

# Health Law Alert

## HIPAA Breach Notification Rules Effective September 23, 2009

Effective on September 23, 2009, HIPAA covered entities and their business associates must comply with new federal health information breach notification requirements. Published in the Federal Register on August 24<sup>th</sup> by the Department of Health and Human Services Office of Civil Rights (OCR), these new breach notification regulations are the first in a series of additions to existing HIPAA regulations mandated by the Health Information Technology for Economic and Clinical Health Act (HITECH).

Prior to HITECH, which was part of the federal stimulus law enacted on February 17, 2009, HIPAA covered entities had no legal obligation to notify individuals of breaches of protected health information (PHI) unless they were required to do so by state law, and business associates were not directly regulated under any of HIPAA's statutory or regulatory provisions. However, as of September 23<sup>rd</sup>, both HIPAA covered entities and their business associates must take specific actions to assess and respond to breaches of certain PHI. And while OCR indicated that enforcement of the breach notice rules will be delayed, the rules bring a significant compliance to-do list for covered entities and business associates.

### *Who must comply?*

The new breach notification rules apply to HIPAA "covered entities" and HIPAA "business associates." As background, HIPAA covered entities are primarily health care providers, including institutional and professional providers, and health plans, including group health plans and health insurance issuers. Health care clearinghouses that engage in certain data conversion activities are also covered entities under HIPAA. Business associates are persons or entities who perform services on behalf of a HIPAA covered entity and in so doing access the PHI of the covered entity.

While vendors of personal health records are also mandated by HITECH to provide notice of certain breaches of personal health records, such vendors who are not covered entities or business associates are subject to the FTC's breach notice regulations issued on August 18, 2009.

### *What is a breach?*

The breach notice rules apply when there is a breach of unsecured PHI. Key to successful compliance is an understanding of the meaning of "breach" and "unsecured PHI."

### *Breach*

HITECH defined "breach" as the acquisition, access, use or disclosure of PHI in a manner not permitted by HIPAA which compromises the security or privacy of the PHI. The breach notice rules define "compromises the security or privacy of the PHI" to mean posing a significant risk of financial, reputational or other harm to the individual. OCR provided insight in the preamble to the breach notice rules as to how to determine whether a breach of unsecured PHI has occurred: upon discovery of a breach, covered entities and business associates should undertake a risk assessment to determine if there is significant risk of harm to the individual as a result of the disclosure. OCR indicated a number of factors that could be assessed, including to whom the information was disclosed, whether mitigating steps were immediately taken when the breach was discovered, and the type and amount of PHI disclosed. Depending on the assessment of these and other factors, the risk of harm may or may not be eliminated or reduced to less than the "significant risk of financial, reputational or other harm" threshold required to establish a breach. Documentation of the risk assessment is required, according to OCR, because the breach notice rules impose the burden of proof on covered entities and business associates to show that no breach occurred if an impermissible use or disclosure did not pose significant risk of harm.

HITECH excluded from the definition of breach those disclosures of PHI where there is a good faith belief that the unauthorized recipient of the disclosure would not reasonably be able to retain the PHI. The breach notice rules also exclude from the definition of breach the unintentional acquisition, access or use of PHI inside a covered entity or business associate by a work force member if the acquisition was made in good faith and within the scope of authority and does not result in further impermissible uses or disclosures.

### *Unsecured PHI*

The breach notice rules do not apply to breaches of PHI that has been secured. HITECH addressed the issue of what makes PHI secure by defining "unsecured PHI" as PHI that is not secured through the use of a technology or methodology specified by the Secretary of Health and Human Services (Secretary), and by directing the Secretary to issue guidance on the technologies and methodologies that

render PHI unusable, unreadable or indecipherable to unauthorized individuals. The Secretary issued this guidance on April 27<sup>th</sup> which essentially directed that encryption and destruction of PHI are the only technologies/methods that meet the statutory requirement of rendering PHI unusable, unreadable or indecipherable to unauthorized individuals. Accordingly, the breach notice requirements are not triggered where the PHI involved is encrypted.

The breach notice rules republish the guidance, which can also be found at <http://www.hhs.gov/ocr/privacy/>, and clarify several issues related to securing PHI. In reiterating that encryption and destruction are the only acceptable technologies/methods that secure PHI for purposes of avoiding the breach notification requirements, OCR rejected including redaction of paper records and access controls, such as password protection, as acceptable security measures. OCR indicated that redaction and access controls do not meet the statutory criteria of rendering PHI unusable, unreadable or indecipherable to unauthorized individuals. The guidance also clarified that, in order to avoid breaching the confidential encryption or decryption process, decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt.

## ***Notice individuals, to the government, and to a covered entity by a business associate***

The breach notice rules implement the HITECH requirement that following the discovery of a breach of unsecured PHI, a covered entity must notify affected individuals whose unsecured PHI has been or is reasonably believed by the covered entity to have been accessed, acquired, used or disclosed as a result of the breach. Additionally, if the breach involves the information of 500 or more individuals, the covered entity must make immediate notification to the Secretary. The breach notice rules clarify “immediate” notice to the Secretary to mean notice that is provided concurrently with the notice provided to affected individuals. For breaches involving less than 500 individuals, the breach notice rules implement the HITECH requirement that the covered entity to maintain a log of such breaches and submit the log annually to the Secretary. OCR indicated in the preamble to the breach notice rules that for calendar year 2009, covered entities are required only to submit information to the Secretary related to breaches that occur after the September 23<sup>rd</sup> effective date of the regulations.

The breach notice rules also implement HITECH’s requirement that following a discovery of a breach of unsecured PHI, a business associate must notify the covered entity of the breach and must include the identification of each individual whose unsecured PHI was breached. The preamble to the breach notice rules clarifies that the business associate need only notify the covered entity to which the breached information relates, but if multiple covered entities are involved and it

is unclear to whom the information relates, the business associate must notify all potentially affected covered entities.

## ***Notice clock starts ticking with discovery of breach***

Covered entities are required under HITECH and the breach notice rules to provide notice without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. Likewise, business associates are required to notify covered entities without unreasonable delay and no later than 60 calendar days after discovery of a breach.

Breaches are treated as discovered 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. The breach notice rules provide that a covered entity is deemed to have knowledge about a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity under federal common law agency principles. OCR underscored in the preamble to the breach notice rules that knowledge of a breach by a workforce member is attributable to the covered entity. The importance of implementing reasonable systems for discoveries of breaches was also emphasized by OCR, because knowledge of a breach “starts the clock” on the time requirements for providing notice.

The same provisions for treating a breach as discovered apply to business associates. OCR further explained that the relationship between a covered entity and its business associate will drive the covered entity’s notice timing requirements. If a business associate is the agent of the covered entity, the business associate’s discovery of a breach will be imputed to the covered entity, and the timing of the notice will be based on the business associate’s discovery of the breach. This contrasts to an independent contractor relationship between a covered entity and a business associate in which the covered entity’s obligation to provide notice will be based on when the business associate notifies the covered entity of the breach.

## ***Form and content of notice***

The breach notice rules implement and clarify HITECH’s notice requirements.

### ***Individual notice***

Notice must be provided to individuals in writing by first-class mail or by email if the individual has specified a preference to receive electronic communications. Where the information of deceased individuals is involved in the breach, notice must be sent to the next of kin or to the individual’s personal representative if the covered entity both knows that the person is deceased and has the next of kin or personal representative’s contact information. In instances of

insufficient or out of date contact information, substitute notice is permitted; the rules require that substitute notice be reasonably calculated to reach the individuals for whom the notice is being provided. Substitute notice must take the form of a posting on the covered entity's web site home page or a notice in major print or broadcast media in cases where there is no current contact information for 10 or more people. Such substitute web site or media notices must continue for a 90-day period and include a phone number where an individual can learn whether his or her PHI was included in the breach.

HITECH requires that the content of the notice include a brief description of what happened, including the date of the breach and the date of the discovery of the breach, a description of the types of information involved in the breach, the steps that individuals should take to protect themselves from potential harm resulting from the breach, a description of the measures the covered entity is taking to investigate the breach and mitigate any harm, and contact information for individuals to ask further questions. The breach notice rules require that notices be written in plain language; to satisfy this requirement, OCR indicated that notices should be written at an appropriate reading level, in clear language and not include extraneous information that could diminish the message.

### *Media notice*

For breaches involving the unsecured PHI of more than 500 persons in a state or jurisdiction, covered entities are required by HITECH to provide notice to the media. The breach notice rules require that notification be made to prominent media outlets within 60 days of discovery of the breach and require the same content for media notices as for individual notices. OCR reiterated that the media notice requirement supplements, but does not replace, the individual notice requirements; therefore for breaches meeting the 500-person trigger, both media and individual notices must be provided.

### *Delayed enforcement of breach notice rules*

In recognition of concerns expressed regarding the short compliance time period, OCR indicated in the preamble to the breach notice rules that it will use its enforcement discretion to not impose sanctions for failure to provide breach notices for breaches that are discovered before February 22, 2010, 180 days from the publication of the rules. OCR suggested that this time period could assist covered entities to voluntarily choose to secure PHI in accordance with the guidelines in order to avoid the rules' requirements. OCR also suggested that covered entities could use the additional time to implement processes and procedures for compliance, including putting reasonable systems in place to detect breaches.

### *Much to do in little time*

Despite delayed enforcement of the breach notice rules, compliance is expected within weeks. Compliance checklists should include at least the following immediate steps:

- As with other HIPAA requirements, covered entities and now business associates must have specific policies and procedures for compliance with the new breach rules, and their workforce members must be trained on the new procedures;
- Risk assessment tools and processes should be developed to be quickly deployed, in order that a timely determination can be made and documented as to whether an incident meets the "significant risk of financial, reputational or other harm" threshold required to establish a breach;
- Template notice letters should be developed in order to avoid spending drafting time when the notice clock is ticking. Business associates should also develop forms to notify their covered entity customers of suspected breaches; and
- Covered entities and their business associates should confer with each other about expectations regarding fulfilling breach notification requirements. While both covered entities and business associates have independent obligations under the rules, consideration should be given to whether and to what extent existing and new business associate agreements should incorporate provisions on breach notification responsibilities.

– Katherine M. Keefe, Esq.

*For questions about this Health Law Alert or for assistance with health law issues, please contact:*

**Katherine M. Keefe, Esquire**

Phone: (610) 354-8270

[kmkeefe@mdwceg.com](mailto:kmkeefe@mdwceg.com)

