BNA's

HEALTH CARE POLICY

BNA Employee-Owned Since 1947

VOL. 0, NO. 0 REPORT MAY 11, 2009

Information Technology

HITECH Updates: FTC Proposes Health Breach Notification Rule; HHS Releases Guidance on How to Render PHI 'Unusable, Unreadable, or Indecipherable'

By Robert Hudock and Patricia Wagner[1]

Introduction

As a result of the American Recovery and Reinvestment Act of 2009 (ARRA), laws in the privacy and security arena are rapidly emerging. This article details new proposed FTC requirements for notification of security breaches as well as new HHS guidance for encrypting or destroying protected health information.

First, the Federal Trade Commission (FTC) released proposed regulations titled the ''Health Breach Notification Rule'' on April 16, 2009.[2] Public comments on the proposed rule are due by June 1, 2009. Once final, these FTC regulations will apply to ''breaches of security'' that occur on or after Sept. 18, 2009, if those breaches involve information contained in or related to personal health records (PHRs).

Second, on April 17, 2009, the Department of Health and Human Services (HHS) released guidance ''specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals for purposes of the HHS's breach notification for covered entities and their business associates'' pursuant to Section 13402 of the ARRA.[3] The guidance became effective upon issuance (April 17, 2009). Comments to the guidance can be submitted to HHS **on or before May 21, 2009**, by posting comments on the HHS Web site, at http://www.hhs.gov/ocr/privacy. Significantly, the FTC's proposed rule specifically references the guidance for the methods to render information unreadable, unusable, or indecipherable, thereby avoiding the notifica-

[1] *Patricia Wagner is a Member of the Firm in the Health Care and Life Sciences Practice in the Washington, D.C. office of Epstein, Becker & Green PC. Robert Hudock is a Senior Associate in the Health Care and Life Sciences Practice in the Washington, D.C. office.*

[2] The proposed regulations are available at http://law2point0.com/wordpress/wp-content/uploads/2009/04/ftc-r911002healthbreach.pdf. Comments can be submitted at https://secure.commentworks.com/ftc-healthbreachnotification.

[3] The guidance is available at http://law2point0.com/wordpress/wp-content/uploads/2009/04/hitechrfi1.pdf.

tion requirements under the proposed rule.[4] (16 CFR 318.2(h)).

FTC Proposed PHR Rule

The proposed rule sets forth new breach notification requirements for PHRs. It was promulgated pursuant to Section 13407(g)(1) of the ARRA and will apply to vendors of PHR products or services and related entities to the extent they are not already covered entities or indirectly covered through a business associate relationship under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[5] As stated in the preamble, the FTC ''is consulting with HHS to harmonize its proposed rule with HHS' proposed rule.'' HHS will promulgate its breach notification requirements for entities covered by HIPAA no later than Aug. 17, 2009. Details of particular note, including the broad application of the proposed rule, are discussed below.

The proposed rule expands the traditional scope of the FTC's enforcement authority:

> The Commission also notes that the proposed rule applies to entities beyond the FTC's traditional jurisdiction under Section 5 of the FTC Act, since the Recovery Act does not limit the FTC's enforcement authority to its enforcement jurisdiction under Section 5. Indeed, section 13407 of the Recovery Act expressly applies to ''vendors of personal health records and other non-HIPAA covered entities,'' without regard to whether such entities fall within the FTC's enforcement jurisdiction. Thus, the proposed rule would apply to entities such as non-profit entities that offer personal health records or related products and services, as well as non-profit third party service providers.

The FTC interprets the key term ''identifiable health information'' to include ''the fact of having an account with a vendor of personal health records or related entity, where the products or services offered by such vendor or related entity relate to particular health conditions.'' (Proposed Rule at 12). Examples under the FTC's interpretation where breach notification would be required, even where no specific health information is disclosed, include the theft of a vendor's unsecured customer list of patients disclosing HIV status or mental illness. (Proposed Rule at 12).

The proposed rule covers vendors of PHRs, PHR-related entities and third-party service providers. A vendor of PHRs is an entity, other than a HIPAA covered entity or a business associate, that ''offers or maintains a personal health record.'' PHR-related entities include non-HIPAA covered entities ''that access information in a personal health record or send information to a personal health record.'' (16 CFR 318.2(f)). A third-party service provider is an entity that provides services to a PHR entity or PHR-related entity, where those services include accessing, maintaining, modifying, recording, storing, destroying, holding, using, or disclosing PHR-identifiable health information.

Thus, although the proposed rule excludes HIPAA covered entities and business associates of covered entities (to the extent those services are being provided as a business associate), the proposed rule will apply broadly to any entity that offers products or services through the Web site of a PHR vendor, and any entity that accesses information in a PHR or sends information to a PHR. (16 CFR 318.2(f)).

The definition ''*breach of security*'' in the proposed rule mimics most state-based security breach notification laws. Section 318.2 defines ''breach of security'' as the *acquisition* of unsecured *PHR identifiable health information* of an individual without the authorization by that same individual. This definition is identical to the definition of ''breach of security'' found in Section 13407(f)(1) of the ARRAt. The term ''acquisition,'' according to the proposed rule, ''suggests that the information is not only available to unauthorized persons, but in fact has been obtained by them.'' (Proposed Rule at 8). However, the FTC's position is a presumption that any information that is available has been obtained. ''[T]he proposed rule creates a presumption that unauthorized persons have acquired information if they have access to it, thus creating the obligations to provide breach notification.'' (Proposed Rule at 9).

Nevertheless, in the proposed rule, the FTC describes a scenario where an employee inadvertently accesses a database but realizes that it was not the one he or she intended to view, and logs off without reading, using, or disclosing anything. For this example, the FTC's view is that there has not been a breach of security. (Proposed Rule at 9). In contrast, were an employee to review records to obtain information about friends or about a public figure to sell to the press, a security breach would have occurred.

As noted above, under the proposed rule, where the information is available to unauthorized parties, there is a presumption that a breach has occurred. However:

> [T]his presumption can be rebutted with reliable evidence showing that the information was not or could not reasonably have been acquired. Such evidence can be obtained by, among other things, conducting appropriate interviews of employees, contractors, or other third parties; reviewing access logs and sign-in sheets; and/or examining forensic evidence.

(Proposed Rule at 9). If an entity can demonstrate that the information could not ''reasonably'' have been acquired, the entity can rebut the presumption that a security breach occurred.

A security breach will be treated as discovered ''as of the first day on which such breach is known to a vendor of personal health records, PHR related entity, or third party service provider, respectively, including any person (other than the individual committing the breach).'' (16 CFR 318.3(c)). Notice must be provided without unreasonable delay, but no later than 60 days after the breach is discovered. Moreover, the FTC must be notified within five business days of discovery if the breach involves more than 500 individuals. (16 CFR 318.4). Where a breach involves fewer than 500 individuals, a PHR vendor or a PHR related entity must report such incidents in an annual report to the FTC. Third-party service providers also are required to notify a ''senior official'' of the PHR vendor or PHR related entity. Receipt of such notice must be acknowledged by the se-

[4] ''Unsecured means PHR identifiable information that is not protected through the use of a technology or methodology specified by the Secretary of Health and Human Services in the guidance issued under section 13402(h)(2) of the American Reinvestment and Recovery Act of 2009.'' (16 CFR 318.2(h)).

[5] HIPAA covered entities include health care providers, payers, and clearinghouses. Under the HITECH Act, business associates of covered entities also will be covered by the HHS security breach notification requirements.

nior official. The FTC notes that the acknowledgment requirement limits the likelihood that the notification will be lost or overlooked in mail or e-mail.

Finally, Section 318.9 clarifies that the proposed rule will sunset when Congress enacts new legislation affecting PHR related entities and third-party vendors of PHR vendors.

HHS Guidance on Rendering PHI Unreadable and/or Indecipherable

As noted above, the FTC's proposed rule references HHS guidance for determining methods to render information unreadable. Thus, the HHS guidance encompasses both PHI and identifiable health information held by PHR vendor and related entities. In sum, no security breach will have occurred where the health information is rendered unreadable and/or indecipherable. Section 13402(h) defines ''unsecured protected health information'' as protected health information that is not secured through the use of a technology or methodology specified by the HHS secretary. Encryption or destruction are the only recognized methods of securing PHI. Details for implementing these two methodologies depend upon the situation and the process by which the data are encrypted and/or destroyed. HHS guidance refers the reader to an array of National Institute of Standards and Technology (NIST) special publications.

Unlike the more general HIPAA privacy and security regulations, NIST publications provide very specific criteria that must be met. As a consequence, what HHS in the future will deem an appropriate level of protection will likely be much different. It is likely that a thorough analysis by covered entities and business associates as to the application of physical, technical and administrative safeguards will be essential. The HHS guidance will require entities to be familiar with at least 10 of the core NIST special publications to gain a working understanding of the methods by which PHI can be rendered unreadable or indecipherable.

The guidance also provides a framework by which appropriate safeguards for securing protected health information can be evaluated. For example, the guidance identifies vulnerabilities and suggests safeguards to mitigate threats to protected health information. The following data ''states'' are delineated within the guidance:

- **data in motion** meaning data that is moving through a network, including wireless transmission;
- **data at rest** meaning data that resides in databases, file systems, and other structured storage methods;
- **data in use** meaning data in the process of being created, retrieved, updated, or deleted; and
- **data disposed** meaning discarded paper records or recycled electronic media).

While these data states are not new to computer security practitioners, they reflect a much more advanced approach, compared to earlier HIPAA privacy and security guidance. (Guidance at 12). The guidance states that HHS consulted the NIST when identifying appropriate safeguards. The reader also is directed to review the NIST Special Publication 800-66-Revision1 ''An Introductory Resource Guide for Implementing the HIPAA Security Rule.''

Encryption is one of the core methods to render PHI unreadable. However, encryption encompasses domains such as cryptology, number theory, and cryptoanalysis. For even the most advanced security expert, understanding how to encrypt information properly can be complex. HHS solves this problem simply by relying on NIST. PHI must be encrypted using a NIST-approved algorithm and procedure to be considered unreadable. Electronic PHI is properly encrypted 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 CFR 164.304), and the key to decrypt the PHI has not been breached. Encryption identified by NIST and judged to meet NIST's encryption standards is acceptable to render PHI unreadable. (Guidance at 16). Current acceptable encryption methods include:

- For data at rest, those methods contained within NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Device*; and
- For data in motion, those methods contained within the Federal Information Processing Standards (FIPS) 140-2. These methods are explained in detail 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 others which are FIPS 140-2 validated. (Guidance at 17).[6]

In addition to encryption, destruction also is deemed an acceptable method to render PHI unreadable and/or unusable.

Acceptable methods for destroying PHI are specified:

- paper, film, or other hard copy media must be shredded or destroyed such that the PHI cannot be read or otherwise reconstructed; and
- electronic media must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*, such that the PHI cannot be retrieved. (Guidance at 17).

Conclusion

We encourage affected parties to comment on both the proposed rule and guidance so that these policy/compliance initiatives by the FTC and HHS take into account business realities. The FTC's proposed rule addressing security breach notice requirements and the HHS guidance for encryption/destruction should be considered by all affected entities as they review and refine their privacy and security policies or consider investment in new information technologies. We can expect additional, similarly detailed guidance to be promulgated in the months to come as other privacy and security provisions of the HITECH Act and the ARRA are implemented by regulation.

[6] Links to the above-referenced publications are available at http://law2point0.com/wordpress/2009/04/23/hhs-releases-guidance-on-how-to-render-phi-unusable-unreadable-or-indeciperable-that-relies-on-nist-to-define-acceptable-methods-for-destruction-and-encryption/.