

The New HIPAA Breach Notification Rules: A Guide for Covered Entities and Business Associates to the Breach Reporting Obligations under the HITECH Act and HHS Regulations

by **Alicia H. Sable and Robert Hudock**

August 2009

The Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”), which is part of the sweeping American Recovery and Reinvestment Act of 2009,¹ contains a series of laws that dramatically expand the privacy and security aspects of the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder (the “Privacy and Security Rules” or “HIPAA”). One of the most significant changes in the HITECH Act is the requirement that Covered Entities (as defined under the Privacy Rule)² notify individuals when there is a “breach” of such individual’s “unsecured” protected health information (“PHI”). The breach reporting obligation also requires that Covered Entities provide notice of the breach to the Secretary of the Department of Health and Human Services (respectively, the “Secretary” and “HHS”), and in some instances, the media. The breach reporting obligations also apply to Business Associates (as defined under the Privacy Rule)³ who are required to report breaches to Covered Entities.

* For more information on the HITECH Act, please see the following Client Alerts, which are available under “News and Publications” at www.ebglaw.com: “HITECH Updates: Proposed Health Breach Notification Rule Promulgated by the FTC; HHS Releases Guidance on How to Render PHI ‘Unusable, Unreadable, or Indecipherable’” and “Analysis of the HITECH Act’s Incentives to Facilitate Adoption of Health Information Technology.”

¹ Pub. L. No. 111-5 (2009), at § 13000 (hereinafter “HITECH Act”).

² A “Covered Entity” is defined as a: (i) health care provider who transmits health information in electronic format in connection with HIPAA-covered transactions, (ii) a health plan, or (iii) a health care clearinghouse. 45 C.F.R. § 160.103.

³ A “Business Associate” is defined under the Privacy Rule as an entity that either performs or assists in the execution of a function or activity involving the use or disclosure of PHI, or provides services for a Covered Entity where the provision of the service involves the disclosure of PHI. 45 C.F.R. § 160.103.

On August 24, 2009, HHS published regulations⁴ clarifying the breach reporting obligations and providing guidance on the meaning of “secured” and “unsecured” PHI (the “Breach Notification Rules”). Pursuant to the new Breach Notification Rules, Covered Entities are required to report breaches that are discovered after **September 23, 2009**. However, the Secretary has decided to further delay enforcement of these regulations in order to give Covered Entities and Business Associates a reasonable amount of time to come into compliance with the breach reporting obligations. It is critical that Covered Entities and Business Associates undertake steps to come into compliance immediately because the breach reporting requirements obligate Covered Entities and Business Associates to develop new security breach reporting policies and procedures.

Breach Reporting Obligations

In the event of a “breach” of “unsecured” PHI, a Covered Entity must notify each individual whose unsecured PHI has been, or is reasonably believed to have been, breached.⁵ A “breach” is defined as “the acquisition, access, use, or disclosure” of PHI in a manner that violates the Privacy Rule or Security Rule and which “compromises the security or privacy of the [PHI].”⁶ “Unsecured” PHI is PHI that is “not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary.”⁷

Risk of Harm Standard

A breach that “compromises the security or privacy of the [PHI]” has its own definition, which is that such breach “poses a **significant risk of financial, reputational, or other harm** to the individual.”⁸ This risk of harm standard is a new development that qualifies the meaning of a “breach” in the HITECH Act and guidance issued by the Secretary on April 17, 2009.⁹ The risk of harm standard requires that a Covered Entity undertake some form of risk assessment in the event of a breach, and based upon the assessment, determine in good faith whether it is necessary to notify the individual of the breach.

Significantly, the preamble to the Breach Notification Rules specifically references a 2007 Memorandum (M-07-16) issued by the Office of Management and Budget “for examples of the types of factors that may need to be taken into account in determining whether an impermissible use or disclosure presents a significant risk of harm to the

⁴ Breach Notification for Unsecured Protected Health Information; Interim Final Rule, 74 Fed. Reg. 42740 (Aug. 24, 2009) (to be codified at 45 C.F.R. Parts 160 and 164) (hereinafter “Breach Notification Rules”). Note that the Federal Trade Commission has issued separate regulations with respect to the breach notification obligations applicable to entities that collect or use “Personal Health Records,” which are defined under the HITECH Act. The Federal Trade Commission regulations are outside of the scope of this article.

⁵ 45 C.F.R. § 164.404(a)(1).

⁶ *Id.* at § 164.402.

⁷ *Id.*

⁸ *Id.* (emphasis added).

⁹ See HITECH Act, *supra* note 1, at § 13400(1). The April 17, 2009 guidance from the Secretary is available at <http://law2point0.com/wordpress/wp-content/uploads/2009/04/hitechrfi1.pdf>.

individual.”¹⁰ This Memorandum provides guidance to federal agencies on assessing the risk of harm in the event of a security breach. This guidance will become a basis for determining compliance with the risk assessment requirement under the Breach Notification Rules, and therefore entities should consider the following factors in conducting their risk assessment:¹¹

1) Nature of the Data Elements Breached. Entities should analyze the nature of the data elements compromised. For example, the disclosure of a person’s name in one context may be more sensitive than the disclosure of a name in another context.

2) Likelihood the Information is Accessible and Usable. Entities should assess the likelihood that unsecured PHI will be or has been used by unauthorized individuals.

3) Likelihood the Breach May Lead to Harm. In the context of the type(s) of data involved in the breach, entities should consider the number of possible harms that could arise as a result of the breach of unsecured PHI, and further assess the likelihood of harm.

4) Ability of the Entity to Mitigate the Risk of Harm. The risk of harm may depend upon the ability of the entity to mitigate the effects of the breach. An entity should consider appropriate breach prevention, monitoring, and mitigation measures that it can take in response to the breach.

On one hand, the risk of harm standard is beneficial to the Covered Entity¹² because it eliminates the “strict liability” aspect of the breach notice requirement in the HITECH Act, and brings the HHS definition of “breach” more in line with many state security breach notification laws. On the other hand, it means that the Covered Entity will need to adopt policies and procedures for conducting and documenting a risk assessment, and incorporating them into its existing Privacy and Security Policies and Procedures.

Notice Requirements

Notice must be made to the affected individuals “without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.”¹³ A breach is considered to be “discovered” by the entity as of the first day on which the breach is known to the entity, or should have been known to the entity if it had exercised reasonable due

¹⁰ Breach Notification Rules, *supra* note 3, at pg. 42744 n. 7.

¹¹ See OMB Memorandum M-07-16, page 14 (*available at* <http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf>)

¹² The burden to determine whether there is a risk of harm resulting from the breach is on the Covered Entity; not the Business Associate. Therefore, a Business Associate should not have discretion to determine whether there is a risk of harm. A Business Associate is obligated to report the breach to the Covered Entity regardless of whether there is a risk of harm.

¹³ 45 C.F.R. § 164.404(b). One exception to the 60-day notification window occurs if law enforcement officials inform a Covered Entity or Business Associate that notification would interfere with a criminal investigation. *Id.* at § 164.412.

diligence.¹⁴ The due diligence requirement means that Covered Entities and Business Associates should have policies and procedures in place to detect and identify breaches, which likely will require coordination among the individuals and departments that are responsible for the physical, administrative and technical aspects of the entity's compliance with the Privacy and Security Rules.

The notice shall be made in writing, except under circumstances where the Covered Entity does not have the correct contact information for the affected individual, or where there is particular urgency to the notification. The notice to affected individuals must contain the following 5 elements:

- 1) A brief description of what occurred with respect to the breach, including, to the extent known, the date of the breach and the date on which the breach was discovered;
- 2) A description of the types of unsecured PHI that were disclosed during the breach;
- 3) A description of the steps the affected individual should take in order to protect himself or herself from potential harm caused by the breach;
- 4) A description of what the Covered Entity is doing to investigate and mitigate the breach and to prevent future breaches; and
- 5) Instructions for the individual to contact the Covered Entity.¹⁵

If the breach of unsecured PHI involves more than 500 residents of a state, the Covered Entity must notify media outlets within that state. The Covered Entity must also notify the Secretary of any breach involving 500 or more people. Notification through the media and to the Secretary must be made within 60 days of the discovery of the breach. If the breach involves fewer than 500 individuals, the Covered Entity shall create a log documenting the breach. The Breach Notification Rules do not specify what information must be maintained in the annual log. The Covered Entity shall provide a copy of the log of all such breaches to the Secretary within 60 days after the end of each calendar year.¹⁶

If the breach occurs at or through a Business Associate, the Business Associate must notify the Covered Entity of the breach within 60 days of discovering the breach so that the Covered Entity is able to comply with its breach reporting obligations.¹⁷

Methods of Securing PHI

As discussed above, the breach reporting obligations are implicated when there is a breach of "unsecured" PHI. Pursuant to the HITECH Act, on April 17, 2009, the

¹⁴ *Id.* at § 164.404(a)(2).

¹⁵ *Id.* at § 164.404(c).

¹⁶ *See* 45 C.F.R. §§ 164.406 and 164.408 for guidance on notice to the media and to the Secretary.

¹⁷ *Id.* at § 164.410.

Secretary 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.”¹⁸ The guidance provides a framework by which methods of safeguarding and securing PHI should be evaluated, and provides definitions of various “states” of data that should be analyzed, including:

- “**data in motion**,” which is data that is moving through a network, including wireless transmission;
- “**data at rest**,” which is 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 data.¹⁹

While these categories of data are not new to computer security practitioners, they represent a much more advanced approach to data security as compared to earlier HIPAA privacy and security guidance. The commentary notes that HHS consulted the National Institute of Standards and Technology (the “NIST”) when identifying appropriate safeguards.

Encryption is one of the core methods to render PHI unreadable; however, encryption encompasses domains such as cryptology, number theory, and crypto analysis, for even the most well-versed security expert, understanding how to encrypt information properly is complex. To be considered unreadable, PHI must be encrypted using an NIST approved algorithm and procedure. Electronic PHI is encrypted when “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”²⁰ and the key to decrypt the PHI has not been breached.²¹ It is important to note that in order to comply with the encryption standards and ensure the keys are not compromised, Covered Entities and Business Associates must keep encryption keys on a separate device from the data that they encrypt or decrypt.

The commentary to the Breach Notification Rules notes that “covered entities and business associates may continue to create limited data sets or de-identify [PHI]

¹⁸ The Secretary’s guidance is available at <http://law2point0.com/wordpress/wpcontent/uploads/2009/04/hitechrfi1.pdf> (last visited August 23, 2009).

¹⁹ Breach Notification Rules, *supra* note 3, at pg. 42742.

²⁰ 45 C.F.R. § 164.304.

²¹ Current acceptable encryption methods include: (i) for data at rest, those methods contained within NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Device; and (ii) for data in motion, those methods contained within the Federal Information Processing Standards (FIPS) 140-2 are acceptable. 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. *See* Breach Notification Rules, *supra* note 3, at pg. 42742.

through redaction if the removal of identifiers results in the information satisfying the criteria of [sections 164.514(e)(2) or 164.514(b) of HIPAA], respectively. Further, a loss or theft of information that has been redacted appropriately may not require notification under these rules either because the information is not [PHI] (as in the case of de-identified information) or because the unredacted information does not compromise the security or privacy of the information.”²² HHS is required to update its guidance on encryption/destruction annually.²³

Destruction is also an acceptable method of rendering PHI unreadable. The commentary to the Breach Notification Rules states that paper, film, or other hard copy media be shredded or destroyed such that the PHI cannot be read or otherwise reconstructed. 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.²⁴

HHS draws a distinction between encryption and other access controls:

While we believe access controls may render information inaccessible to unauthorized individuals, we do not believe that access controls meet the statutory standard of rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals. If access controls are compromised, the underlying information may still be usable, readable, or decipherable to an unauthorized individual, and thus, constitute unsecured protected health information for which breach notification is required.²⁵

Following the same line of reasoning, HHS rejects redaction of PHI as a method of rendering PHI unreadable. The preamble states that “redaction is not a standardized methodology with proven capabilities to destroy or render the underlying information unusable, unreadable or indecipherable, we do not believe that redaction is an accepted alternative method to secure paper-based protected health information.”²⁶ However, the physical destruction of paper is a method of rendering PHI unreadable. This again is a rather interesting distinction, considering that both paper and electronic documents (for example PDFs) can be redacted such that the information cannot be recovered.

Practical Steps in the Event of a Breach

In the comments to the new Breach Notification Rules, HHS provides a basic overview of the steps that Covered Entities and Business Associates should follow in order to

²² Breach Notification Rules, *supra* note 3, at pg. 42742.

²³ See HITECH Act, *supra* note 1, at § 13402(h)(2).

²⁴ Breach Notification Rules, *supra* note 3, at pg. 42743.

²⁵ *Id.* at pg. 42742. While, HHS appears to believe that strong access controls are required, a review of potential safeguards is beyond the scope of the guidance which primarily details methods of rendering PHI unreadable.

²⁶ *Id.*

determine whether the entity has breach reporting obligations. The recommended steps are as follows:

Step 1 Determine whether the disclosure or use of PHI was impermissible under the HIPAA Privacy Rule.

Step 2 Determine whether the PHI was “secured” or “unsecured,” and whether the impermissible use or disclosure of PHI compromises the security or privacy of such PHI, and document its process and determination. The use or disclosure would be impermissible if it poses a “significant risk of financial, reputational, or other harm to the individual.”

Step 3 Determine whether the use or disclosure falls under one of the exceptions to the definition of a “breach.” The exceptions to the definition of a “breach” are: (i) any unintentional access or use of PHI by a Covered Entity’s or Business Associate’s workforce or person acting under the authority thereof, if such access was in good faith, within that person’s scope of authority, and did not result in further impermissible use or disclosure of the PHI; (ii) any inadvertent disclosure by a person who is authorized to have access to such PHI to another authorized person at the same Covered Entity or Business Associate, or organized health care arrangement in which the Covered Entity participates, and the PHI disclosed is not further used or disclosed in an impermissible manner; and (iii) disclosure of PHI where the Covered Entity or Business Associate has a good faith belief that the unauthorized person who received the PHI would not reasonably have been able to retain such PHI.²⁷

If the breach poses a significant risk to the individual whose PHI was disclosed, and the disclosure does not fall under one of the enumerated exceptions to the definition of a “breach,” the entity must take the following step:

Step 4 Provide appropriate notice of the breach in accordance with the Breach Notification Rules.

Regardless of whether a breach is in violation of the Privacy Rule or Security Rule and raises reporting obligations under the Breach Notification Rules, the entity may have reporting obligations under state security breach reporting laws that are not preempted by the Privacy Rule or Security Rule. Therefore, it would be prudent for the entity to take the following additional step:

Step 5 Determine whether the breach raises any additional reporting obligations under applicable state security breach reporting laws.²⁸

²⁷ *Id.* at pg. 42748.

²⁸ As of August 2009, the following states have enacted security breach notification laws: Alabama, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan,

Policies and Procedures

Covered Entities will need to revise their Privacy and Security Policies and Procedures and/or create new policies, in order to comply with the new breach reporting obligations.²⁹ Among the new Privacy and Security Policies and Procedures that are required under the Breach Notification Rules are:

- Policies and procedures providing for the training of all members of their workforce with respect to the breach reporting obligations and procedures;
- Sanctions that will be imposed upon members of the workforce who fail to comply with the entity's breach notification policies and procedures;
- Processes by which individuals can make complaints regarding the entity's compliance with the breach reporting rules; and
- Prohibition on retaliation against individuals who exercise a right, or file a complaint under the applicable HHS regulations.³⁰

The HITECH Act makes Business Associates directly subject to the Security Rule and to portions of the Privacy Rule as of February 17, 2010, and therefore, Business Associates will need to develop and implement comprehensive Policies and Procedures as of that date, including procedures to detect breaches and provide notice to Covered Entities in the event of a breach.

Covered Entities and Business Associates should consult with legal counsel in developing or amending Policies and Procedures to incorporate the new breach reporting obligations.

Effective Date and Enforcement

Section 13402(j) of the HITECH Act states that the breach reporting obligations become effective 30 calendar days after the publication of the Breach Notification Rules (which would be on **September 23, 2009**). In the comments to the new Breach Notification Rules, the Secretary stated that HHS "will use [its] enforcement discretion to not impose sanctions for failure to provide the required notifications for breaches that are discovered before 180 calendar days from the publication [of the HHS regulations],"³¹ which will be the middle of **February 2010**. However, Covered Entities and Business Associates cannot be complacent during this 6 month grace period. The Secretary

Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin and Wyoming.

²⁹ 45 C.F.R. § 164.530(i).

³⁰ *Id.* at § 164.530.

³¹ Breach Notification Rules, *supra* note 3, at pgs. 42756-7 (*emphasis added*).

made clear that entities are to use this period of non-enforcement to properly prepare for the breach notification requirements by stating, “we expect covered entities to comply with this subpart and will work with covered entities, through technical assistance and voluntary corrective action, to achieve compliance.”³² The civil monetary penalties for noncompliance can range from \$100 to \$50,000 per violation. The maximum penalties that can be applied for additional violations in any one year are within a range of \$25,000 to \$1,500,000.³³ Therefore, Covered Entities and Business Associates must take action now to develop and implement their breach reporting policies and procedures so that they are prepared to comply with the breach reporting obligations once enforcement begins.

* * *

For questions regarding this alert and topic, please contact:

Alicia H. Sable
New York
(212) 351-4514
Asable@ebglaw.com

Robert Hudock
Washington, DC
(202) 861-1893
Rhudock@ebglaw.com

The EpsteinBeckerGreen Client Alert is published by EBG's Health Care and Life Sciences practice to inform health care organizations of all types about significant new legal developments.

Lynn Shapiro Snyder, Esq.
EDITOR

If you would like to be added to our mailing list or need to update your contact information, please contact, Jennifer Sunshine, jsunshine@ebglaw.com or (202) 861-1872.

This document has been provided for informational purposes only and is not intended and should not be construed to constitute legal advice. Please consult your attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on you and your company.

© 2009 Epstein Becker & Green, P.C.

ATLANTA • BOSTON • CHICAGO • HOUSTON • LOS ANGELES • MIAMI
NEW YORK • NEWARK • SAN FRANCISCO • STAMFORD • WASHINGTON, DC

Attorney Advertising

www.ebglaw.com



³² *Id.* at pg. 42757.

³³ See HITECH Act, *supra* note 1, at § 13410(d).