

HHS and FTC Dive Into the Breach: Update on Breach Notification Under The HITECH Act

Reprinted with permission from the June 2009 issue of the *Privacy & Data Security Law Journal*. Copyright © 2009 ALEXeSOLUTIONS, INC. For further information, see <http://www.aspratt.com/store/L87.php> or call 1.800.572.2797.

The Health Information Technology for Economic and Clinical Health (HITECH) Act signed into law on February 17, 2009, as Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA), made many changes to the privacy and security of health information. Among the particularly significant changes are the HITECH Act's security breach notification provisions. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) did not include requirements for HIPAA covered entities to notify individuals in the event of breaches of their protected health information (PHI). Although nearly all states now have security breach notification laws (of varying applicability to personal health information), the adoption of the HITECH Act provisions establishes a federal standard for the health care industry.

The HITECH Act includes two sets of new breach notification requirements. Section 13402 of the HITECH Act requires HIPAA covered entities to notify individuals if there has been a breach involving their "unsecured PHI." Section 13407 of the HITECH Act includes breach notification requirements for vendors of personal health records (PHR) and related entities that are **not** subject to the HIPAA requirements and therefore not covered by the Section 13402 requirements.

DHHS Guidance on Unsecured PHI

Section 13402 of the HITECH Act includes the breach notification obligations for HIPAA covered entities and their business associates for breaches of "unsecured" PHI (including methods of notification, timeliness, content of the notice, etc.). The U.S. Department of Health and Human Services (DHHS) must issue interim final rules implementing these requirements not later than 180 days after enactment of the HITECH Act (by August 16, 2009). When issued, the rules will apply to breaches

The authors discuss the breach notification provisions of the HITECH Act that will affect covered entities already subject to HIPAA and other non-HIPAA covered entities and their business associates to be regulated by the FTC.

that are discovered on or after thirty (30) days following issuance of the rules.

Unsecured PHI is defined in Section 13402(h)(1)(A) as PHI that "is not secured through the use of a technology or methodology specified by the Secretary [of the DHHS] in the guidance issued under paragraph (2)." Section 13402(h)(2) of the HITECH Act requires the DHHS to issue guidance regarding the technologies and methodologies that would render PHI unusable, unreadable, or indecipherable to unauthorized individuals. On April 17, 2009, the DHHS issued guidance and a request for information developed through a joint effort by the DHHS Office of Civil Rights, the Office of the National Coordinator for Health Information Technology, and the Centers for Medicare and Medicaid Services.

In addition to applying to the breach notification regulations for HIPAA covered entities and their business associates, the DHHS guidance relates to the regulations to be issued by the Federal Trade Commission (FTC) for vendors of personal health records and other non-HIPAA covered entities.¹ If the entities subject to the HITECH breach notification regulations apply the technologies

and methodologies specified in the DHHS guidance to secure information, they will not be required to provide the notifications required by the HITECH Act and implementing regulations in the event there is a breach of the information. In other words, the guidance provides the means by which entities, regulated by the DHHS or the FTC under the applicable HITECH Act provisions, are to determine whether or not a breach has occurred requiring notifications.

The DHHS guidance² provides that PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals if the methodologies or technologies for encrypting or destroying the PHI as described in the guidance are used. The guidance provides this description of valid encryption processes:

(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” [45 C.F.R. §164.304] and such confidential process or key that might enable decryption has not been breached. Encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

(i) Valid encryption processes for data at rest are consistent with NIST Special Publication 800–111, *Guide to Storage Encryption Technologies for End User Devices*.

(ii) Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140–2. These include, as appropriate, standards described in NIST Special Publications 800–52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; 800–77, *Guide to IPsec VPNs*; or 800–113, *Guide to SSL VPNs*, and may include others which are FIPS 140–2 validated.

Another way to render PHI unreadable, unusable or indecipherable is to destroy it effectively. Importantly, the government has recognized that complete destruction of PHI when no longer necessary is as critical as encryption. Many breaches of PHI have been caused by sloppy destruction practices. The guidance provides several

methods of destroying the PHI depending on the type of media storing the PHI (paper, film, hard copy or electronic):

(b) The media on which the PHI is stored or recorded has 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.

(ii) 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.

The DHHS notes that it intends the guidance to be an exhaustive list and therefore is soliciting comments on additional technologies and methodologies to include in future versions of the guidance which is to be updated annually. Importantly, the government has recognized that complete destruction of PHI when no longer necessary is as critical as encryption.

The DHHS also is soliciting comments on a number of questions in connection with breach notification and HIPAA covered entities (and their business associates). One of the solicited questions is whether limited data sets (PHI where 16 identifiers have been removed but the information is not completely de-identified) can be used in manners that would be sufficiently protected to be unusable, unreadable or indecipherable to unauthorized individuals. Striking the proper balance between the necessity of the use of limited data sets especially in research and the risk of re-identification has been a challenge. While the HIPAA Privacy Rule treated information in a limited data set as PHI, its regulations distinguished between PHI in a limited data set and fully-identifiable PHI and relaxed certain requirements such as accounting of disclosures. The DHHS asked for public comment on whether the federal breach notification requirements should apply in the same way to limited data sets and fully identifiable PHI

In the guidance, the DHHS recognized and solicited comments on ways to harmonize the federal breach notification with state law concerning notification of breaches of privacy and security. State legislation on breach notification is a patchwork quilt of conflicting

requirements for, among other things, type and timing of notice. While federal pre-emption was not directly addressed in the HITECH Act, the comments in the guidance point to sensitivity by the DHHS not to add to an already confusing environment for patients/consumers by requiring a federal notice on top of state notices to one individual victimized by a breach of security. The guidance also asks a question as to whether there are areas of potential conflict with state breach notification laws which the DHHS should consider in promulgating federal breach notification regulations.

Finally, in the preamble to the guidance the DHHS emphasizes a critical point—the guidance does not address de-identified information as a method to render PHI unusable, unreadable or indecipherable to unauthorized individuals because once PHI has been de-identified it is no longer PHI and not subject to the HIPAA privacy and security rules. Health care entities especially business associates should carefully analyze their need for data to be personally identified and look for ways to properly de-identify PHI so that such data streams are outside regulatory purview. The DHHS is to issue further guidance on de-identification by February 17, 2010.

FTC Proposed Rule

The HITECH Act requires the FTC to issue interim final rules implementing breach notification requirements for PHR vendors and certain other non-HIPAA covered entities not later than 180 days after enactment of the HITECH Act (by August 16, 2009). On April 16, 2009, the FTC issued a proposed rule seeking comments by June 1, 2009.³ The HITECH Act also directs the DHHS and the FTC to study and submit a joint report to Congress, by February 17, 2010, on privacy and security and breach notification requirements for entities that are not HIPAA covered entities or business associates, such as PHR vendors and other related entities and service providers. Until Congress enacts any new legislation implementing recommendations included in the DHHS/FTC report, the notification requirements of Section 13407 of the HITECH Act and the proposed implementing regulations provide temporary breach notification requirements enforceable by the FTC.

The FTC's proposed rule⁴ includes a section-by-section analysis of the provisions of the proposed rule. Many of the FTC proposed requirements are similar to those applicable to HIPAA-covered entities; in fact a number of

requirements included in Section 13407 of the HITECH Act direct that the statutory requirements included in Section 13402 applicable to HIPAA covered entities are to apply to the FTC-regulated entities. The FTC notes in the preamble that it is consulting with the DHHS to "harmonize" its proposed rule with the DHHS proposed rule. The provisions of the proposed FTC rule will apply to breaches discovered on or after September 18, 2009.

Who Is Subject to the FTC Proposed Rule?

Three different categories of organizations will be subject to the FTC proposed rule:

1. Vendors of personal health records (known as PHR vendors) which are entities, other than HIPAA covered entities or business associates, that offer or maintain personal health records.
2. PHR related entities which are entities, other than HIPAA covered entities or business associates, that:
 - (a) offer products or services through the Web site of a PHR vendor, (b) offer products or services through the Web sites of HIPAA covered entities that offer individuals PHRs, or (c) access information in a PHR or send information to a PHR. The FTC provides some examples of organizations that could be PHR related entities including Web-based applications that help consumers manage medications, Web sites offering online personalized health checklists, and online applications through which individuals connect blood pressure cuffs, blood glucose monitors and other devices so that information can be tracked through their PHR.
3. Third party service providers which are entities that
 - (a) provide services to a PHR vendor in connection with the offering or maintenance of a PHR or to a PHR related entity in connection with a product or service offered by that entity; and (b) access, maintain, retain, modify, record, store, destroy or otherwise hold, use, or disclose unsecured PHR identifiable health information as a result of such services. It is worth noting that "third party service provider" was not defined in the HITECH Act, however, the FTC based its definition on the description of such parties included in Section 13407(b) of the Act.

The FTC notes that the proposed rule would apply to entities "beyond the FTC's traditional jurisdiction," such as nonprofit entities that offer PHR or related products and services as well as non-profit third party service providers. Both the preamble to the proposed rule and the proposed

rule itself clarify that the FTC regulations will not apply to HIPAA covered entities or business associates. And to the extent that FTC-regulated entities are engaged in activities as business associates of HIPAA covered entities, those entities will be subject only to the DHHS breach notification requirements.

What Is PHR Identifiable Health Information?

In order to understand whether a breach has occurred, it is important to understand what is the information being protected. “PHR identifiable health information” is defined as individually identifiable health information (as defined under HIPAA), and, with respect to an individual, information (1) that is provided by or on behalf of the individual, and (2) that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

The FTC notes three points in comments to this definition. First, as the definition includes information that relates to payment for health care, the proposed rule would cover a breach of a database containing names and credit card information even if no other information (e.g., health information) was included. This is a very broad definition and arguably broader than PHI has been interpreted under HIPAA and its implementing regulations. Second, the rule applies to the fact of having an account with a PHR vendor where the products or services offered by that vendor relate to particular health care conditions. The example included in the preamble is for the theft of an unsecured customer list of a vendor of PHR directed to AIDs patients or people with mental illness.

Third, if there is no reasonable basis to believe that the information can be used to identify the individual, the information does not meet the definition of PHR identifiable health information and therefore no breach notification need be provided. The FTC points to the HIPAA de-identified information standard and notes that if information has been de-identified under the HIPAA standards, the FTC will deem that information to fall outside of the definition of PHR identifiable health information. However, the FTC also notes that there may be other instances where even though the information is not de-identified there would be no reasonable basis to believe that the information is individually identifiable and the FTC asks for comments and examples on its interpretation.

If the schedule mandated by Congress remains on track, by the fall of 2009 HIPAA covered entities and their business associates, PHR vendors, PHR related entities and third party service providers will all need to be in compliance with the federal breach notification provisions.

What Constitutes a Breach of Security?

The FTC’s proposed rules define a “breach of security” as the acquisition of unsecured PHR identifiable health information of an individual in a PHR without the authorization of the individual. The breach notification requirements only apply if there is a breach of unsecured information; the information is unsecured if it is not protected through technology or methodology identified in the DHHS guidance addressed above.

Under the proposed rule, the key to determining whether there has been a breach requiring notification is being able to answer the question of whether the information has been acquired, not simply accessed. The proposed rule creates a rebuttable presumption that unauthorized persons have acquired PHR identifiable health information, if those persons had access to the information. The burden is placed on the entity where the breach occurred to determine whether the unauthorized access lead to acquisition of the information. The presumption can be rebutted with reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of the information. Entities can examine the following information to make this analysis: interviews with employees and contractors, access logs, and forensic analysis. The FTC provides a number of examples of acquisition and one example where they would find no acquisition took place and therefore no notification need be provided: when an employee inadvertently accesses a database realizes it is not the one he intended to view and immediately closes it without reading or disclosing anything. Conducting such analysis is critical to determining whether or not an entity needs to notify individuals of a breach, however, conducting this analysis

each time there is a potential breach can be a time-consuming and potentially costly endeavor. As a result to be sure of compliance with the law, entities may opt to make notifications rather than risk incorrectly (at least as interpreted by the FTC) concluding no acquisition of the information transpired. However, such notifications where there is no likelihood of harm potentially alarm patients/consumers needlessly.

Breach Notification Requirements

PHR vendors and PHR-related entities must notify the FTC and each individual who is a citizen or resident of the United States whose unsecured PHR identifiable health information was acquired by an unauthorized person. Third party service providers must notify the PHR vendor or PHR-related entities following the discovery of a breach and, to ensure notice is received, the proposed rule also requires the third party entity to notify a senior official of the PHR vendor or PHR-related entities and to obtain an acknowledgement of receipt of the notice.

Notice must be made “without unreasonable delay” and not later than sixty (60) days after the discovery of the breach. The FTC emphasizes that the 60 days is an outer limit and that it could be found to be an unreasonable delay to wait until the 60th day to provide notification if the entity was prepared to provide the notification earlier. In those situations where a third party entity notifies a PHR vendor or related entity of a breach it is not clear when the 60 day notice period begins to run. In comments to the proposed rule, the FTC notes that if a PHR vendor becomes aware of a breach at the third party entity before receiving notice from the third party, the PHR vendor should treat it as discovered. It is possible to infer from this comment that the notification time period commences when the PHR vendor becomes aware of the breach, however, added clarification by the FTC would be helpful. Finally, there is an exception if law enforcement determines that providing the notice would impede a criminal investigation or cause damage to national security.

Individual notice, made by a PHR vendor or PHR related entity, may be made by first class mail or by e-mail if the individual has provided express affirmative consent to receive e-mail notification. Telephone notice may be appropriate if urgency is required due to possible imminent misuse of the information. If 10 or more individuals cannot be reached using reasonable methods to contact

the individuals, the entity must provide notice (1) in a conspicuous posting on its Web site, and (2) in major print and broadcast media where affected individuals are likely to reside. Such a media notice must include a toll free number for the individuals to call to find out if their information was included in the breach. Entities must have methods in place to verify they are providing requested information to the individual and not to an unauthorized person.

Notice of breach should include:

- a brief description of how the breach occurred
- a brief description of the type of information involved (SSN, date of birth, names, address, account number)
- steps individuals can take to protect themselves from potential harm from the breach- these steps will vary depending on the circumstances of the breach and the type of information involved
- what the entity is doing to investigate the breach, mitigate the losses, and to protect from future breaches
- contact procedures for individuals to ask questions or to learn more - a toll-free telephone number, e-mail address, Web site or postal address must be included.

Notices should not include any requests for personal or financial information as the FTC notes this would raise individuals’ concerns about phishing.

In addition to the substitute media notice described above, the proposed rule includes a media notice if the breach involves unsecured PHR identifiable health information for 500 or more people. This notice is intended to supplement required individual notice. Furthermore, notice must be provided to the FTC as soon as possible and not later than five days if the breach involved information for 500 or more people. If the breach was for fewer than 500 people, the entity is to maintain a log and submit the log one year from the date of the first breach. The proposed rule provides that the FTC will have instructions on its Web site for submitting the information.

What Is Next?

The DHHS guidance and FTC proposed rule are the first in what will be a series of regulations, guidance and studies issued by these two agencies addressing breach notification under the HITECH Act. If the schedule mandated by Congress remains on track, by the fall of 2009 HIPAA covered entities and their business associates,

PHR vendors, PHR-related entities and third party service providers will all need to be in compliance with the federal breach notification provisions.

Although interim final regulations likely will not be issued for a few more months, compliance is required just 30 days later. While there are open questions that the DHHS and the FTC have opportunities to clarify, organizations should start to prepare now. Organizations should identify the members of an interdisciplinary team who will handle breach and related notifications. Composition of a team will vary among organizations but consider including the chief information officer, compliance officer, human resources, legal/risk management and public relations. The team should educate themselves about the new requirements and develop templates of policies and procedures and forms of documents (e.g., notice letter, media relations scripts) compliant both with the new federal standard and applicable state notification laws. Having an action plan, including checklists of key contacts such as media and others both within and outside of the organization, will enable organizations to effectively and timely respond to potential breach notification situations.

Authors:

Sharon R. Klein
949.567.3506
215.981.4172
kleins@pepperlaw.com

Rebekah A. Z. Monson
215.981.4031
monsonr@pepperlaw.com

Endnotes

- 1 Section 13407 of the HITECH Act.
- 2 74 *Federal Register* 19006, 19009-19010 (April 27, 2009).
- 3 74 *Federal Register* 17914 (April 20, 2009).
- 4 Proposed 16 C.F.R. Part 318 at 74 *Federal Register* 17914, 17923-17925 (April 20, 2009).

Pepper Hamilton LLP Attorneys at Law

The material in this publication is based on laws, court decisions, administrative rulings and congressional materials, and should not be construed as legal advice or legal opinions on specific facts. The information in this publication is not intended to create, and the transmission and receipt of it does not constitute, a lawyer-client relationship.

Please send address corrections to phinfo@pepperlaw.com.

www.pepperlaw.com

Berwyn | Boston | Detroit | Harrisburg | New York | Orange County | Philadelphia | Pittsburgh | Princeton | Washington, D.C. | Wilmington

© 2009 Pepper Hamilton LLP. All Rights Reserved.
This publication may contain attorney advertising.