;
- Assignment of security responsibilities to a designated official;
- Implementation of workforce security measures, including authorization and/or supervision of workforce members who work with electronic PHI, clearance procedures, and termination procedures;
- Information access management, including isolation of health care clearinghouse functions (if any), access authorization, and access establishment and modification;
- Security awareness and training, including issuance of periodic security reminders, measures to protect against malicious software, log-in monitoring, and password management;
- Implementation of security incident procedures, including response to, and reporting of, such incidents;
- Contingency planning, including planning for data backup, disaster recovery, and emergency mode operation, as well as testing and revision of such plans, and analysis of applications and data criticality;
- Periodic security evaluation; and
- Business associate contracts, including written contracts or other arrangements.

Physical Safeguards

- Facility access controls, including contingency operations, facility security plans, access control and validation procedures, and maintenance records;
- Workstation use;
- Workstation security; and
- Device and media controls, including disposal of electronic PHI, media re-use, accountability, and data backup and storage.

Technical Safeguards

- Access control, including unique user identification, emergency access procedures, automatic logoff procedures, and encryption/decryption;
- Audit controls;
- Protection of the integrity of electronic PHI, including authentication mechanisms;
- Verification of identity of persons or entities seeking access to electronic PHI; and
- Transmission security, including integrity controls and encryption of electronically transmitted PHI.

The Security Rule has been written "to frame the standards in terms that are as generic as possible and which, generally speaking, may be met through various approaches or technologies." As HHS acknowledges in the Rule's Preamble, "the entities affected by this regulation are so varied in terms of . . . technology, size, resources, and relative risk, that it would be impossible to dictate a specific solution or set of solutions that would be useable by all covered entities."

As a result, the steps that a covered entity must actually take to comply with the Security Rule will depend on its own unique environment, circumstances, and risk assessment. In evaluating what steps to take, a covered entity may balance the "risks and vulnerabilities" associated with the information it handles against the "cost of various protective measures."

Overlap with Privacy Rule

HHS emphasizes that the Security Rule and the Privacy Rule are "inextricably linked." To this end, the Security Rule has been designed to incorporate some of the same concepts and terminology that appear in the Privacy Rule. The Security Rule, for example, sets forth security-specific provisions that must be addressed in "business associate" agreements and group health plan/plan sponsor relationships, and adopts the concepts of "hybrid entities" and "affiliated covered entities" first introduced in the Privacy Rule.

Despite these similarities, the focus of the two rules differs slightly. The Privacy Rule addresses how PHI should be controlled by setting forth what uses and disclosures are authorized or required and what rights patients have with respect to their health information. The Security Rule, on the other hand, implements safeguards to protect electronic PHI from unauthorized access, alteration, deletion, and transmission. It is important to emphasize that the Security Rule covers only electronic PHI, not PHI held in paper records.

Changes from 1998 Proposed Rule

The Security Rule contains several key differences from the security standards originally proposed by HHS in 1998. See 63 Fed. Reg. 43242 (Aug. 12, 1998). For example, the Security Rule introduces the concept of the "addressable" implementation specification (AIS). Unlike a "required" implementation specification, an AIS need not be implemented if it is not reasonable and appropriate for the covered entity to do so. Rather, a covered entity has the option of implementing an alternative means of satisfying a security standard so long as the covered entity has assessed the reasonability and appropriateness of the AIS, and documented why it has chosen to implement an equivalent alternative measure.

The Security Rule also abandons a number of proposed requirements that were either duplicative, unnecessary, or required adjustment in light of other existing HIPAA regulations. For example, the concept of a "chain of trust" agreement has been dropped in favor of adopting the Privacy Rule's concept of a "business associate" agreement. Similarly, the proposed requirement for a "formal mechanism for processing records" has been abandoned as "ambiguous" and "unnecessary."

By the same token, the Security Rule expands on proposed requirements in at least some respects. For example, the Security Rule adds a required implementation specification addressing the removal of electronic PHI from electronic media before such media are made available for re-use.

Timeframe for Compliance

Absent intervention by Congress, the Security Rule will become effective on April 21, 2003. Most health care entities covered under the Rule will then have two years to come into compliance before HHS is authorized enforce the Rule as of April 21, 2005. Small health plans have an additional year to comply.

[1] This quote and subsequent quotes included in this summary are from the Security Rule, published at 68 Fed. Reg. 8334 (Feb. 20, 2003).

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Barbara H. Ryland
Senior Counsel – Washington, D.C.
Phone: +1 202.624.2970
Email: bryland@crowell.com