

“What keeps you up at night?”

Saul Ewing Health Law
Practice Group:

George W. Bodenger
Chair

Feds release guidance and proposed rule-making for HITECH Act compliance

By Bruce D. Armon and Evan J. Foster

The first wave of guidance and proposed rulemaking mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act passed as part of American Recovery and Reinvestment Act of 2009 have been released. On April 17th, the U.S. Department of Health and Human Services ("HHS") released the HITECH Act Breach Notification Guidance (the "Guidance"). One day earlier, on April 16th, the Federal Trade Commission ("FTC") released the proposed Health Breach Notification Rulemaking (the "Proposed Rule"). HIPAA covered entities, business associates, and vendors of so-called personal health records are advised to review the Guidance and Proposed Rule and submit comments, as appropriate, to HHS and FTC. For previous Saul Ewing alerts on the HITECH Act, see http://www.saul.com/common/publications/pdf_1894.pdf, http://www.saul.com/common/publications/pdf_1875.pdf and http://www.saul.com/common/publications/pdf_1877.pdf.

GUIDANCE FOCUSES ON TECHNOLOGIES AND METHODOLOGIES TO SECURE HEALTH INFORMATION

HITECH requires HHS to issue interim final regulations within one hundred eighty (180) days of the statute's enactment to require HIPAA covered entities and business associates to provide notification in the case of breaches of unsecured protected health information. The Guidance concerns the technologies and methodologies that would render protected health information ("PHI") "secure" by making such PHI "unusable, unreadable, or indecipherable to unauthorized individuals." Covered entities are required to notify affected individuals, and business associates are required to notify covered entities, upon discovery of a breach of "unsecured" PHI. However, if the PHI is rendered unusable, unreadable or indecipherable, the information is not unsecured. There is no breach and no notification obligation. The Guidance also applies to personal health records ("PHR") which is detailed in the Proposed Rule.

“What keeps you up at night?”

HHS is accepting comments to the Guidance received on or before May 21, 2009.

In the Guidance, HHS identifies two methods for rendering PHI and PHR data unusable, unreadable, or indecipherable to unauthorized individuals: 1) data encryption; or 2) destruction of the media on which the data is stored. Under the Guidance, to effectively secure PHI data using data encryption, technology that meets Federal Information Processing Standards (FIPS) 140-2 must be used to secure “data in motion,” such as PHI data transmitted over a network, while “data at rest,” such as PHI data stored in databases or within file systems, must be secured with technology that is compliant with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices. It is important to note that the Guidance is in addition to existing encryption requirements under HIPAA, and that all encryption used to secure PHI data must comply with the provisions of the HIPAA Security Rule. Furthermore, in the event an encryption key is breached, any data protected by such key will no longer be considered “secure,” and breach notification is required.

For PHI data that has been “disposed,” such as discarded paper records or electronic media, destruction of the media on which the PHI data is stored is required to render the PHI “secure.” Hardcopy media, such as paper or microfilm, must be shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Electronic media, such as hard disk drives, tapes or CDs, must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

The Guidance does not address the use of de-identified information as a method to render PHI unusable, unreadable or indecipherable because it is no longer PHI if it has been de-identified. The Guidance is also not intended to instruct covered entities and business associates on how to prevent breaches of PHI.

Importantly, the Guidance notes that covered entities and business associates must still comply with all other federal and state statutory and regulatory obligations that govern breaches of PHI, including applicable state-law breach notification requirements, as well as the obligation on covered entities under the HIPAA Privacy Rule, to mitigate any harmful effects resulting from a breach of PHI.

As required by the HITECH Act, the Guidance was developed by HHS in conjunction with external experts in security and informatics, as well as representatives from Federal agencies. While the Guidance provides direction, HHS has requested comments with respect to eleven (11) different questions related to technologies and methodologies that render PHI unusable, unreadable or indecipherable and with regard to the breach notification provisions. After final guidance is released, HHS is required to update the Guidance annually to account for new methodologies and technologies that may not yet be developed.

PROPOSED RULE IS FIRST STEP FOR VENDORS OF PERSONAL HEALTH RECORDS AND RELATED ENTITIES

The HITECH Act requires HHS, in consultation with FTC, to study potential privacy, security and breach notification requirements for PHR vendors and other entities that are not otherwise covered by HIPAA, and submit a report to Congress within one (1) year of enactment of the HITECH Act. Until Congress enacts new legislation resulting from the HHS/FTC Study, HITECH imposes certain requirements to be enforced by FTC against these entities in the event of a security breach. The Proposed Rule begins that process.

The Proposed Rule requires vendors of PHRs to notify affected individuals and the FTC upon discovery of a breach of “unsecured” individually identifiable health information (“IIHI”) contained in a PHR maintained or offered by such vendor. The Proposed Rule adopts the Guidance discussed above to determine whether IIHI in a PHR has been “secured,” and the same exceptions to a breach notification will apply to IIHI secured pursuant to the Proposed Guidance. In defining a “breach,” however, the FTC has limited the definition to the unauthorized “acquisition” of information, from the broader terms “accessed, acquired, or disclosed,” used in the HITECH Act. The Proposed Rule does specify that unauthorized “acquisition” will be presumed to include unauthorized access to unsecured IIHI unless the vendor of PHRs, PHR related entity, or third party service provider that experienced the breach can prove that there has not been, or could not reasonably have been, any unauthorized acquisition of such information. The burden of

“What keeps you up at night?”

overcoming this presumption falls on the PHR vendor, PHR related entity, or third party service provider.

The Proposed Rule defines a “PHR related entit[y]” as an entity that: “(1) offers products or services through the website of a vendor of [PHRs]; (2) offers products or services through the websites of HIPAA-covered entities that offer individuals [PHRs]; or (3) accesses information in a [PHR] or sends information to a [PHR].” The Proposed Rule identifies a “third party service provider” as an entity that: “(1) provides services to a vendor of in connection with the offering or maintenance of a [PHRs] or to a PHR related entity in connection with a product or service offered by that entity; and (2) accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information as a result of such services.”

The Proposed Rule states that when unsecured IIHI is breached, notice must be given to affected individuals “without unreasonable delay” and in any event no more than sixty (60) days after any employee, officer, or agent (other than the one committing the breach) of the vendor knows or “should reasonably have known” that a breach has occurred. For a breach involving 500 or more individuals’ information, the FTC must be notified no more than 5 business days from the date of discovery. For a breach involving less than five hundred (500) individuals’ information, the vendor may maintain a log of any such breach occurring over the ensuing twelve (12) months and submit the log to the FTC at the end of the year. The contents and methods of notification are prescribed in detail in the Proposed Rule, and may include a posting on the vendor’s website and notice to “prominent media outlets” for breaches involving more than five hundred (500) individuals’ information.

In addition to the notification requirements for PHR vendors, the Proposed Rule also requires “PHR related entities,” and “third party service providers,” who discover a breach to give timely notice to a senior officer of the vendor or PHR related entity (where the third

party service provider is providing services to such entity), which will then be obligated to provide appropriate notice to affected individuals and to the FTC, as above.

FTC estimates approximately nine hundred (900) entities will be subject to the Proposed Rule, and that an average of two hundred thirty two thousand (232,000) consumers per year will receive a breach notification. The FTC is inviting interested parties to comment on multiple elements related to the Proposed Rule. The FTC will accept comments to the Proposed Rule received on or before June 1, 2009.

The Guidance and the Proposed Rule contain many important provisions. HIPAA covered entities, business associates and vendors of personal health records and related entities should review both documents and provide comments in a timely manner to HHS and FTC.

This Alert was written by Bruce D. Armon, a Partner in the firm’s Health Law Practice Group and Managing Partner of the firm’s Philadelphia office and Evan J. Foster, an Associate in the firm’s Health Law Practice Group. Bruce can be reached at 215.972.7985 or barmon@saul.com. Evan can be reached at 610.251.5762 or efoster@saul.com. This publication has been prepared by the Health Law Practice Group for information purposes only.

The provision and receipt of the information in this publication (a) should not be considered legal advice, (b) does not create a lawyer-client relationship, and (c) should not be acted on without seeking professional counsel who have been informed of the specific facts. Under the rules of certain jurisdictions, this communication may constitute “Attorney Advertising.”

© 2009 Saul Ewing LLP, a Delaware Limited Liability Partnership.
ALL RIGHTS RESERVED.