Health Law @ manatt

August 26, 2009

HHS Issues Breach Notification Regulations Under HITECH

Robert D. Belfort
Karyn E.B. Bell

On August 24, 2009, the U.S. Department of Health and Human Services ("HHS") published interim final regulations (the "Regulations") implementing the security breach notification provisions of the Health Information Technology for Economic and Clinical Health Act ("HITECH"). The Regulations become effective September 23, 2009. HHS has indicated, however, that it will not impose penalties based on violations of the Regulations prior to February 22, 2010.

The Regulations largely mirror those provisions of HITECH specifying who must be notified in the event of a security breach involving unsecured protected health information ("PHI"), the content of the notice and the timing of notification. HIPAA covered entities must provide notice of breaches to affected individuals, to the Secretary of HHS and, if there are more than 500 affected individuals in a particular state, to prominent media outlets. Notice must be provided without unreasonable delay but in no event more than 60 days after discovery, subject to temporary delays if requested by law enforcement officials. Business associates must notify covered entities of breaches involving the business associate's use or disclosure of unsecured PHI. Covered entities must generally provide written notice to the individual by mail but may send notice by e-mail if the individual has agreed to receive communications in this manner. Alternative notification methods are permitted if the covered entity lacks contact information for some or all of the affected individuals.

While the Regulations primarily reiterate obligations set forth in HITECH or clarify minor statutory ambiguities, several provisions of the Regulations go beyond the language of the statute and define new substantive standards for breach notification. Several of these provisions significantly increase the flexibility of covered entities and their business associates in determining

Newsletter Editors

Helen Pfister
Partner
hpfister@manatt.com
212.830.7277

Our Practice

The Healthcare professionals at Manatt represent major Healthcare companies in a broad range of regulatory, litigation, and transactional work. Our attorneys have successfully represented clients in investment matters, litigation, ...more

Practice Group Overview
Practice Group Members

Info & Resources

Subscribe
Unsubscribe
Newsletter Disclaimer
Manatt.com

whether a breach requiring notification has occurred. These key provisions of the Regulations include the following:

Application of "Harm Threshold" to Determination of Breach
The Regulations define a "breach" as the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule that "compromises the security or privacy" of the PHI. A use or disclosure compromises privacy or security only if it creates "a significant risk of financial, reputation, or other harm to the individual." In order to determine whether the harm threshold has been met, covered entities and business associates must perform and document a fact-specific risk assessment that takes into account, among other things, the following factors: (1) the person or entity to whom the information was impermissibly disclosed; (2) whether immediate mitigating steps eliminated or reduced the risk of harm to the individual and (3) the nature and amount of PHI involved in the impermissible use or disclosure. The establishment of a harm threshold relieves covered entities and business associates of the obligation to issue notices for the many improper disclosures that pose little or no risk of harm to individuals. However, the Regulations impose a new duty on organizations to conduct and document formal risk assessments in connection with each improper use or disclosure.

Exception for Disclosures Involving Limited Data Sets That do not Contain Zip Codes or Birth Dates
The Regulations provide that an improper use or disclosure does not compromise privacy or security if the unsecured PHI is a limited data set (that does not contain the 16 direct identifiers specified in the HIPAA Privacy Rule) and excludes both birth dates and zip code information. As a result, improper uses or disclosures of such data sets do not trigger breach notification obligations.

Expansion of "Same Facility" Exception
HITECH excludes from the definition of a "breach" disclosures by one authorized person to another authorized person working at the same "facility." The Regulations interpret the term "facility" to mean any covered entity, business associate or organized health care arrangement. This broadens the exception to include inadvertent, improper exchanges of data within an entire organization, without regard to whether the individuals involved in the exchange work at the same physical facility.

Harmonization of FTC and HHS Requirements
HITECH imposes similar breach notification obligations on vendors of personal health records ("PHRs"), which are enforced by the Federal Trade Commission ("FTC"). HHS notes that covered entities and business associates are subject to HHS and not FTC breach notification rules, but also acknowledges that there are limited cases where an entity may be subject to both HHS and FTC requirements. For example, a company may maintain a

PHR as a business associate on behalf of covered entities but also offer a PHR directly to consumers in its capacity as a PHR vendor. To minimize confusion, HHS and FTC have worked to harmonize their rules. For example, entities subject to the FTC breach notification rules must rely on the HHS guidance to determine whether information subject to a breach was "unsecured." HHS also notes that the FTC will deem compliance with certain provisions of the Regulations as compliance with the FTC's rule.

Rejection of Expanded Mechanisms for Deeming PHI Secured

Unsecured PHI means "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance published on the HHS website." On April 17, 2009, HHS issued guidance specifying the encryption and other methods that may be used to secure PHI and eliminate the obligation to provide notice in the event of a breach. The Regulations reject several proposals for expanding the range of these methods and basically adhere to the April 17th guidance with minor clarifications.

Limited Preemption of State Breach Notification Laws

Most states have adopted their own breach notification laws that potentially overlap with HITECH. These state laws will be preempted by HITECH only if it is impossible to comply with both the state law and HITECH or the state law stands as an obstacle to the accomplishment and execution of HITECH's full purposes and objectives. HHS believes that few such conflicts exist. HHS further notes that a single notification can generally be used to satisfy the requirements of both state breach notification laws and the Regulations.

To ensure compliance with the Regulations, covered entities and business associates should update business associate agreements to reflect the requirements of HITECH and the Regulations, adopt policies and procedures for breach notification and conduct training programs for their employees and agents. In addition, organizations that want to submit comments on the Regulations may do so on or before October 23, 2009.

back to top

For additional information on this issue, contact:

Robert D. Belfort Mr. Belfort has extensive experience representing healthcare organizations on regulatory compliance and transactional matters. His clients include hospitals, community health centers, mental health providers, pharmacy chains, health insurers, IPAs, pharmaceutical manufacturers, pharmacy benefit managers, information

technology vendors and a variety of other businesses in the healthcare industry.

Karyn E.B. Bell Ms. Bell's practice focuses on a wide range of healthcare issues, including Medicare fraud and compliance, Medicare and Medicaid reimbursement and coverage, compliance for federally qualified health centers, and corporate and transactional matters.