

Authors:**Patricia C. Shea**

patricia.shea@klgates.com
+1.717.231.5870

Richard P. Church

richard.church@klgates.com
+1.919.466.1187

Darlene S. Davis

darlene.davis@klgates.com
+1.919.466.1119

K&L Gates is a global law firm with lawyers in 33 offices located in North America, Europe, Asia and the Middle East, and represents numerous GLOBAL 500, FORTUNE 100, and FTSE 100 corporations, in addition to growth and middle market companies, entrepreneurs, capital market participants and public sector entities. For more information, visit www.klgates.com.

HIPAA Update: Breach Notification— Are You Prepared?

On August 24, 2009, the United States Department of Health and Human Services (“HHS”) published an interim final rule (the “Rule”) that establishes notification obligations for covered entities and their business associates for breaches of unsecured protected health information (“PHI”), as mandated by the Health Information Technology for Clinical Health (“HITECH”) Act.¹ The Rule also updates the guidance HHS issued in April 2009 on technologies and methodologies to make PHI unusable, unreadable, or indecipherable.

The Rule was effective September 23, 2009. However, HHS indicated that it will not impose sanctions for failure to provide the required notifications for breaches discovered before February 22, 2010. Nevertheless, as discussed below, covered entities must still report breaches of unsecured PHI that occur between September 23, 2009 and the end of the calendar year to HHS no later than March 1, 2010. Likewise, covered entities must also report breaches occurring between January 1, 2010 and February 22, 2010 on the following year’s report to HHS. And although HHS may not impose sanctions for not providing notification as specified in the Rule, HHS may nevertheless attempt to impose sanctions on a covered entity because the breach occurred in the first place.

When Is Notification Required?

As a threshold matter, the Rule applies only to a breach of unsecured PHI. “Unsecured PHI” means PHI that has not been made unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology approved by HHS. In the Rule, HHS explains that electronic PHI that is not encrypted according to the standards HHS specifies is unsecured PHI and is subject to the breach notification requirements. Conversely, a breach of PHI that has been encrypted according to HHS’ specifications would not trigger the notification requirements of the Rule. The Rule updates HHS’ guidance on how to secure PHI.

If the PHI is unsecured, the covered entity must determine whether a breach occurred. Under the Rule, a breach is the “acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the Privacy Rule] which compromises the security or privacy of the protected health information.”² Once a covered entity determines that the Privacy Rule has been violated, it then must determine whether the second part of this definition has been met. HHS indicates that the security or privacy of the PHI is compromised if the use or disclosure “poses a significant risk of financial, reputational, or other harm to the individual.”³ In making this determination, the covered entity should conduct a risk assessment and consider a variety of factors such as the identity of the person or entity that impermissibly used or received the PHI; steps the covered entity took to mitigate the potential for harm; whether the PHI was recovered prior to being accessed; the nature and scope of the PHI that was impermissibly used or disclosed; and whether the PHI was part of a limited data set.⁴

Additionally, three situations are statutorily excepted from the definition of a breach: (1) certain unintentional acquisition, access, or use of information by a workforce member or person acting under the authority of the covered entity; (2) certain inadvertent disclosures among persons similarly authorized to access PHI at the covered entity; or (3) where the recipient would not reasonably have been able to retain the information.⁵

A covered entity that determines that a breach did not occur based on its assessment that risk of harm was not significant or that an exception applies should maintain documentation supporting its determination, as HHS has indicated that the burden is on the entity to prove notification was not required.⁶

Who Must Be Notified?

Individual Notification.⁷ Covered entities must notify each individual whose unsecured PHI has been or is reasonably believed to have been breached. Unless delayed by law enforcement, notification is required without unreasonable delay and in no instance later than sixty (60) calendar days after discovery of the breach. A breach is considered discovered on the first day a covered entity knew or, by exercising reasonable diligence, would have known of the breach. Any workforce member's knowledge is attributable to the covered entity, unless that individual committed the breach. Further, HHS has indicated that covered entities are required to implement reasonable systems for the detection of breaches.

The individual notification should be written in plain language and include, to the extent possible: (1) a brief description of what happened, including the date of the breach and date it was discovered; (2) a description of the types of unsecured PHI involved in the breach; (3) steps individuals should take to mitigate potential harm; (4) steps the covered entity is taking to investigate the breach, mitigate harm, and protect against additional breaches; and (5) a contact person at the covered entity to receive questions or provide additional information. The covered entity is required to provide written notice by first-class mail to an individual's last known address or by email consistent with an individual's

agreement to receive electronic notice, if any. If an individual is deceased, the written notice must be sent to his or her next of kin or personal representative.⁸ Additionally, if a covered entity suspects imminent misuse of the PHI, individuals may also be contacted by telephone or other means.

If the covered entity has out-of-date or insufficient contact information for fewer than ten (10) individuals, the covered entity may provide substitute notice by either (1) an alternative form of written notice, (2) telephone, or (3) other means reasonably calculated to reach the individual. If ten (10) or more individuals cannot be contacted, the covered entity must provide notice through a conspicuous posting on its web-based home page for at least ninety (90) days or a conspicuous notice in major print or broadcast media in the geographic area where individuals affected by the breach likely reside. The post or media notice *must include a toll-free phone number active for at least ninety (90) days* for an individual to call to learn if his or her unsecured PHI might have been included in the breach.

Media Notification.⁹ In addition to providing notice to affected individuals, if more than 500 residents of a state or jurisdiction are affected by a breach, the covered entity must also notify prominent media outlets serving that state or jurisdiction. Unless delayed by law enforcement, such notification must be made without unreasonable delay and in no instance later than sixty (60) calendar days after the breach is discovered. The notification must include the same information identified above that is required in an individual notification as well as a toll-free contact number.

Notification to the Secretary.¹⁰ If 500 or more individuals are affected, unless delayed by law enforcement, the covered entity must also notify the HHS Secretary concurrently with the notifications sent to individuals. HHS will post information about such large breach notices on its website. For breaches that involve fewer than 500 individuals, the covered entity must maintain a log or other documentation identifying each breach and submit a report on each breach to HHS within sixty (60) days after the end of the calendar year in the format specified by HHS. HHS has recently posted a reporting form on its website for covered

entities to report breaches affecting any number of individuals.¹¹ To make certain that the annual reports of breaches include all necessary information about each breach, covered entities should look to the form on the HHS website to develop a complete log or other running documentation on breaches involving less than 500 individuals.

Breaches Discovered by Business Associates

Under the Rule, covered entities must also provide notice of breaches discovered by their business associates. When determining whether a breach has occurred, business associates follow the same process described above for covered entities. HHS indicates that the required notices under the Rule may come directly from the business associate pursuant to an agreement with a covered entity or the business associate may report such breaches to the covered entity, which will in turn provide the required notices under the Rule.

In the latter instance, the business associate must notify the affected covered entity of a breach without unreasonable delay and in no instance more than sixty (60) days after the breach is discovered. If the business associate is an agent of the covered entity (determined in accordance with the federal common law of agency), the date of discovery for the covered entity is considered to be the date the business associate knew or should have known of the breach. If the business associate is not deemed an agent of the covered entity, the covered entity may treat the date on which the business associate provided it notice as its date of discovery.¹²

What Should Covered Entities and Business Associates Be Doing Before the Compliance Deadline?

While the Rule is currently effective and covered entities and business associates must comply with its requirements, HHS has indicated that it will not impose sanctions under the Rule until February 22, 2010. During this period, covered entities should:

1. Develop and adopt a breach notification policy consistent with the Rule, including procedures to detect breaches;
2. Conduct workforce training on breach detection and notification¹³;
3. Assess the adequacy of breach notification requirements in existing and new business associates agreements, and modify as appropriate;
4. Log breaches affecting fewer than 500 individuals that occur after September 23, 2009 for reporting to HHS annually within the first 60 days of each calendar year; and
5. To the extent possible, begin implementing notification procedures to individuals, and for breaches involving more than 500 individuals, to the media and HHS so that the workforce is familiar with the process before the enforcement period begins.

Additionally, many states have implemented privacy and security requirements related to sensitive health or consumer information that may also have breach notification requirements. Covered entities should confirm that policies and procedures implemented under the Rule are consistent with all state or federal requirements that may otherwise be applicable to the covered entity.

Anchorage Austin Beijing Berlin Boston Charlotte Chicago Dallas Dubai Fort Worth Frankfurt Harrisburg Hong Kong London
Los Angeles Miami Newark New York Orange County Palo Alto Paris Pittsburgh Portland Raleigh Research Triangle Park
San Diego San Francisco Seattle Shanghai Singapore Spokane/Coeur d'Alene Taipei Washington, D.C.

K&L Gates is a global law firm with lawyers in 33 offices located in North America, Europe, Asia and the Middle East, and represents numerous GLOBAL 500, FORTUNE 100, and FTSE 100 corporations, in addition to growth and middle market companies, entrepreneurs, capital market participants and public sector entities. For more information, visit www.klgates.com.

K&L Gates comprises multiple affiliated partnerships: a limited liability partnership with the full name K&L Gates LLP qualified in Delaware and maintaining offices throughout the United States, in Berlin and Frankfurt, Germany, in Beijing (K&L Gates LLP Beijing Representative Office), in Dubai, U.A.E., in Shanghai (K&L Gates LLP Shanghai Representative Office), and in Singapore; a limited liability partnership (also named K&L Gates LLP) incorporated in England and maintaining offices in London and Paris; a Taiwan general partnership (K&L Gates) maintaining an office in Taipei; and a Hong Kong general partnership (K&L Gates, Solicitors) maintaining an office in Hong Kong. K&L Gates maintains appropriate registrations in the jurisdictions in which its offices are located. A list of the partners in each entity is available for inspection at any K&L Gates office.

This publication is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer.

©2009 K&L Gates LLP. All Rights Reserved.

¹ Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740 (Aug. 24, 2009).

² 45 C.F.R. § 164.402.

³ *Id.*

⁴ If a limited data set also excluded zip codes and dates of birth, HHS has deemed that the covered entity may conclude that no breach occurred.

⁵ 45 C.F.R. § 164.402.

⁶ *See id.* § 164.414.

⁷ *See id.* § 164.404.

⁸ The requirements for substitute notice do not apply to next of kin or personal representatives.

⁹ *See* 45 C.F.R. § 164.406.

¹⁰ *See id.* § 164.408.

¹¹ *See*

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html>.

¹² *See* 45 C.F.R. § 164.410.

¹³ *See id.* § 164.414.