SCOTT TECHNOLOGY ATTORNEYS

HIPAA / HITECH BREACH NOTIFICATION GUIDE

As part of the American Recovery and Reinvestment Act of 2009, the federal legislature passed significant revisions to the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. Entitled the Health Information Technology for Economic and Clinical Health Act, or HITECH Act[1], these revisions now require both Covered Entities and Business Associates to report any breaches of unsecured protected health information ("PHI"). Depending on the severity of the breach in question, the Covered Entity[2] or Business Associate[3] may be required to notify the individual whose PHI was leaked, the Secretary of the Department of Health and Human Services, and the media. In addition, Covered Entities or Business Associates can be subject to criminal charges of up to $250,000 in fines and 10 years imprisonment.[4]

In accordance with HITECH, the Department of Health and Human Services ("HHS"), issued an Interim Final Rule setting out, among other things, the standards of the breach notification requirements under HITECH.[5] This guide is meant to assist a company with interpretation of the HITECH Act requirements for breach notification, but is not a substitute for competent legal advice.

[1] HITECH Act (full text available here: http://waysandmeans.house.gov/media/pdf/111/hitech.pdf).
[2] "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] "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.
[4] 42 U.S.C. 1320d-6, Wrongful Disclosure of Individually Identifiable Health Information
[5] Breach Notification for Unsecured Protected Health Information: Interim Final Rule (full text available here: http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf).

DEFINITION OF BREACH

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.[6] This includes Covered Entities and Business Associates (Business Associates are entities that either perform a function or provide a service involving the use of PHI.[7]

RISK OF HARM STANDARD

Breaches that "compromise the security or privacy of PHI" are ones that "poses a significant risk of financial, reputational, or other harm to the individual."[8] This standard suggests that a Covered Entity should conduct some form of risk assessment in the event of a breach. Risk factors include: 1) nature of the data elements breached; 2) likelihood the information is accessible and usable; 3) likelihood that the breach may lead to harm; and 4) ability of the entity to mitigate the risk of harm.[9]

EXCEPTIONS:

Below is a list of built-in exceptions to what constitutes a breach under the rules. If a breach occurs under these narrow circumstances, it is not a "breach."

1. Unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of a covered entity or business associate.[10]
2. Inadvertent disclosure of protected health information from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate.[11]

For the first two exceptions, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.

3. The covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.[12]

UNSECURED PHI

The HITECH breach notification requirement is implicated when a breach of "unsecured" PHI occurs.[13] So naturally, organizations should endeavor to ensure that their PHI is not "unsecured." Under HITECH, unsecured PHI is

---

[6] 45 CFR § 164.402.
[7] *Id.* at § 160.103.
[8] *Id.* at § 164.402.
[9] *2007 Memorandum (M-07-16) issued by the Office of Management and Budget*. (full text here: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf).
[10] HITECH Act § 13400(1)(B)(i).
[11] *Id.* at § 13400(1)(B)(ii).
[12] *Id.* at § 13400(1)(B)(iii).
[13] 45 C.F.R. § 164.404(a)(1).

protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance.[14]

RENDERING UNUSABLE, UNREADABLE OR INDECIPHERABLE:

ENCRYPTION: Encryption is an acceptable method of securing PHI. PHI is considered encrypted if it meets the definition in the HIPAA Security Rule: using "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" and such confidential process or key that might enable decryption has not been breached. [15] To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The following methods meet the encryption standard:

1. Data at Rest (i.e., data that resides in databases, file systems, and other structured storage methods):
    - NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices
2. Data in Motion (i.e., data moving through a network, including wireless transmission):
    - 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,
    - or others which are Federal Information Processing Standards (FIPS) 140-2 validated. [16]

DESTRUCTION: The media on which the PHI is stored or recorded can be destroyed in one of the following ways:

1) Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
2) 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.[17]

It is important to note that redaction as a method for destruction is specifically rejected by the HHS for rendering PHI unreadable.

BREACH NOTIFICATION REQUIREMENTS

In the event of a breach of unsecured PSI, notice must be given "without unreasonable notice and in no case later than 60 days" after discovery.[18] Discovered is the first day the entity knew or should have known. Notice is to be in writing (with some exceptions) and must contain 5 elements: [19]

1) Brief description of breach
2) Description of the type of PHI disclosed
3) Description of the steps affected individuals should take to protect themselves
4) Descriptions of the steps the Entity is taking to investigate and mitigate

---

[14] *Id.* at § 164.402.
[15] *Id.* at § 164.304.
[16] *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* pg. 19008 (full text available here: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf).
[17] *Id.*
[18] 45 C.F.R. § 164.404(b).
[19] *Id.* at § 164.404(c).

5) Entity contact information

The HHS website provides the following guidance for

INDIVIDUAL NOTICE

Covered entities must notify affected individuals following the discovery of a breach of unsecured PHI via first-class mail or where individuals have previously consented, e-mail. If a Covered Entity does has inaccurate or out-of-date contact information for 10 or more individuals, the notice must be either posted to the Covered Entity's web site, or submission to major print or broadcast media in the area of the individuals' likely residence. In situations where there are less than 10 inaccurate contacts, the Covered Entity can utilize other means to contact the individual.

Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.[20]

MEDIA NOTICE

Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.[21]

NOTICE TO THE SECRETARY

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.[22]

NOTIFICATION BY A BUSINESS ASSOCIATE

As stated above, Business Associates are also subject to the security provisions of HITECH. If a breach of unsecured protected health information occurs at or by a Business Associate, the Business Associate must notify the Covered Entity following the discovery of the breach within the same time frame as all other notice requirements. The

[20] HITECH Act § 13402(e)(1).
[21] *Id.* at § 13402(e)(2).
[22] *Id.* at § 13402(e)(3).

business associate should provide the covered entity with the identification of each individual, along with any other information that the Covered Entity requires for its notice to the affected individuals.[23]

RECOMMENDED PROCEDURE IN THE EVENT OF A BREACH

The Breach Notification Rules include comments from the HHS which sets out a recommended procedure for Covered Entities and Business Associates to follow in the event of a suspected breach of PHI.

1. Determine whether there has been an impermissible use or disclosure of PHI;
2. Determine and document whether the impermissible use or disclosure of PHI compromises the security or privacy of the PHI; and,
3. Determine if the impermissible use or disclosure of PHI falls under one of the statutory exceptions.[24]

If the Covered Entity or Business Associate concludes that a breach has occurred that compromises the security or privacy of the PHI that is not covered by one of the exceptions, they must take appropriate notification steps to comply with the requirements under the rules.

Robert J. Scott and Andrew Martin are attorneys at intellectual property and technology law firm Scott & Scott, LLP. For more information, visit http://scottandscottllp.com or call 214.999.0080, 800.596.6176.

[23] *Id.* at § 13402(b).
[24] *Interim Final Rule* at 42748.