BNA, INC.

HEALTH IT LAW & INDUSTRY

BNA Employee-Owned Since 1947

REPORT

HIPAA Breach Notification Rules and Reporting Obligations Under the HITECH Act and Final HHS Regulations

By Robert Hudock and Patricia Wagner

On August 24, 2009, HHS published regulations[1] clarifying the breach reporting obligations and updating the earlier guidance on the meaning of ''secured'' and ''unsecured'' PHI (the ''Breach Notification Rules''). Pursuant to the new Breach Notification Rules, covered entities (and business associates) are required to report breaches that are discovered after September 23, 2009. The new Breach Notification Rules were enacted pursuant to the Health Information Technology for Economic and Clinical Health Act (''HITECH''), which is found within the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (2009), at § 13000.

This article addresses four key areas related to the new Breach Notification Rules:

(i) the details of the notice requirement to HHS in light of the recently released electronic breach submission form;

(ii) a candid evaluation the new harm standard with the Breach Notification Rules and the political unpopularity of this standard among a small group of congressmen and privacy rights advocates;

(iii) the harm standard versus a strict liability trigger (an acquisition based trigger); and

(iv) effective date and enforcement of the new Breach Notification Rules.

Generally, the new HHS Security Breach Notification Rule requires that:

1. A covered entity (defined under the HIPAA Privacy Rule)[2] must notify individuals when there is a ''breach'' of an individual's ''unsecured'' protected health information (''PHI'');
2. Covered entities are also required to provide notice of the breach to the Secretary of the Department of Health and Human Services (the ''Secretary''), and in some instances, the media; and
3. Business associates (as defined under the Privacy Rule)[3] are required to report breaches to covered entities.

The reporting requirement in the event of a security breach and more specifically, when and how a covered entity should conclude that a reportable security breach

[1] 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). 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.

Wagner is a member of the firm in the Health Care and Life Sciences Practice in the Washington office of Epstein, Becker & Green, P.C. Hudock is a senior associate in the Health Care and Life Sciences Practice in the Washington office. Wagner may be contacted at pwagner@ebglaw.com and Hudock may be contacted at rhudock@ebglaw.com.

[2] A ''Covered Entity'' is defined as: (i) a health care provider who transmits health information in electronic format in connection with HIPAA-covered transaction, (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, and in general is an entity that provides a service for a Covered Entity and in doing so uses, creates, receives or discloses PHI,. 45 C.F.R. § 160.103.

 ISSN 2151-2876

has (or has not) occurred is key in assessing a covered entity's (and perhaps a business associate's) responsibilities under the new regulations. This is especially significant given the addition of a harm (or risk based) analysis that a covered entity must undertake to determine whether a security breach is a reportable event.

Notice Requirements

The breach notification interim final rule requires covered entities to provide the Secretary with notice of breaches of unsecured protected health information (45 CFR § 164.408). The number of individuals affected by the breach determines when the notification must be submitted to the Secretary.

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.'' (45 C.F.R. § 164.404(b).) There is one exception to the 60-day notification window, which occurs if law enforcement officials inform a Covered Entity or Business Associate that notification to affected individuals would interfere with a criminal investigation. (45 C.F.R. § 164.412).

A breach is considered to be discovered by the covered entity as of the first day on which the breach is known to the covered entity, or should have been known to the covered entity if the covered entity exercised reasonable due diligence.[4] The due diligence requirement indicates that covered entities must 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 covered entity's compliance with the Privacy and Security Rules.

The notice to affected individuals must contain the following elements: (i) 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; (ii) a description of the types of unsecured PHI that were disclosed during the breach; (iii) a description of the steps the affected individual should take in order to protect himself or herself from potential harm caused by the breach; (iv) a description of what the Covered Entity is doing to investigate and mitigate the breach and to prevent future breaches; and (v) instructions for the individual to contact the Covered Entity. (45 C.F.R. § 164.404(c))

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. (45 C.F.R. § 164.404(d)).

Content of Notice to the HHS Secretary for a Reportable Security Breach

The Notification Rules also require that a covered entity notify the Secretary of the breach. If a covered entity that has submitted the required breach notification forms to the Secretary and discovers additional information, the covered entity must submit an additional form. (*See* Instructions for Submitting Notice of a Breach to the Secretary, available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.) The Secretary has delayed enforcement of the Security Breach Rules to give covered entities and business associates a reasonable amount of time to come into compliance.

However, in anticipation of covered entities' new reporting obligations, HHS on October 7, released an online form (OMB No. 0990-0346) that appears to be the exclusive mechanism by which a covered entity can provide the required notice to the Secretary in the event of a security breach. (The form is available at http://transparency.cit.nih.gov/breach/index.cfm). The form is intended only for security breach submissions by covered entities to the Secretary. Breaches involving business associates must be reported directly to the Secretary by the affected covered entity and not by the business associate; although covered entities will want to ensure that they receive sufficient information from their business associates to complete the form.

Analysis of OMB No. 0990-0346 – HHS's Security Breach Reporting Form

The form itself offers some insight into HHS's understanding of security breaches and how HHS believes breaches can be mitigated and/or avoided altogether. For example:

1. HHS has defined seven categories of breaches within the form: theft, loss, improper disposal, unauthorized access, hacking/IT incident, other, and unknown. Theft, loss, and improper disposal are breaches that can be easily mitigated by encryption or by following the guidelines referenced by HHS for the destruction of paper/and electronic media.
2. The ''locations'' where a breach may occur as identified by HHS include: laptops, desktops, network servers, e-mail, other portable electronic devices, electronic medical records, paper, and other. Again this question and the pre-populated responses echo HHS's interest in encryption for data stored on laptops, desktops, and other portable media devices. Moreover, loss of PHI related to theft/loss of computer equipment, fraud, hacking and e-mail are the biggest source of breaches involving PHI. (*See* http://law2point0.com/wordpress/american-recovery-and-reinvestment-act/significant-security-breaches-36-months/).
3. The form identifies four categories of PHI—demographic information, financial information, clinical information and other. Demographic information and financial information are high value targets to potential identity thieves.
4. The form requires the covered entity to identify whether any of the following security controls were in place before the security incident: firewalls, packet filtering (router based), secure browser sessions[5], strong authentication[6], en-

[4] *Id.* at § 164.404(a)(2).

[5] The term ''secure browser sessions'' is an unusual term, it is not clear whether secure browser sessions mean: encrypted sessions (i.e. https opposed to http); configuring the browser to remove traces of sites visited by deleting the data from the computer's registry, cache and temporary files; preventing the installation of browser plugins (e.g. active, etc.); and/or blocking the use of cookies by websites.

[6] Strong authentication has not been clearly defined in the literature, the term has been defined to include: (i) two-factor authentication or more generally multi-factor authentication;

  HITR ISSN 2151-2876

crypted wireless[7], physical security, logical access controls, anti-virus software, intrusion detection, and biometrics. This list of security controls is an odd combination of specific types of security controls (e.g. packet filtering router) and general categories of security controls (e.g. physical/logical access controls). Interestingly however, the form includes biometrics but excludes two factor authentication (a more general category). The utility of biometric access controls relate more generally to creating systems of two factor authentication. Two factor authentication techniques are based on any two of the following three types of methods: something you know, something you are, and something you have. One common example of two factor identification is the use of a security token that generates a seemingly random number in combination with a pin and a password to authenticate a user. Biometric methods of identification, which include fingerprint scanners, facial recognition, and retinal scanners, are either too expensive to implement as a broad-based solution or are poor quality consumer oriented solutions.

As noted above, the form provides insight into the hot button issues that may get HHS Office of Civil Rights' (the federal enforcement agency) attention and more importantly how to avoid them: (i) encrypting portable media, (ii) firewalls, (iii) proper document destruction procedures, (iv) the existence of a physical security plan, (v) two factor authentication, and (vi) antivirus software and procedures.

Harm or Risk Based Contingent Security Breach Reporting Obligations

The most important feature of the new breach regulations from a compliance perspective is the risk of harm standard that qualifies the meaning of a ''breach'' in the HITECH Act and guidance issued by the Secretary on April 17, 2009. (*See* HITECH Act at § 13400(1)).

The regulations provide that a breach is reportable if it is one that ''compromises the security or privacy of the [PHI]'' and is a breach that ''poses a ***significant risk of financial, reputational, or other harm*** to the individual.'' (45 C.F.R. § 164.402). The risk of harm standard requires that a covered entity undertake a risk assessment of the potential harm to the affected individuals, and based upon this assessment; determine in good faith whether it is necessary to notify the individual(s) of the breach.

Generally 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. (45 C.F.R. § 164.404(a)(1)).[8]

HHS has developed the harm standard by detailing criteria that a covered entity can use to assess the potential risk of harm or risk to an individual whose information may have been compromised. The harm standard is discussed in detail in the preamble to the Breach Notification Rules. The preamble specifically references a 2007 Memorandum (M-07-16) issued by the Office of Management and Budget (OMB) ''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 individual.'' (74 Fed. Reg. at 42744 n.7).

This guidance is the basis for determining compliance with the risk assessment (harm) requirement under the Breach Notification Rules. The OMB Memorandum includes four factors to consider when conducting a risk assessment of the potential harm resulting from a security breach to a consumer:

1) **Nature of the Data Elements Breached.** In assessing the risk associated with the disclosure of the data elements, entities also should analyze the data element(s) in context and consider the range of potential harms that could arise from disclosure to unauthorized individuals.
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.** Entities should consider the number of possible harms that could arise as a result of the breach of unsecured PHI, and the likelihood of the occurrence of that 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.

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

Despite the obvious utility of the new harm standard, a few privacy advocates (and some members of Congress) have expressed displeasure with the new HHS harm standard.[9] An October 1st letter from congressional leaders sent to HHS Secretary Sebelius argues that the ARRA did not imply a harm standard in the breach notification requirements, and requests that HHS repeal the harm standard that was included in the interim final regulations on Breach Notification for Unsecured Protected Health Information. (See http://law2point0.com/sebelius_letter.pdf.)[10]

(ii) multiple challenge/ response questions; (iii) the type of encryption method used for transmission/storage of passwords used for authentication (e.g. FIPS 140-2 certified method/ product); and (iv) authentication accomplished without the transmission of a password.

[7] Many common wireless encryption systems are easily cracked. For example Wi-Fi Protected Access (WPA) is a wireless security protocol to fix known security issues of WEP. However, WPA-PSK, where the administrator specifies a shared password, which must be known by all users for access is now known to be vulnerable to a dictionary attack. Wired Equivalency Privacy (WEP) was the first generation of encryption for wireless networks (the key can be either 64-bit or 128-bit) and can be easily cracked in less than 30 minutes.

[8] ''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.'' (45 C.F.R. § 164.402).

[9] Jaikumar Vijayan, *HHS guts health-care breach notification law, groups warn: Use of 'harm threshold' undermines intent of law passed by Congress* (Computer World September 18, 2009) (Available at http://www.computerworld.com/s/article/9138220/HHS_guts_health_care_breach_notification_law_groups_warn.)

[10] The letter was signed by **Henry A. Waxman**, Chairman of the Committee on Energy and Commerce (Democrat, California); **Charles B. Rangel**, Chairman of the Committee of Ways and Means (Democrat, New York); **John D. Dingell**, Chairman

However, many states use a standard similar to the harm standard under the federal Breach Reporting Rules (including Michigan and New Jersey). Only six states have a strict acquisition based standard including California, New York, and Texas. (http://law2point0.com/wordpress/2009/09/15/50-state-security-breach-notice-law/).

Without the harm standard, covered entities would be forced into over-reporting incidents — over-reporting can be just as damaging as not reporting any security incidents. Two studies help put the ''harm'' or risk-based standard for security breach reporting in an appropriate (real-world) context.

The first study is a report prepared by the General Accounting Office (GAO) from 2007 entitled *PERSONAL INFORMATION — Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (the report is available for free at http://www.gao.gov/new.items/d07737.pdf). This report evaluated the 24 largest breaches reported in the media from January 2000 through June 2005. The study found that:

- In only three instances was there evidence of fraud on existing accounts and in only one instance of the three identified cases did the GAO find evidence of unauthorized creation of a new account;
- For 18 of the breaches, no clear evidence was uncovered linking the breach to identity theft; and
- In the remaining two cases there was insufficient information to make a determination.

A second article, by S. Romanosky, R. Telang, and A. Acquisti, entitled *Do Data Breach Disclosure Laws Reduce Identity Theft?* (available for free at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1268926) summarizes the debate surrounding security breach notification laws and their impact. The authors' analyses reveal a modest effect of security breach disclosure laws in reducing identity theft rates by approximately 2%. However, this article also notes that over-reporting has many negative consequences — including unnecessary costs and desensitizing consumers such that when a real incident that they should take notice of is ignored.

The harm standard may result in fewer notices in some states where there are explicit state based exceptions for HIPAA covered entities from provisions of the applicable state reporting requirements—but absent an applicable exception, there is no federal preemption that would prevent a state from adopting a strict liability reporting obligation. A covered entity might be bound by the higher state standard (depending on the data element focus of the state requirements), and certainly would be bound if the state includes health information within the scope of the state's breach reporting statute.

The acquisition based standard reaches the wrong result for both consumers and companies. HHS's new Breach Reporting Rules for covered entities and business associates includes a rational framework for entities to frame analysis of a security incident and the potential risk to consumers.

Rendering PHI Unusable, Unreadable, or Indecipherable

Breach reporting obligations are implicated when there is a breach of ''unsecured'' PHI. Pursuant to the HITECH Act, on April 17, 2009, the 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.''[11] This guidance has remained largely unchanged in the Breach Reporting Rules. 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: (i) ''**data in motion**,'' which is data that is moving through a network, including wireless transmission; (ii) ''**data at rest**,'' which is data that resides in databases, file systems, and other structured storage methods; (iii) ''**data in use**,'' meaning data in the process of being created, retrieved, updated, or deleted; and (iv) ''**data disposed**,'' meaning discarded data. The commentary to Breach Notification Rules includes further details regarding the distinctions between data at rest and data in motion. (74 Fed. Reg. at 42742).

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] 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.'' (74 Fed. Reg. at 42742) HHS is required to update its guidance on encryption/destruction annually. (HITECH Act at § 13402(h)(2)).

Destruction is also an acceptable method of rendering PHI unreadable, acceptable methods for destroying PHI at this time. 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. (74 Fed. Reg. at 42743).

HHS draws an interesting 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***

Emeritus of the Committee on Energy and Commerce (Democrat, Michigan); **Pete Fortney Stark,** Chairman, Subcommittee of Health Committee on Ways and Means (Democrat California), **Joe Barton** Ranking Member Committee on Energy and Commerce (Republican, Texas) and **Frank Pallone**, Jr., Chairman Subcommittee on Health Committee on Energy and Commerce (Democrat, New Jersey).

[11] The Secretary's guidance is available at http://law2point0.com/wordpress/american-recovery-and-reinvestment-act/hhs-releases-guidance-on-how-to-render-phi-unusable-unreadable-or-indeciperable-that-relies-on-nist-to-define-acceptable-methods-for-destruction-and-encryption/ (*last visited* October 13, 2009).

  HITR ISSN 2151-2876

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.

(74 Fed. Reg. at 42742).

HHS believes that strong access controls are required; however, a review of potential safeguards is beyond the scope of the guidance which primarily details methods of rendering PHI unreadable.

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.'' (74 Fed. Reg. at 42742). However, the physical destruction of paper is a method 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.

Effective Date and Enforcement

Section 13402(j) of the HITECH Act states that the breach reporting obligations became effective 30 calendar days after the publication of these HHS regulations (which was on **September 23, 2009**). However, in the comments to the new Breach Reporting 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],'' (74 (Fed. Reg. at 42756-7), which will be the middle of **February 2010**.

The Secretary 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.'' (Fed. Reg. at 42757). 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. (HITECH Act at § 13410(d)).

Covered entities and business associates should take action to develop and implement breach reporting policies and procedures to be prepared to comply with their new breach reporting obligations prior to enforcement.