

DHHS Issues Breach Notification Requirements

As part of the American Recovery and Reinvestment Act of 2009 signed by President Obama in February, the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") requires covered entities to report to individuals security breaches of their protected health information ("PHI"). Before the HITECH Act, HIPAA covered entities were not required to notify individuals regarding security breaches of their PHI, although some may have done so voluntarily as part of their mitigation efforts. Covered entities, business associates, and personal health record vendors will now be required to report breaches of "unsecured PHI" (defined below) to individuals (or in the case of business associates, to the relevant covered entity) whose PHI has been used or disclosed in violation of the HIPAA rules.

As required by the HITECH Act, on August 24, 2009, the Department of Health and Human Services ("DHHS") published an interim final rule implementing the breach notification requirements. Compliance is required by September 23, 2009, but DHHS has stated that the Office of Civil Rights ("OCR") will use its "enforcement discretion" and not impose sanctions for failing to provide notice for breaches that are discovered for six months from August 24. In particular, during the time after the rule has taken effect but before DHHS imposes sanctions, DHHS expects covered entities to comply with the regulations and will work with covered entities, through technical assistance and voluntary corrective action, to achieve compliance. The interim final regulations generally reiterate the HITECH statutory requirements and clarify several of these requirements.

Breach

With certain exceptions, "breach" means the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of such information, except where an

unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. "Compromises the security and privacy" of PHI means "poses a significant risk of financial, reputational, or other harm to the individual." This means that not all impermissible uses or disclosures of PHI need to be reported. Instead, covered entities and business associates must perform a risk assessment to determine whether there is significant risk of harm to the individual as a result of the impermissible use or disclosure. The preamble to the final interim regulations lists a number of factors, as well as some examples of potentially reportable and nonreportable breaches, to be considered in making potential of harm assessments.¹ This required risk analysis process will need to be conducted quickly, and covered entities and their business associates will need to develop policies and procedures for conducting and documenting these analyses.

¹ For examples of such factors and reportable and nonreportable breaches, see <http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf> at pages 42744 - 45.

Unsecured PHI

Under breach regulations, “unsecured” PHI means PHI in any form 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 issued by the Secretary of DHHS. This means that PHI may be “secured” only by using one of the methods described in such Guidance: *encryption* and *destruction*. Encryption means that the “[e]lectronic PHI has been encrypted as specified in the HIPAA Security Rule by ‘the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key’ and such confidential process or key that might enable decryption has not been breached.” The decryption tools or key must be kept separately from the data that they encrypt or decrypt. The Guidance lists two sources describing encryption processes that meet DHHS’ requirements.

“Destruction” means that the “media on which the PHI is stored or recorded has been destroyed in one of the following ways:

- Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise reconstructed. Redaction is specifically excluded as a means of data destruction;
- Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.”

To the extent PHI has been secured (encrypted or destroyed) as described in the Guidance issued by DHHS, covered entities will not have to notify individuals of any breach of such information.

Reporting Timeframe

As of September 23, 2009, covered entities will be required to report to individuals any breaches of unsecured PHI. covered entities are required to report such breaches to individuals without unreasonable delay after discovery (as defined by the HITECH Act and the regulations) of the breach. Except under very limited circumstances, notifications must be made no later than 60 calendar days after discovery of the breach.

Method of Notice

Under the HITECH Act, the notice must be:

- In writing to the last known address of the individual via first class mail (or via e-mail if specified by the individual);
- By substitute notice where the contact information is insufficient or out-of-date, including where there are 10 or more individuals with insufficient information, conspicuous posting on the home page of the website of the covered entity (for 90 days), or in major print or broadcast media for a period determined by the Secretary;
- By telephone or other method where there is a possibility of imminent misuse, in addition to written notice;
- To prominent media outlets within the jurisdiction if the breach is reasonably believed to affect more than 500 residents of that jurisdiction;
- To the Secretary for breaches involving more than 500 individuals and annually for all other breaches; and
- By the Secretary posting on the DHHS website of a list that identifies each covered entity involved in a breach in which the unsecured PHI of more than 500 individuals is acquired or disclosed.

Content of Notification

The HITECH Act and the implementing regulations require breach notifications to include certain information. Among other items, the notification must include a brief description of what happened, including the date of the breach and the date of the discovery, if known; the types of unsecured PHI that were involved in the breach (e.g., social security numbers, addresses, diagnosis codes); steps individuals should take to protect themselves from potential harm resulting from the breach; and a brief description of what the covered entity is doing to investigate the breach, mitigate losses, and protect against any further breaches. The notification also must include contact procedures for individuals to ask questions or obtain additional information, which must include a toll-free telephone number, an email address, a web site, or postal address.

Breach by Business Associates

In the event a business associate discovers a breach of unsecured PHI, the business associate must notify the covered entity of such breach. The business associate must notify the covered entity of the breach without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. To the extent a business associate is considered an agent under federal common law, the business associate's discovery of the breach will be imputed to the covered entity. This means that the covered entity must provide the required breach notification within 60 days from the time the business associate discovered the breach—not from the time the business associate notifies the covered entity. By contrast, if the business associate is an independent contractor of the covered entity (not an agent), then the covered entity must provide the notice within 60 days of the date the covered entity receives notice of the breach.

The notification to the covered entity by the business associate must identify each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during the breach. The business associate also must provide the covered entity with any other available information that the covered entity is required to include in its notification to the individual.

Administrative Requirements

Covered entities must develop breach notification policies and procedures and train their workforce members regarding such policies and procedures. They also must adopt and apply sanctions against workforce members who violate the entities' policies and procedures, including the breach notification policies and procedures.

Temporary Breach Notification Requirements for Personal Health Record Vendors and Other Non-HIPAA Covered Entities

The HITECH Act also included breach notification provisions for personal health record vendors ("PHR Vendors") and certain other entities (PHR-related entities and third party service providers) that are not HIPAA covered entities. The Federal Trade Commission is responsible for developing regulations for implementing these PHR Vendor requirements, and issued its regulations on August 18, 2009. The new FTC regulations address in detail the required methods of notice, timeliness of the notice, and content of such notices.

Practice group contacts

If you have questions regarding the information in this legal update, please contact the Dechert attorney with whom you regularly work, or any of the attorneys listed. Visit us at www.dechert.com/health.

Susan M. Hendrickson
Princeton
+1 609 620 3206
susan.hendrickson@dechert.com

Beth L. Rubin
Philadelphia
+1 215 994 2535
beth.rubin@dechert.com

Teresa L. Salamon
Philadelphia
+1 215 994 2273
teresa.salamon@dechert.com