JULY 2009

HHS Issues Guidance on Technologies and Methodologies That Render Protected Health Information Secure

The Health Information Technology for Economic and Clinical Health Act ("HITECH") provisions of the American Recovery and Reinvestment Act of 2009, enacted on February 17, 2009, create new data breach notification obligations for entities covered under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") ("Covered Entities") and their Business Associates 1. Covered Entities and Business Associates that do not secure protected health information2 ("PHI") in accordance with the guidance issued by the Department of Health and Human Services ("HHS") on April 17, 20093 , and as thereafter updated ("Guidance"), must, in the event of a breach of unsecured PHI, provide notification to patients and to HHS that patient data has been compromised.

New Breach Notification Requirement

HITECH requires a Covered Entity that holds, uses, or discloses unsecured PHI to notify each individual in the event of a breach of such information whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of such breach. "Unsecured PHI" is PHI that is not secured through the use of a technology or methodology specified by HHS in the Guidance. "Breach" is 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 4.

HITECH also requires a Business Associate to notify the Covered Entity of a breach of unsecured PHI, including the identification of each affected individual.

Covered Entities are further required to provide notice to HHS in the event of a breach of unsecured PHI.

Guidance Issued by HHS on Technologies and Methodologies for Securing PHI; Regulations to Follow

HITECH requires HHS to issue, and annually update, guidance specifying the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals. The Guidance is HHS's first attempt to do so. HITECH also requires HHS to issue interim final regulations within 180 days of enactment to address the new breach notification obligations placed on Covered Entities, and Business Associates.

The Federal Register notice in which the Guidance was published includes a request for public comment on the Guidance as well as on the breach notification provisions generally, to inform the future rulemaking and updates to the Guidance. The Guidance was developed through a joint

effort by the Office for Civil Rights within HHS, the Office of the National Coordinator for Health Information Technology, and the Centers for Medicare and Medicaid Services.

In addition to the breach notification regulations to be issued by HHS, the Guidance is also applicable to regulations to be issued by the Federal Trade Commission ("FTC") for vendors of personal health records and other non-HIPAA Covered Entities pursuant to Sec. 13407 of HITECH. For more information on the FTC's proposed rule on breach notification requirements applicable to personal health record vendors and related entities, see our July 2009 Privacy and Data Security Legal Update.

The Guidance applies to breaches of unsecured PHI 30 days after publication of interim final regulations.

Technologies and Methodologies Specified by HHS in the Guidance That Render PHI Unusable, Unreadable, or Indecipherable

The Guidance provides that PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals only if one or more of the following applies:

> (a) Electronic 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"[5] and such confidential process or key that might enable decryption has not been breached. The Guidance goes on to identify certain encryption processes for data at rest and data in motion that have been tested by the National Institute of Standards and Technology ("NIST") and judged to meet this standard.
>
> (b) The media on which the PHI is stored or recorded have been destroyed in one of the following ways: (i) Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed; or (ii) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*[6], so that the PHI cannot be retrieved.

As it stands, the Guidance does not specify a method for securing paper-based PHI maintained by a Covered Entity or Business Associate.

Use of HHS's Specified Technologies and Methodologies Create a "Safe Harbor"

If PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals by one or more of the methods or technologies identified in the Guidance, then such information is not "unsecured" PHI. In the Federal Register notice, HHS states, "While Covered Entities and Business Associates are not required to follow the guidance, the specified technologies and methodologies, if used, create the functional equivalent of a safe harbor, and thus, result in Covered Entities and business associates not being required to provide the notification otherwise required by section 13402 [of the HITECH Act] in the event of a breach."

Covered Entities and Business Associates Must Comply with Other Federal and State Laws That May Apply in the Context of a Breach of PHI

While Covered Entities and Business Associates that adhere to the Guidance may have no obligation to provide the breach notifications required under HITECH in the event of a breach of PHI, Covered Entities and Business Associates must comply with other federal and state statutory and regulatory obligations that may apply following a breach of personally identifiable information, such as state breach notification requirements. Forty-five states, including Connecticut and Massachusetts, have statutes that require notice of security breaches, and such statutes may contain additional or different requirements. In addition, Covered Entities are required under HIPAA to mitigate, to the extent practicable, any harmful effect that is known to the Covered Entity as a result of a breach of PHI by the Covered Entity or Business Associate [7].

HHS's Request for Public Comment

In the Federal Register notice, HHS has requested public comment on a number of specific issues, including the following:

- Whether additional technologies and methodologies exist that HHS should consider adding to the exclusive list compromising the Guidance in future iterations of the Guidance

- Whether PHI in limited data set[8] form should be treated as unusable, unreadable, or indecipherable to unauthorized individuals for purposes of breach notification, and thus, included in the Guidance

- Whether there are additional methods HHS should consider for rendering paper PHI unusable, unreadable, or indecipherable to unauthorized individuals

HHS has indicated that if it determines the Guidance should be modified, based on public comments, it will issue updated guidance prior to or concurrently with the breach notification regulations.

1 "Business Associate", as defined in the HIPAA regulations at 45 CFR 160.103, is a person (other than a member of the Covered Entity's workforce) or entity that provides services to, or performs certain functions or activities on behalf of, a Covered Entity, to the extent that such services, functions or activities involve the use or disclosure of protected health information.

2 "Protected health information", as defined in the HIPAA regulations at 45 CFR 160.103, means individually identifiable health information transmitted or maintained by a Covered Entity or its Business Associate in any form or medium.

3 Published in the Federal Register on April 27, 2009, 74 Fed. Reg. 79, 19006.

4 There are certain exceptions to this definition for inadvertent unauthorized acquisition, access, or use of PHI and inadvertent disclosures within a facility, as long as such information is not further used, accessed, acquired, or disclosed. See definition of "breach" at Section 13400 of the HITECH Act.

5 45 CFR 164.304, definition of "encryption."

6 Available at http://www.csrc.nist.gov/.

7 45 CFR 164.530(f).

8 A limited data set is protected health information from which the 16 direct identifiers listed at 45 CFR 164.514(e)(2) of the HIPAA Privacy Rule, including an individual's name, address, Social Security number, and account number, have been removed.

Robinson & Cole's Health Law Group includes:

Lisa M. Boyle
Theodore J. Tucci
Michael J. Kolosky
Karen P. Conway
B. Moses Vargas
Brian D. Nichols
Susan E. Roberts
Kimberly E. Troland

The information in this update should not be considered legal advice. Consult your attorney before acting on anything contained herein.