

BOSTON
WASHINGTON
NEW YORK
RESTON
NEW HAVEN
LOS ANGELES
LONDON

www.mintz.com

If you would like further information on these or any health law issues, please contact one of our health law attorneys.

Linda D. Bentley617 348 1784
Susan W. Berson202 661 8715/212 692 6750
Raymond D. Cotton202 434 7322
Thomas S. Crane617 348 1676/202 661 8787
Stephen C. Curley212 692 6217
Deborah A. Daccord617 348 4716
Hope S. Foster202 661 8758
Marie C. Infante202 434 7489
Ellen L. Janos617 348 1662
Peter M. Kazon202 661 8739
Carolyn J. McElroy202 434 7408
M. Daria Niewenhous617 348 4865
Stephen M. Weiner617 348 1757
Richard J. Zall212 692 6844
Michael D. Bell202 434 7481
Theresa C. Carnegie202 661 8710
Io C. Cyrus617 348 4777
Erin Lewis Darling202 434 7478
Karen S. Lovitch202 434 7324
Nell M. Ma'luf617 348 4496
Diana Puknys Schad202 434 7328
Heather L. Westphal202 585 3538
Jennifer E. Williams202 585 3542

Advisory

June 2, 2003

HEALTH LAW

New Final HIPAA Regulations Emphasize Flexibility

With the recent publication of its rule on Security Standards and the first installment of its enforcement procedures, the United States Department of Health and Human Services (HHS) continues its implementation of the Administrative Simplification requirements of the Health Insurance Portability and Accountability Act of 1996 or HIPAA.

The federal Privacy Rule, which governs the use and disclosure of Protected Health Information (PHI), has received the most attention among the HIPAA requirements. However, in addition to the Privacy Rule, which had a compliance date of April 14, 2003, HIPAA also mandated the adoption of standards for certain basic transactions that are done electronically, a requirement that will become effective on October 16, 2003. The final Security Standards and the Enforcement Rule are additional pieces to the HIPAA puzzle. These new rules make clear, as HHS stated in the recent enforcement rule, that “the duty to comply with certain of the HIPAA rules is now a reality for many, if not most, covered entities.”

The Security Standards and the Privacy Rule

The Security Standards were released this winter with little fanfare, four and one-half years after the proposed rule was first published. Like the Privacy Rule, the Security Standards will require covered entities to conduct an internal review and gap analysis and implement remedial measures to ensure compliance with the regulatory requirements. The good news is that HHS, both in the preamble to the regulations and in security-related teleconferences, has stressed that the requirements are “scalable” and that implementation should be reasonable under the given circumstances.

The Security Standards are designed to protect the integrity, confidentiality, and availability of electronic PHI and are “inextricably linked” to the Privacy Rule. However, the scope of Security Standards differs from that of the Privacy Rule. Specifically, in contrast to the Privacy Rule, which governs *all forms* of PHI, the Security Standards regulate only PHI that is maintained or transmitted using *electronic media* such as computers and computer networks, optical and magnetic storage, and the Internet. Thus, according to the preamble, a paper fax sent using a standard fax machine would not be electronic PHI, but the same information scanned and faxed using computer software would be.

Overview of the Security Standards

The Security Standards are predicated on three basic principles: (i) comprehensiveness; (ii) scalability; and (iii) technical neutrality. With respect to comprehensiveness, the Security Standards are intended to address and coordinate all aspects of security and require the implementation of administrative, physical, and technical safeguards. The specific standards contained in these broad categories (a total of 18) range from the designation of assigned security responsibility (*e.g.*, a Security Officer) to “visitor control” to encryption. Thus, despite common perceptions, the Security Standards reach well beyond a covered entity’s computers and telecommunications equipment.

Perhaps most significant to covered entities is the principle of scalability. Similar to the reasonableness standard that permeates the Privacy Rule, the concept of scalability

allows a covered entity to implement security safeguards that are appropriate to its specific needs, identified security risks and vulnerabilities, and the environment. Indeed, the subsection of the regulations entitled, "Flexibility of approach," provides that covered entities may "reasonably and appropriately" implement the regulatory requirements. When deciding which security measures to use, an entity must take into account the following factors: (i) the size, complexity, and capabilities of the covered entity; (ii) the covered entity's technical infrastructure, hardware, and software security capabilities; (iii) the costs of security measures; and (iv) the probability and criticality of potential risks to electronic PHI. Consequently, what is required for a small physician practice will differ significantly from what is needed for a large, national insurance organization.

This scalability concept is further reflected in HHS's approach to implementation of the specific standards themselves. Unlike the proposed rule, in order to promote flexibility HHS adopted both "required" and "addressable" implementation specifications. When a standard includes *required* implementation specifications, a covered entity must implement the specification as written. However, when a standard is *addressable*, a covered entity must "[a]ssess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information." The entity then must implement the specification or, if implementation is not reasonable and appropriate, document its rationale for not doing so. In this regard, HHS provides: "[o]ur decision to classify many implementation specifications as addressable, rather than mandatory, provides even more flexibility to covered entities to develop cost effective solutions."

The third tenet on which the Security Standards are based involves technical neutrality. The Security Standards do not require or otherwise promote any one technological solution over another. Nor does HHS prescribe minimum requirements for the technology employed. For example, when asked to establish a specific or minimum standard for encryption, an addressable implementation specification, HHS explained that "rapidly changing technology makes it impractical and inappropriate to name a specific technology."

In summary, while the Security Standards will require covered entities to engage in an exercise similar to that performed for privacy compliance, the requirements have been streamlined, and covered entities are afforded the flexibility to implement security safeguards that are appropriate for the organization.

First Installment of HIPAA Enforcement Rules

The theme of flexibility and cooperation was also reflected in the more recent Civil Money Penalties regulation that was issued on April 17, 2003. Under the HIPAA statute, HHS can impose civil money penalties for violations of its provisions. The penalties are up to \$100 per violation, up to a maximum of \$25,000 for violations of the same requirement. The rule sets procedures by which HHS may impose penalties upon covered entities who violate the regulations and standards adopted under HIPAA's Administrative Simplification provisions (*e.g.*, the Privacy Rule, Security Standards, Transaction and Code Set Standards). The procedures that HHS would follow in seeking such penalties will closely track the procedures used by the Office of Inspector General when it seeks civil money penalties for violations of the fraud and abuse laws.

The Office of Civil Rights (OCR) will administer and enforce the Privacy Rule, while the Centers for Medicare & Medicaid Services (CMS) will administer and enforce the remaining HIPAA rules. Both OCR and CMS intend to approach enforcement issues by seeking voluntary compliance from covered entities, and by providing technical assistance to aid in compliance efforts. Although the rule is an interim final rule, comments may be filed until June 16, 2003.

HHS states that this new set of rules is only the first installment of what it expects will be an "Enforcement Rule," which will eventually set out all of the procedural and substantive requirements related to the imposition of civil money penalties. The most significant thing about the current regulation, however, is HHS's restrained approach to the imposition of penalties. The regulation emphasizes that HHS intends to seek voluntary compliance with the rules and that it will seek to issue guidance and technical assistance to help covered entities comply with the Privacy Rule and other HIPAA standards. To the extent that issues arise, HHS states it will seek to resolve them by informal means before taking more serious actions. The primary driver of enforcement activities will be complaints received by the Department. To the extent complaints reveal problems that entities need to address, the rule states that entities will be given opportunities to demonstrate compliance and to submit a corrective action plan.

Thus, HHS appears to acknowledge the significant change in health care operations being brought about by HIPAA, and seems to be going out of its way to signal that it will be reasonable in enforcing the new requirements, and in seeking penalties for noncompliance.

* * * * *