SEPTEMBER 2009

New Interim Final Regulations Clarify HITECH's Breach of Health Information Notification Requirements

The Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), part of the American Recovery and Reinvestment Act of 2009, enhances the responsibilities that covered entities and business associates have under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). One of the HITECH Act's key requirements is that covered entities and business associates are now required to provide notification when there is a breach of protected health information ("PHI") that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through encryption or destruction [1] ("Unsecured PHI").

On August 24, 2009, the Department of Health and Human Services ("HHS") promulgated interim final regulations that clarify the responsibilities of covered entities and business associates when providing notification of a breach of Unsecured PHI ("Breach Notification Regulations"). The Breach Notification Regulations are effective September 23, 2009; however, HHS will not enforce the Breach Notification Regulations until February 22, 2010, so that covered entities and business associates have extra time to become compliant with the regulations. A summary of the key elements of the Breach Notification Regulations is provided below.

Definition of Breach

Covered entities are required to notify each individual whose Unsecured PHI has been or is reasonably believed to have been accessed, acquired, or disclosed as a result of a breach of Unsecured PHI ("Affected Individual"). A "breach" is defined as the acquisition, access, use or disclosure of PHI that (i) violates the HIPAA privacy rules and (ii) compromises the security or privacy of such PHI. When determining whether an impermissible use or disclosure compromises the security or privacy of PHI, covered entities and business associates will need to perform a risk assessment to determine whether the unauthorized use or disclosure poses a significant risk of financial, reputational, or other harm to the Affected Individual ("Risk Assessment"). The Risk Assessment should be a fact-specific analysis that varies with each impermissible use or disclosure. If a Risk Assessment reveals that there is less than a significant risk of harm as a result of the impermissible use or disclosure, then such use or disclosure is not a breach and no notice is required. Covered entities and business associates need to document their respective Risk Assessments so that they can demonstrate, if necessary, that no breach notification was required following an impermissible use or disclosure that does not satisfy the definition of a breach of Unsecured PHI under the Breach Notification Regulations.

The definition of "breach" excludes (i) any unintentional acquisition, access, or use of PHI by a workforce member or individual acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith, within the course and

scope of employment or other professional relationship, and does not result in further use or disclosure; (ii) any inadvertent disclosures from an individual who is otherwise authorized to access PHI at a facility operated by a covered entity or business associate to another individual authorized to access PHI at the same covered entity, business associate, or organized health care arrangement in which the covered entity participates and such information is not further used or disclosed without authorization; or (iii) situations in which the covered entity or business associate has a good faith belief that the unauthorized individual to whom PHI has been disclosed would not reasonably have been able to retain the information. In the event that a covered entity or business associate determines that an impermissible use or disclosure of Unsecured PHI satisfies an exception to the definition of breach, it must document the reasons why such use or disclosure satisfies the respective exception.

When a Breach is Considered "Discovered"

A breach is considered discovered by a covered entity as of the first day the breach is known to the covered entity or, by exercising reasonable diligence, would have been known to the covered entity. A covered entity is considered to have knowledge of a breach if any person (other than the person committing the breach) who is a workforce member or agent of the covered entity has knowledge of such breach. As such, covered entities should ensure that their workforce members and other agents receive adequate training and are aware of the importance of the timely reporting of privacy and security incidents and the consequences for failing to do so.

Notice Requirements

Covered entities must provide breach notices that are written in plain language and include:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

2. A description of the types of Unsecured PHI that were involved in the breach (i.e. full name, social security number, date of birth, home address, account number, diagnosis, disability code, etc.) without including a list of the actual PHI that was breached;

3. Any steps the Affected Individuals should take to protect themselves from potential harm resulting from the breach;

4. A brief description of what the covered entity is doing to investigate the breach, mitigate harm to the Affected Individual, and protect against any further breaches; and

5. Contact procedures that Affected Individuals can use to ask questions or learn additional information, including a toll-free telephone number, e-mail address, Web site, or postal address.

The notice must be sent to the Affected Individual by first-class mail (or by electronic mail if the Affected Individual has specified such preference) at the last known address of such individual or next of kin without unreasonable delay and in no case later than 60 days after the discovery of such breach. Where the Affected Individual is a minor or otherwise lacks legal capacity due to a physical or mental condition, notice must be given to the parent or other person who is the personal representative of the individual. Where the Affected Individual is deceased, notice must be sent to the last known address of the next of kin or personal representative but only if the covered entity knows the individual is deceased and already has the address of the next of kin or personal representative of the decedent.

Insufficient Contact Information

In the event that a covered entity does not have current contact information for one or more Affected Individuals, the covered entity must provide notification through a substitute form as soon as reasonably possible after the covered entity is aware that it has insufficient or out-of-date contact information. If there are fewer than 10 Affected Individuals for whom the covered entity has insufficient or out-of-date contact information, the covered entity may provide substitute notice through an alternative form of written notice, by telephone, or other means. If there are 10 or more Affected Individuals for whom the covered entity has insufficient or out-of-date contact information, the covered entity must provide a conspicuous posting for a period of 90 days on the

home page of its Web site or a conspicuous notice in major print or broadcast media in geographic areas where the Affected Individuals likely reside. Such conspicuous postings must include a toll-free telephone number, which remains active for 90 days, where individuals can learn whether their Unsecured PHI was included in the breach. In urgent cases where there is a possible imminent misuse of Unsecured PHI, covered entities can give notice by telephone or other means in addition to the written notice.

Notice to HHS and Media Outlets

Covered entities are required to maintain a log of any breaches that affect less than 500 Affected Individuals and annually submit such log to HHS no later than 60 days after the end of each calendar year. As for breaches that affect more than 500 Affected Individuals, a covered entity must notify HHS of such breach contemporaneously with the notice provided to the Affected Individuals. If there is a breach that affects more than 500 Affected Individuals that reside in the same state, the covered entity must provide notice to prominent media outlets serving the state in which the breach occurred without unreasonable delay and in no case later than 60 days after discovery of the breach, in addition to providing written notice to the Affected Individuals and notifying HHS of such breach. HHS will specify on its Web site the information that covered entities must submit to HHS and how such information should be submitted to HHS.

Policies and Procedures

Covered entities are required to implement policies and procedures that address their compliance with the following requirements:

1. Train workforce members regarding their responsibilities under the Breach Notification Regulations;

2. Provide a process for individuals to make complaints concerning the covered entity's obligations under the Breach Notification Regulations;

3. Apply appropriate sanctions against workforce members who fail to comply with the privacy policies and procedures of the covered entity or the Breach Notification Regulations;

4. Refrain from intimidating or retaliatory acts against an individual who files a complaint regarding the covered entity's compliance with the Breach Notification Regulations; and

5. Not require individuals to waive their rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Covered entities must maintain these policies and procedures for six years and make such policies and procedures available to HHS upon request. Business associates are required to implement policies and procedures to demonstrate their compliance with HIPAA's security rules and the additional requirements provided under the HITECH Act.

Business Associate Notice Requirements

Business associates are required to notify covered entities upon discovery of a breach of Unsecured PHI so that the covered entity can notify Affected Individuals of such breach. A breach is considered "discovered" by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate or to any person, other than the person committing the breach, who is an employee, officer, or agent of the business associate. The notice must be made without unreasonable delay and in no case later than 60 days after the discovery of the breach. The notice must include, to the extent possible, the identity of each individual whose Unsecured PHI has been, or is reasonably believed to have been, breached. Additionally, a business associate must provide the covered entity with any other available information that the covered entity is required to include in the notice to the Affected Individual, either at the time it provides notice to the covered entity or promptly thereafter as information becomes available. Business associates should provide a covered entity with the foregoing information even if it becomes available after notifications have been sent to Affected Individuals or after the 60-day period has elapsed.

Delaying Notice

Covered entities and business associates must delay providing notice if a law enforcement official determines that providing such notice would impede a criminal investigation or cause damage to national security. If the law enforcement official notifies the covered entity or business associate of the delay in writing and such notice includes the length of time that the notice must be delayed, then the covered entity or business associate must delay providing notice for the time specified. If the law enforcement official provides such notice orally, the covered entity or business associate must document the statement and identity of the official and delay notification for no longer than 30 days, unless the law enforcement official provides such entity with a written statement as provided above.

Other Applicable Laws

Covered entities and business associates may have additional obligations under other federal laws that require them to translate the notice required under the Breach Notification Regulations into frequently encountered languages and/or make such notice available in alternate formats (i.e., Braille, large print, or audio). In addition, many states, including Connecticut and Massachusetts, have statutes that require notice of data security breaches and such statutes may contain additional or different requirements than those provided under the Breach Notification Regulations.

Step-by-Step Analysis

HHS's commentary to the Breach Notification Regulations provides practical steps for covered entities and business associates to use when determining whether a breach of Unsecured PHI has occurred:

> *Step 1:* The covered entity or business associate must determine whether there has been an impermissible use or disclosure of PHI that would violate the HIPAA privacy rules.
>
> *Step 2:* The covered entity or business associate must determine, and document, whether the impermissible use or disclosure compromises the security or privacy of the PHI by performing a risk assessment to ascertain whether there is a significant risk of financial, reputational, or other harm to the individual.
>
> *Step 3:* The covered entity or business associate may need to determine whether the impermissible use or disclosure falls under one of the exceptions to the definition of "breach."

If, after making these determinations, the covered entity or business associate concludes there has been a breach of Unsecured PHI, the covered entity or business associate must provide the appropriate notice as required under the Breach Notification Regulations.

---

1 As required under the HITECH Act, HHS has issued guidance specifying that encryption and destruction are two technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals. Such guidance is available on the HHS Web site.

If you have any questions regarding how the Breach Notification Regulations affect your operations, please feel free to contact any member of Robinson & Cole's Health Law Group.

Robinson & Cole's Health Law Group includes:

Lisa M. Boyle	Theodore J. Tucci
Michael J. Kolosky	Karen P. Conway
B. Moses Vargas	Brian D. Nichols

Susan E. Roberts Kimberly E. Troland

The information in this update should not be considered legal advice. Consult your attorney before acting on anything contained herein.