

Regulatory Update: HITECH's Security Breach Notification Requirements

April 22, 2009

The Health Information Technology for Economic and Clinical Health Act (HITECH Act), part of the American Recovery and Reinvestment Act of 2009, includes significant investment in health information technology (IT) to facilitate the adoption of a nationwide health information network. Recognizing that the expansion of health IT creates the need for additional safeguards to protect personal information, among other measures, the HITECH Act requires covered entities, business associates, vendors of personal health records (PHR) and related entities to notify individuals when their *unsecured* protected health information (PHI) and PHR identifiable health information is subject to a breach of security.

The HITECH Act provides a framework for these security breach notification requirements and directs both the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) to promulgate further regulations. Recently, HHS issued guidance, and the FTC issued a notice of proposed rulemaking related to these security breach notification requirements. While HHS has not yet issued proposed regulations, the FTC noted that it is consulting with HHS to harmonize their respective security breach notification rules and, accordingly, the FTC's proposed regulations provide some insight as to what may be expected from the forthcoming HHS regulations. Both agencies are seeking public comment in order to issue interim final regulations by August 17, 2009, as required by the HITECH Act. Compliance with these regulations may require the expenditure of significant time and expense, therefore generating keen interest within health care and related industries.

For additional information regarding the security breach notification requirements set forth in the HITECH Act, see McDermott's *White Paper* "Economic Stimulus Package: Policy Implications of the Financial Incentives to Promote Health IT and New Privacy," available at <http://www.mwe.com/info/news/wp0209e.htm>.

HHS Breach Notification Guidance and Request for Public Comment

As required by the HITECH Act, HHS issued guidance on April 17, 2009, specifying the technologies and methodologies that will be considered to render PHI unusable, unreadable or indecipherable to unauthorized individuals. If covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or their business associates secure PHI using the methods identified in the guidance, then the HITECH Act's notification requirements are not triggered in the event of a breach involving that PHI. Covered entities and business associates must still comply with all other federal and state statutory and regulatory obligations that may apply following a breach of PHI, including state breach notification requirements and the obligation of covered entities to mitigate harmful effects that are a result of the breach.

Securing PHI

The guidance identifies two methods for rendering PHI unusable, unreadable or indecipherable to unauthorized individuals, encryption and destruction. In particular, the guidance for securing PHI focuses on three main areas, including PHI at rest, PHI in motion and the destruction of PHI.

At first glance, the guidance appears relatively short and deceptively simple. This brevity is because the guidance does not explicitly set forth the standards for securing information, and instead references hundreds of pages of various National Institute of Standards and Technology (NIST) publications which themselves elaborate upon the standards set by the guidance.

Encryption

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 the use of a confidential process or key" and such confidential process or key that might enable decryption has not been breached. Because of the increasing capabilities of computers, encryption key lengths must increase over time in order to keep data secure. Therefore, it is likely that encryption standards will continue to be revised as technology develops and will require periodic updating by covered entities and business associates in order to remain exempt from the HITECH Act's notification obligations.

PHI AT REST

According to the guidance, valid encryption processes for data at rest will be those that are consistent with NIST Special publication 800-111, *Guide to Storage Encryption Technologies for End User Devices* available at <http://esrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf>. For data at rest, the NIST document suggests using the Advanced Encryption Standard. For example, if a user edits documents using both a desktop PC at the organization’s office and a personally owned computer at home by transferring the documents between the computers using a USB flash drive, the organization could either: use a flash drive with self-contained storage encryption capabilities, such as encryption software and secure key storage; or use a volume, virtual disk or file/folder encryption solution that will work on both PCs, encrypting the documents on the local system and storing the encrypted data on the flash drive.

The chart below from the *Guide to Storage Encryption Technologies for End User Devices* describes the characteristics of several storage encryption technologies.

TABLE 3-1. CHARACTERISTICS OF STORAGE ENCRYPTION TECHNOLOGIES

Characteristic	Full Disk Encryption	Volume Encryption	Virtual Disk Encryption	File/Folder Encryption
Typical platforms supported	Desktop and laptop computers	Desktop and laptop computers, volume-based removable media (e.g., USB flash drives)	All types of end user devices	All types of end user devices
Data protected by encryption	All data on the media (data files, system files, residual data, and metadata)	All data in the volume (data files, system files, residual data, and metadata)	All data in the container (data files, residual data and metadata, but not system files)	Individual files/folders (data files only)
Mitigates threats involving loss or theft of devices?	Yes	Yes	Yes	Yes
Mitigates OS and application layer threats (such as malware and insider threats)?	No	If the data volume is being protected, it sometimes mitigates such threats.* If the data volume is not being protected, then there is no mitigation of these threats.	It sometimes mitigates such threats*	It sometimes mitigates such threats*
Potential impact to devices in case of solution failure	Loss of all data and device functionality	Loss of all data in volume; can cause loss of device functionality, depending on which volume is being protected	Loss of all data in container	Loss of all protected files/folders

Characteristic	Full Disk Encryption	Volume Encryption	Virtual Disk Encryption	File/Folder Encryption
Portability of encrypted information	Not portable	Not portable	Portable	Often portable

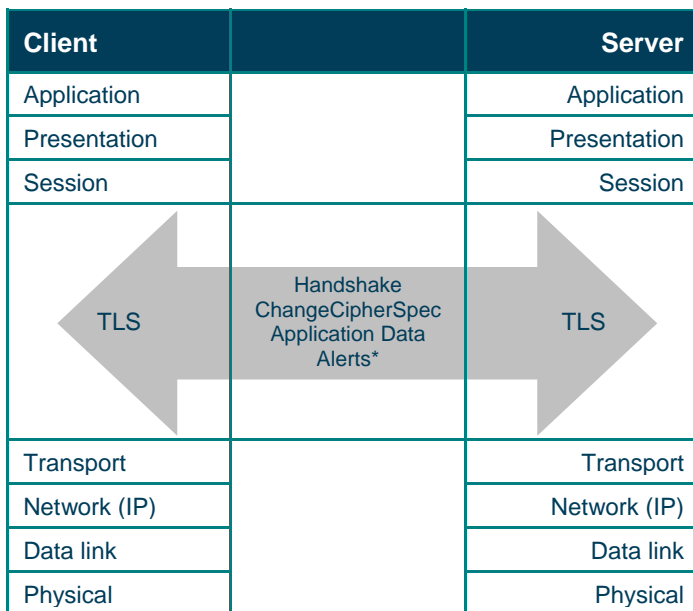
* These storage encryption technologies can only protect the files against some OS and application layer threats if the user has not been authenticated in this session to access the files. If a single sign-on solution is used, then generally the user is authenticated to the storage encryption technology during OS login, so the files are not protected against these threats once OS login occurs. If a separate authentication solution is used, the files are protected until that separate authentication is performed.

PHI IN MOTION

The guidance specifies that valid encryption processes for data in motion will be those that comply with the requirements of Federal Information Processing Standards 140-2, which include standards described in the following NIST Special Publications:

- 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations* available at <http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf>
- 800-77, *Guide to IPsec VPNs* available at <http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf>
- 800-113, *Guide to SSL VPNs* available at <http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf>

For data in motion, several different cryptographic protocols are specified by the NIST document, including Transport Layer Security (TLS). TLS is based on Secure Sockets Layer (SSL), which employs a public key system for authenticating users and systems and for exchanging keys. SSL virtual private networks (VPNs) can provide secure remote access to an organization’s resources when configured with appropriate cryptographic algorithms, cipher suites and versions of SSL. An SSL VPN consists of one or more VPN devices to which users connect using their web browsers. The data transmitted between the web browser and the SSL VPN device is encrypted with the SSL protocol or its successor approved cryptographic protocol, the TLS. The chart below from page 14 of the *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations* depicts the interaction between a computer and server using TLS implementations.



*Alerts can occur at anytime during the transaction process

Destruction

In order to secure information through destruction, the guidance requires the media on which the PHI is stored or recorded to be shredded or destroyed such that the PHI cannot be read or otherwise reconstructed and for electronic media to be cleared, purged or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization* available at http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf. The *Guidelines for Media Sanitization* describes various methods for sanitizing media prior to disposal, including clearing, purging and destroying, which are outlined in the chart below taken from page 16 of these NIST guidelines.

TABLE 5-1. SANITIZATION METHODS

Method	Description
Clear	One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
Purge	<p>Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging.</p> <p>Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36]</p>
Destroy	<p>There are many different types, techniques, and procedures for media destruction. If destruction is decided on because of the high security categorization of the information, then after the destruction, the media should be able to withstand a laboratory attack.</p> <ul style="list-style-type: none"> ▪ <i>Disintegration, Pulverization, Melting, and Incineration.</i> These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. ▪ <i>Shredding.</i> Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. <p>Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. When material is disintegrated or shredded all residues must be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm²).</p>

Limited Data Sets

A limited data set (LDS) is PHI from which 16 direct identifiers listed in the HIPAA Privacy Rule, such as the individual's name, address and social security number, have been removed. Although an LDS requires the removal of direct identifiers, the information is not completely de-identified for purposes of the HIPAA Privacy Rule because it may permissibly contain dates and zip codes. Because of the risk of re-identification of an LDS, the HIPAA Privacy Rule treats certain information within an LDS as PHI. Nevertheless, the HIPAA Privacy Rule makes distinctions between PHI in an LDS and PHI which contains direct identifiers, and permits covered entities to use or disclose PHI in an LDS in certain circumstances, including for some research purposes.

HHS notes that in developing the guidance, it considered whether PHI in LDS form should be treated as "secured" for purposes of the breach notification requirements. At present, the guidance treats LDS information as "unsecured" and therefore subject to the breach notification requirements. The guidance specifies that HHS is interested in receiving public comments on whether LDS should be included as a means of securing information and whether removal of one further piece of information, for example, the month of birth or the last three digits of the zip code, from the LDS would sufficiently reduce the risk of re-identification such that this modified data set could be added to the guidance as secured PHI.

Request for Public Comment

HHS is seeking public comments on the guidance, available at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechrfi.pdf>, as well as the breach notification provisions of the HITECH Act generally.

The technologies and methodologies for securing PHI listed in the guidance are intended to be exhaustive and not merely illustrative. Therefore, HHS is also soliciting comments on whether there are additional technologies and methodologies that HHS should consider adding to the exclusive list in the future.

Comments must be submitted on or before May 21, 2009.

FTC's Proposed Breach Notification Rule

Pursuant to the requirements of the HITECH Act, the FTC has published a *Federal Register* notice seeking public comment on a proposed rule that would require vendors of PHRs and related entities to notify individuals when the security of their identifiable health information is breached. The proposed Health Breach Notification Rule will place considerable obligations on vendors of PHRs and related entities in the event of a security breach. In addition, vendors of PHRs will likely incur significant time and expense to implement measures to secure individually identifiable health information to prevent security breaches. Comments to the proposed rule must be received by June 1, 2009, and, if adopted, the proposed rule will apply to breaches that are discovered on or after September 18, 2009.

In large part, the proposed rule follows the security breach notification requirements set forth in the HITECH Act. Following the discovery of a security breach, the proposed rule requires vendors of PHRs and related entities to notify the FTC and each individual whose unsecured PHR identifiable health information was acquired by an unauthorized person as a result of the breach. The FTC's definition of "unsecured" is derived from the guidance issued by HHS, as more fully described above. A key addition to the FTC proposed regulations from the HITECH Act itself is the FTC's pronouncement that an unauthorized acquisition will be *presumed* to include unauthorized access to unsecured PHR identifiable health information *unless the vendor or entity that experienced the breach has reliable evidence showing there has not been, or could not reasonably have been, any unauthorized acquisition of such information*. This addition offers at least some opportunity by organizations who have suffered a breach to examine the particular facts involved and then assess whether there was merely an opportunity to access information (which under the FTC's interpretation would not be reportable) versus determining that the information was actually acquired, which would be reportable. It will be interesting to see how HHS approaches this same issue in its regulations because the HITECH Act language relating to the reporting of security breaches by covered entities and business associates is slightly different from the HITECH Act language regarding PHRs.

Additional requirements set forth in the proposed rule include:

- *Who Must Comply:* Vendors of PHRs and PHR related entities that offer products or services through the website of a vendor of PHRs, offer products or services through the websites of covered entities that offer individuals PHRs, access information in a PHR or send information to a PHR must comply. Third party service providers which provide services to a vendor of PHRs or to a PHR related entity must notify the PHR vendor or related entity of a security breach.
- *Timeliness of Notification:* Notifications must be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security, unless otherwise directed by a law enforcement official.
- *Methods of Notice:* Notice must be provided in writing by first class mail to the affected individuals or by electronic mail if the individual provides express affirmative consent. In circumstances where there are 10 or more individuals who cannot be reached, a conspicuous posting on the vendor or related entity's internet home page or notice in major print or broadcast media may serve as a substitute form of notice. If the breach has affected the unsecured PHR identifiable health information of more than 500 residents, notice must also be provided to prominent media outlets following the discovery of a breach. The vendor or related entity must also notify the FTC following the discovery of a breach of security.
- *Contents of Notice:* Notice of a security breach must include a brief description of the events that occurred, the types of unsecured PHR identifiable health information that were involved, and actions performed by the entity to investigate the breach, to mitigate losses and to protect against further breaches. Notices should also include recommended steps individuals should take to protect themselves from potential harm and contact procedures for individuals to ask questions or learn additional information.
- *Enforcement:* A violation of the proposed rule will be treated as an unfair or deceptive act or practice in violation of the Federal Trade Commission Act.

The text of the proposed rule is available from the FTC's website at <http://ftc.gov/os/2009/04/R911002healthbreach.pdf>. Comments to the proposed rule can be submitted electronically by accessing <https://secure.commentworks.com/ftc-healthbreachnotification/>.

Implications of the HHS Guidance and the Proposed FTC Regulations

The HHS guidance carries with it critically important implications for HIPAA covered entities and their business associates in that each must look deeply and critically into their current security infrastructures—covered entities because they are currently covered by HIPAA, and business associates because they are already contractually committed to notify their covered entity customers of breaches, and will, as of February 17, 2010, be directly subject to HIPAA's civil and criminal penalties. For many of these organizations, particularly those smaller providers and vendors, the concept of encryption and the associated NIST standards are likely to be foreign. These standards are complex and costly, and will involve a great deal of IT management time as well as training of users in order to meet even the spirit of the guidance. Nevertheless, taking steps now to begin implementing the proper encryption components to one's operations should prove to be a wise investment when a laptop, for example, is lost or stolen. Similarly, the FTC's proposed regulations offers some useful commentary regarding the difference between situations where information could have been accessed contrasting that to situations in which it was actually acquired.

These two pronouncements represent the beginning of a series of proposed and interim final regulations to be issued pursuant to the HITECH Act, and the industry should anticipate a busy spring and summer with more regulations to come.

For more information, please contact your regular McDermott lawyer, or:

Stephen W. Bernstein: +1 617 535 4062 sbernstein@mwe.com

Bernadette M. Broccolo: +1 312 984 6911 bbroccolo@mwe.com

Heidi Y. Echols: +1 312 984 7559 hechols@mwe.com

April Timko: +1 617 535 4043 atimko@mwe.com

Maura Ward: +1 312 984 3275 mward@mwe.com

Stephen White: +1 617 535 4029 swhite@mwe.com

For more information about McDermott Will & Emery visit www.mwe.com

The material in this publication may not be reproduced, in whole or part without acknowledgement of its source and copyright. "Regulatory Update: HITECH's Security Breach Notification Requirements" is intended to provide information of general interest in a summary manner and should not be construed as individual legal advice. Readers should consult with their McDermott Will & Emery lawyer or other professional counsel before acting on the information contained in this publication.

© 2009 McDermott Will & Emery. The following legal entities are collectively referred to as "McDermott Will & Emery," "McDermott" or "the Firm": McDermott Will & Emery LLP, McDermott Will & Emery/Stamford LLP, McDermott Will & Emery Rechtsanwälte Steuerberater LLP, MWE Steuerberatungsgesellschaft mbH, McDermott Will & Emery Studio Legale Associato and McDermott Will & Emery UK LLP. McDermott Will & Emery has a strategic alliance with MWE China Law Offices, a separate law firm. These entities coordinate their activities through service agreements. This communication may be considered attorney advertising. Previous results are not a guarantee of future outcome.