ReedSmith

lshi

Life Sciences Health Industry Alert

If you have questions or would like additional information on the material covered in this Alert, please contact the author:

Brad M. Rostolsky
Associate, Philadelphia
+1 215 851 8195
brostolsky@reedsmith.com

...or other members of the team

Gina M. Cavalier
Partner, Washington, D.C.
+1 202 414 9288
gcavalier@reedsmith.com

Mark S. Melodia
Partner, Princeton
+1 609 520 6015
mmelodia@reedsmith.com

Steven Boranian
Partner, San Francisco
+1 415 659 5980
sboranian@reedsmith.com

Paul Bond
Associate, Princeton
+1 609 520 6393
pbond@reedsmith.com

…or the Chair of the Life Sciences Health Industry Group,

Michael K. Brown
Partner, Los Angeles
+1 213 457 8018
mkbrown@reedsmith.com

Client Alert 09-262

September 2009

reedsmith.com

New HHS Regulations Impose Federal Security Breach Notification Requirements

Until recently, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") did not require a covered entity to notify individuals when their protected health information ("PHI") had been the subject of a security breach unless a particular individual requested an accounting from the covered entity. Furthermore, the vast majority of state security breach notification laws are often inapplicable to the types of security breaches suffered by covered entities and their business associates (e.g., many state security breach laws do not apply to the impermissible disclosure of only medical information). The recently enacted Health Information Technology for Economic and Clinical Health ("HITECH") Act, which amends various aspects of HIPAA (and therefore, the associated Privacy and Security Rules), marks a significant change in how covered entities and their business associates must respond to security breaches under HIPAA.[1]

On August 24, 2009, the United States Department of Health and Human Services ("HHS") issued its interim final rule ("HHS Rule," or the "Rule") regarding a covered entity's obligation to notify individuals when their unsecured PHI is breached. Furthermore, and depending on the nature of the security breach, the HHS Rule also requires a more global notification whereby covered entities must post information regarding certain breaches in newspapers and on the HHS website. Business associates, which will soon be subject to direct regulation and enforcement under HIPAA pursuant to the HITECH Act, will also need to be aware of the requirements within the HHS Rule regarding security breaches of unsecured PHI. Although the HHS Rule is effective on September 23, 2009, HHS will not impose sanctions for failure to provide the required notices for breaches that are discoverable before February 22, 2010.

Further complicating the efforts required of covered entities and business associates to meet the requirements of the new HHS Rule, the Federal Trade Commission ("FTC") has also issued regulations ("FTC Rule") addressing security breach notification with respect to entities that are not HIPAA-covered entities or business associates.[2] As reflected in the agency commentary accompanying the FTC regulations, there will likely be some confusion as to which of the new security breach notification standards certain businesses and individuals must follow.

This memorandum has three parts. First, it will address the applicability of the HHS Rule and associated definitions. Second, it will set forth the content and administrative requirements associated with breach notifications under the HHS Rule. Lastly, it will address the manner in which the FTC and HHS Rules interrelate.

A. Applicability of the HHS Rule

The new HHS Rule applies only to covered entities and their business associates that "access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information." Unlike the FTC Rule, which applies only electronic information, the HHS Rule applies to all types of unsecured PHI. Broken down into its key elements, the rule requires that (i) certain notifications are made, (ii) by covered entities and their business associates, (iii) that discover, (iv) an unauthorized acquisition, access, use, or disclosure (i.e., breach), (v) of unsecured, (vi) protected health information, (vii) so long as that breach compromises the security or privacy of the PHI.

1. Definition of Breach

The HHS rule defines "breach" to mean "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under the [the Privacy Rule] which compromises the security or privacy of the protected health information." There are two key aspects to this definition: (i) a violation of the Privacy Rule; and (ii) the compromise of the security or privacy of PHI.

a. Violation of the Privacy Rule

First, a breach must involve an action in violation of the HIPAA Privacy Rule. Without a Privacy Rule violation, the security breach notification requirements are not triggered. In particular, HHS commentary points to the fact that an impermissible use or disclosure of PHI that involves more than the "minimum necessary" information may qualify as a breach under the new HHS Rule. Because adherence to the minimum necessary standard,[3] which is widely considered to be the most ambiguous requirement of the Privacy Rule, requires the individual workforce members of a covered entity or business associate to demonstrate an effective working knowledge of the Privacy Rule, covered entities and business associates may want to view the new HHS Rule as a call to refocus privacy training efforts.

b. Creation of a "Harm" Threshold

Second, a breach must "compromise the security or privacy" of the PHI at issue. In response to industry commentary requesting that HHS address the extent to which a security breach notification would be triggered by a use or disclosure of PHI that does not pose some kind of harm to the individual, HHS added the definitional requirement that a breach must be found to compromise the security or privacy of PHI. To compromise the security or privacy of PHI, a breach must pose "significant risk of financial, reputational, or other harm to the individual." HHS emphasizes that such harm is not limited to economic loss.

In order to determine whether an impermissible use or disclosure of PHI meets this harm threshold, covered entities and their business associates will need to perform a risk assessment, which HHS believes will assist covered entities and business associates in determining whether a breach notification is required under the Rule.

A risk assessment should be fact specific, and include the following considerations:

- Who impermissibly used or disclosed the PHI?
- To whom was the PHI impermissibly disclosed? (If the PHI is disclosed to another covered entity or business associate, an argument can be made that the risk of further disclosure or inappropriate use is minimal.)
- Is it possible to obtain the recipient's satisfactory assurances that the impermissibly disclosed PHI will not be further used or disclosed, or will be destroyed?
- Has the impermissibly disclosed PHI been returned prior to it being accessed for an improper purpose?
- What is the nature of the PHI at issue? Does the impermissibly disclosed PHI contain financial or specific medical treatment information? (Because the definition of breach includes reputational harm, it is important to consider whether the mere disclosure of an individual's identity along with the name of a specialized treatment facility would constitute reputational damage.)

c. Unique Treatment of Limited Data Sets

With respect to the determination by a covered entity or a business associate as to whether a breach compromises the security or privacy of PHI, HHS has provided a narrow, explicit exception involving the use of Limited Data Sets. A Limited Data Set ("LDS") is defined by the HIPAA Privacy Rule to be PHI that excludes the following 16 direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) names; (ii) postal address information other than town or city, state, and zip code; (iii) telephone numbers; (iv) fax numbers; (v) electronic mail addresses; (vi) Social Security numbers; (vii) medical record numbers; (viii) health plan beneficiary numbers; (ix) account numbers; (x) certificate/license numbers; (xi) vehicle identifiers and serial numbers, including license plate numbers; (xii) device identifiers and serial numbers; (xiii) web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) biometric identifiers, including finger and voice prints; and (xvi) full-face photographic images and any comparable images.

PHI that has been stripped of the aforementioned 16 direct identifiers, however, is not "de-identified" for the purposes of HIPAA.[4] Although the HHS Guidance (defined below) does not include an LDS as a mechanism by which PHI may become secured (because of potential risk of re-identification of this information), the breach notification regulations permit covered entities and their business associates to forgo undertaking a risk assessment following the discovery of a potential breach of unsecured PHI if (i) information at issue constitutes an LDS; and (ii) the LDS does not include zip codes or dates of birth. Though a disclosure of an LDS that does not include zip codes and dates of birth is still technically a breach as defined by the Rule, HHS has, in this narrow instance, performed a de facto risk assessment on behalf of covered entities and business associates for this type of breach. As

such, notification is not required under the Rule. A risk assessment is still required, however, if the breach involves an LDS that includes zip codes or dates of birth.

2. Secured vs. Unsecured: HHS Offers a Safe Harbor to the Rule

The notifications required under the Rule must only be made if the breach involves "unsecured" PHI. Conversely, a breach of "secured" PHI does not trigger the new breach notification requirements. In determining the standards for what constitutes secured PHI, both the FTC and HHS Rules defer to recent HHS guidance[5] ("HHS Guidance") that details the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals. Furthermore, the HHS Rule includes an updated restatement of the initial HHS guidance. Generally, PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals if it has been encrypted or destroyed pursuant to various standards set by the National Institute of Standards and Technology.

Importantly, compliance with the HIPAA Security Rule is not directly tied to compliance with the breach notification requirements under the new HHS Rule. The Security Rule does not require covered entities and their business associates to employ encryption. The manner in which these entities protect the security of PHI is an addressable item under the Security Rule, and many entities choose a security method other than encryption. Therefore, it is likely that many covered entities and business associates will be compliant with the Security Rule and use and maintain PHI that does not meet the definition of "secured" PHI under the HHS Rule.

Although a covered entity or a business associate's compliance with the Privacy Rule is a threshold determination to the applicability of the HHS Rule, it is clear that an entity's de-identification of PHI does not qualify such information as "secured" PHI under the HHS Rule. Because the Rule views paper records as secured only if they have been destroyed, entities that use or disclose PHI in paper format are likely not able to take advantage of the safe harbor.

3. Exceptions to Breach

In addition to the safe harbor discussed above, the HHS Rule includes three exceptions to the definition of breach. Generally these exceptions contextualize certain types of unintended uses and disclosure of PHI. First, the Rule excludes from the definition of breach the unintentional acquisition, access, or use of PHI by an employee or workforce member of a covered entity or business associate if the employee or workforce member (i) is under the direct control of the entity; (ii) is acting under the authority of the entity at the time of an inadvertent use or disclosure; and (iii) the recipient of the PHI at issue does not further use or disclose the information in a manner not permitted under the Privacy Rule. For example, a breach notification is not required if an entity's employee (who has authority to access PHI) receives or views an email (meant for someone else within the entity) containing PHI (so long as the employee does not further use or disclose the PHI at issue).

The second exception is essentially the flip-side of the first exception. In other words, this exception addresses the inadvertent disclosure of unsecured PHI from one employee or workforce member (who is authorized to use and access PHI) to another similarly situated employee or workforce member at the entity, the entity's business associate, or an organized health care arrangement in which the entity is a member. This exception applies even if the two individuals at issue are not authorized to access the same type of PHI. As with the first exception, however, the exception only applies if the information at issue is not further used or disclosed.

The third exception addresses inadvertent disclosures to unauthorized individuals. If such a disclosure is made, notifications under the Rule are not required if the covered entity or business associate has a "good faith belief" that the unauthorized person to whom the disclosure was made would not have "reasonably been able to retain the information." Although it may be atypical for a covered entity or business associate to know, with any certainty, that a recipient is not able to retain the disclosed information, this exception will provide some reassurance to entities in certain narrowly defined situations. For example, a covered entity may send an explanation of benefits to the wrong individual. This inadvertent disclosure would typically trigger the breach notification requirements. However, if the explanation of benefits is returned to the covered entity unopened, the exception applies and notification is not required under the Rule.

4. Discovery of the Breach: Constructive Knowledge Standard Applies

The procedural components of the notification requirements, which are described below, are not triggered until a covered entity or business associate "discovers" a breach. Pursuant to the Rule, a covered entity or business associate is "deemed to have knowledge of a breach" if (i) the breach is

actually known; or (ii) the breach would have been known by any workforce member (other than the member who committed the breach) by exercising reasonable diligence.

B. Notification Mechanics; Roles of Covered Entities and Business Associates

In addition to the substantive issues addressed by the Rule, HHS imposes very specific, and in some cases, very onerous, technical notification obligations on covered entities and business associates.

1. Timeliness, Generally

Generally, a covered entity must send breach notifications to affected individuals "without unreasonable delay." Although the Rule also provides that notifications must be sent "in no case later than 60 calendar days" after the discovery of a breach, HHS commentary emphasizes that notification should not be unreasonably delayed and that entities should not systematically view the notification deadline as 60 days. HHS further underscores that the time period for breach notification begins upon discovery of the breach, and not when the investigation of the incident is complete, "even if it is initially unclear whether the incident constitutes a breach as defined in this [R]ule."

Business associates are required to provide breach notifications only to their covered entities. Such notification must be made without unreasonable delay and in no case later than 60 days. To the extent the information involved in a breach can be associated with a specific covered entity, only that covered entity must be notified by the business associate. If a breach is committed by the business associate, a covered entity's notification clock typically starts ticking from the moment the business associate notifies the covered entity about the breach. If, however, the business associate is an agent of the covered entity (according to the federal common law of agency), the covered entity is deemed to have knowledge of breach at the same time that the business associate first becomes aware of the breach.

As a result, and to the extent necessary, covered entities may want to review their legal relationships with their business associates and to assess whether it may be appropriate to include a provision in business associate agreements clearly identifying certain business associates as independent contractors. Additionally, covered entities and business associates may want to assess to what extent a business associate's notification timeframes should be addressed in business associate agreements.

2. Content of Notifications

Breach notifications must include the following information:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach (if known).
- A description of the types of unsecured PHI involved in the breach (e.g., full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, financial information). This description must be limited to the types of information disclosed, and should not include any actual patient identifying information.
- Any steps individuals should take to protect themselves from potential harm resulting from the breach.
- A brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
- Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an email address, a web site, or a postal address.

3. Methods of Notification; Notification Recipients

a. Notification to Individuals

As a general rule, covered entities are always required to provide written notification to an individual whose unsecured PHI was breached. The written notification must be sent by first-class mail to the last known address of the individual. There are, however, some exceptions to this general rule.

- **Email.** Email notification is permitted if the individual agrees in advance and such consent is not withdrawn.
- **Minors.** If the individual is a minor or otherwise lacks capacity under applicable state law, notice must be sent to the minor's parent or personal representative.

- **Deceased Individual.** Notice must be sent to the deceased individual's next of kin or personal representative, but only if (i) the covered entity knows the individual is deceased; and (ii) has the address of the next of kin or the personal representative.
- **Insufficient contact information.** If the covered entity does not have sufficient contact information for an individual (or a notice is returned as undeliverable), the covered entity must provide a substitute notice, which should be provided as soon as reasonably possible after the covered entity becomes aware that an individual's contact information is insufficient or out-of-date. The Rule provides two methods by which substitute notice may be provided. If there are fewer than 10 individuals to whom substitute notice must be sent, the covered entity may provide substitute notice "through an alternative form of written notice [e.g., email], by telephone, or by other means." For 10 or more individuals, however, substitute notice shall be provided to the individuals through (i) a conspicuous posting on the covered entity's website for a period of 90 days; or (ii) a conspicuous notice in major print or broadcast media in the geographic areas where the affected individuals are likely to reside. HHS also makes clear that a covered entity may attempt to update an individual's insufficient or out-of-date contact information, thereby enabling it to provide written notice by first-class mail.
- **Urgent Situations.** In addition to providing written notice by first-class mail, covered entities may contact an individual "by telephone or other means" if the breach of unsecured PHI appears to involve a possible imminent misuse of the information.

b. Notification to the Media

If a covered entity is aware of or reasonably believes that there has been a breach of the unsecured PHI of more than 500 residents of a state or jurisdiction, the covered entity must (i) notify the affected individuals under the general rule discussed above; and (ii) notify prominent media outlets that serve the geographic area of the affected individuals. The timeliness and content requirements applicable to the notice made to an individual also apply to notifications made to prominent media outlets.

c. Notification to the HHS Secretary

In addition to the aforementioned required notifications under the Rule, covered entities must notify the Secretary of HHS. If a breach involves 500 or more individuals (regardless of whether the breach is limited to a particular state or jurisdiction), the covered entity must notify HHS concurrent with the covered entity's notification to the individual. HHS will post on its website a list of covered entities that have reported breaches of unsecured PHI relating to 500 or more individuals. If a breach involves fewer than 500 individuals, the covered entity must maintain an internal log of such breaches and submit the log to HHS no later than 60 days after the end of each calendar year. HHS will post on its website the specific information that must be contained in a covered entity's internal log of security breaches.

d. Role of the Business Associate

The HHS Rule requires a business associate of a covered entity to notify the covered entity when the business associate discovers a breach of unsecured PHI provided by, or created for, the covered entity. Furthermore, the Rule imposes a maximum 60-day time period within which a business associate must notify its covered entity. To the extent that a covered entity would rather impose the notification obligations on its business associate, or otherwise clarify a business associate's role in addressing breaches, business associate agreements should be amended to address these issues. Additionally, business associates that utilize subcontractors to assist with the business associates' contractual obligations to a covered entity may want to include provisions in business associate subcontractor agreements that sufficiently address the business associate's expectations of a subcontractor if the subcontractor experiences a breach of PHI.

C. Interplay between the HHS and FTC Rules

1. Entities Regulated by both the HHS and FTC

A significant issue that many covered entities and business associates will face is determining the Rules with which they must comply. Many entities regulated by the FTC Rule (e.g., vendors of personal health records) may operate in a dual capacity. A vendor of personal health records may operate (i) independent of HIPAA-covered entities; and (ii) as a business associate of HIPAA-covered entities.[6] If a breach occurs, the vendor of personal health records may send an affected individual a breach notification under the FTC Rule, and notify the covered entity about the breach pursuant to the HHS Rule (whereby the covered entity will notify the affected individual as well).

HHS and the FTC agree that individuals should not receive duplicate notices for a single breach. Therefore, the FTC has agreed to view dual-regulated entities as in compliance with the FTC Rule if: (i) the entity provides breach notification to affected individuals on behalf of a HIPAA- covered entity; (ii) the entity has dealt directly with the affected individuals in managing their personal health records accounts; and (iii) the entity provides notification on behalf of the covered entity at the same time that notice is provided to affected direct consumers of the entity's services. In order for dual-regulated entities to comply with this exception to compliance with the FTC Rule, it is necessary that applicable business associate agreements provide for the dual-regulated entity to make the notifications otherwise required of the covered entity pursuant to the HHS Rule.

2. Applicability of the FTC Rule to Covered Entities

In most cases, the FTC Rule does not apply to HIPAA-covered entities or their business associates. However, to the extent that a covered entity is engaged in activities typically regulated by the FTC Rule and these activities are provided outside the scope of the covered entity's role as a covered entity, the FTC Rule applies. For example, a physician who offers personal health records to his patients and employees is governed by the HHS Rule because the personal health records are offered in the context of the physician's role as a covered entity/provider. If, however, a non-practicing physician operates a personal health records company, the physician is governed by the FTC Rule.

---

1 The HHS Rule, which can be found at 74 F.R. 42740 (August 24, 2009), defines covered entity, business associate, and protected health information through reference to the definitions set forth in HIPAA.

2 The FTC regulations, which were published in the Federal Register on August 25, 2009, address the manner in which security breaches must be handled by vendors of personal health records, PHR related entities, and third-party service providers. For more information regarding these types of entities and the specifics of the FTC rule, please see Reed Smith Alert 09-250, entitled "FTC Issues Final Rule on Notifying Consumers About Breaches of Electronic Health Records (September 3, 2009)."

3 The Privacy Rule requires that covered entities use and disclose only the "minimum necessary" amount of protected health information that is necessary for each particular function undertaken by the covered entity and its employees and contractors.

4 Protected health information that has been de-identified is no longer considered to be protected health information, and can be used or disclosed by a covered entity or business associate in any manner without running afoul of the Privacy or Security Rules.

5 The HHS Guidance can be found at 74 F.R. 19006 (April 27, 2009).

6 For instance, a vendor of personal health records, which offers personal health records directly to consumers, may also serve as a business associate of a health plan by offering personal health records to the plan's members as a benefit of being a member of the plan.

About Reed Smith

Reed Smith is a global relationship law firm with nearly 1,600 lawyers in 23 offices throughout the United States, Europe, Asia and the Middle East. Founded in 1877, the firm represents leading international businesses, from Fortune 100 corporations to mid-market and emerging enterprises. Its lawyers provide litigation services in multi-jurisdictional matters and other high-stakes disputes; deliver regulatory counsel; and execute the full range of strategic domestic and cross-border transactions. Reed Smith is a preeminent advisor to industries including financial services, life sciences, health care, advertising, technology, media, shipping, energy trade and commodities, real estate, manufacturing, and education. For more information, visit **reedsmith.com.**