

Client Alert

Latham & Watkins
Health Care Practice

HHS Issues New HIPAA Breach Notification Rules

Summary

The Health Information Technology for Economic and Clinical Health Act (HITECH), which is part of the American Recovery and Reinvestment Act of 2009, significantly expanded the privacy and security law requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Among these expansions is a requirement that HIPAA-covered entities provide notification to affected individuals and various entities in the event "unsecured" protected health information (PHI) is subject to a "breach." Previously, HIPAA only required covered entities to mitigate any known harm in the event of such a breach, but did not expressly require such entities to notify anyone.

On August 24, 2009, the US Department of Health and Human Services (HHS) issued a new regulation clarifying these breach notification obligations. The rule requires HIPAA-covered entities to notify affected individuals whose unsecured PHI is the subject of a breach. Covered entities will also have to notify HHS, and potentially the media, in the event of a breach. The rule also requires business associates of covered entities to report such breaches to the covered entities. The rule will apply to all breaches of unsecured PHI discovered after September 23,

2009, although covered entities will be afforded additional time to comply.

This rule has broad implications for HIPAA-covered entities and their business associates, and may require them to restructure their employee training, breach-discovery and breach-notification methodologies.

The Federal Trade Commission's (FTC) companion rule, issued on August 17, 2009, addresses breach notification obligations for certain non-HIPAA covered entities, and is summarized here: [Client Alert 928](#).

Types of Breaches Subject to the Rule

The rule applies in the event of a "breach" of "unsecured" PHI. A "breach" is defined as "the acquisition, access, use, or disclosure" of PHI in a manner not permitted under HIPAA, which "compromises the security and privacy of the [PHI]." The phrase "compromises the security and privacy of the [PHI]" is, in turn, defined to mean that it "poses a significant risk of financial, reputational, or other harm to the individual." This risk of harm standard qualifies the meaning of breach and requires an assessment of harm as part of determining what notification obligations apply, as discussed in greater detail in this *Alert*.

"This rule has broad implications for HIPAA-covered entities and their business associates, and may require them to restructure their employee training, breach-discovery and breach-notification methodologies."

HITECH defines "unsecured" as health information that is not secured through the use of technology or methodology that renders this information unusable, unreadable or indecipherable to unauthorized individuals. On April 17, 2009, HHS issued guidance identifying encryption and destruction as the two technologies and methodologies that render health information unusable, unreadable or indecipherable to unauthorized individuals. Therefore, covered entities and business associates can avoid the rule's notification requirements by sufficiently encrypting or destroying the health information in their possession.

Obligation to Discover Breaches and Train Employees/Agents

The rule does not establish a security standard for covered entities and their business associates. However, HHS will consider an entity in violation of the rule if it fails to discover a breach when reasonable diligence would have led to discovery of the breach. Therefore, HHS expects covered entities and business associates to establish breach-detection software and other methodologies. The use of such methodologies will factor into HHS' determination of whether an entity violated the rule when it failed to promptly discover a breach of PHI.

In addition, the rule attributes knowledge of a breach by a "workforce member" or other agent of the entity to the entity itself. Knowledge by an employee is imputed to the employer. Therefore, HHS requires entities to train their employees and agents in breach discovery and timely reporting of breaches of security. HHS also directs covered entities to use sanctions against members of its workforce who fail to comply with the entity's privacy policies.

Breach Determination

Upon discovering a potential breach, HHS envisions entities undertaking a three-step determination of whether a breach has in fact occurred and must be reported.

Has there been a violation of the Privacy Rule?

First, an entity must determine if the incident constitutes a violation of the HIPAA Privacy Rule. Access, acquisition, use or disclosure of unsecured PHI triggers notification only if it also violates the Privacy Rule. Not all use or disclosure violates the Privacy Rule. For example, a use or disclosure of PHI incident to a permissible use or disclosure that occurs despite reasonable safeguards would not violate the Privacy Rule, and thus would not qualify as a breach requiring notification to individuals.

Does this violation of the Privacy Rule compromise the privacy or security of an individual's protected health information?

Next, the rule requires entities to consider whether the violation of the Privacy Rule "compromises the security of the protected health information." A violation compromises the security of PHI if it "poses a significant risk of financial, reputational, or other harm to the individual." This prong of the breach determination process encompasses the "harm threshold" noticeably absent from the FTC companion rule. In short, if the unauthorized use or disclosure of an individual's PHI will not likely harm the individual, covered entities do not have to notify the individual.

HHS provides some examples of when unauthorized disclosure does not compromise the security of protected health information. If, for example, a covered entity accidentally releases PHI to another entity subject to HIPAA, harm to protected individuals is minimal, because the recipient of the PHI is

also obligated by HIPAA to maintain the privacy of protected individuals. Likewise, consider the example of an employee leaving his/her laptop in a public place. If the laptop is returned before an unauthorized individual has an opportunity to view the files, harm to the protected individuals is negligible, and thus notification is unnecessary.

Also, according to the rule, unauthorized disclosure does not compromise the security of PHI if it does not include date of birth, zip code, or the identifiers listed in HIPAA § 164.514(e)(2) (*e.g.*, name, certain postal address information, telephone number, fax number, Social Security number, e-mail address, medical record number, health plan beneficiary member, account number, certificate/license number, vehicle identifier/serial number, device identifier/serial number, URL, IP address, biometric identifier, facial photographic images). In effect, this provision delineates what is already stated within the rule: health information is not protected unless it includes identifiers linking it to a particular individual.

It should be noted that the burden rests on the entity to show that a use or disclosure does not pose a risk to protected individuals. Therefore, to use the laptop example, an entity must show persuasively that the laptop's files were not opened, altered or otherwise transferred. If it cannot, it must follow the notification requirement. HHS encourages entities to document their risk assessments so they can show at a later time that notification was not necessary.

Does the Incident Fall Under One of the Exceptions Permitted by the Rule?

Lastly, an entity must determine if the incident falls under one of the exceptions permitted by the rule. The rule provides three exceptions.

First, breach has not occurred if a workforce member unintentionally acquires, accesses or uses PHI, provided such acquisition, access or use was made in good faith, within the scope of employment and does not result in further use or disclosure. HHS provides the example of a hospital billing clerk. If the clerk receives an e-mail including PHI, inadvertently sent to him by a nurse, promptly informs the nurse of her mistake and deletes the e-mail, no breach has occurred. The billing clerk's use of the PHI was inadvertent, done in good faith, within the scope of his employment and led to no further disclosure. Thus, notification of the protected individual would not be required.

Second, breach has not occurred if an authorized person inadvertently discloses PHI to another authorized person within the same entity, provided the PHI disclosed is not further used or disclosed in a manner violative of the Privacy Rule. For example, if a doctor discloses PHI to a nurse in the same hospital, no breach has occurred, provided the nurse does not disclose the PHI to an unauthorized individual.

Third, breach has not occurred if an entity discloses PHI to an unauthorized recipient, provided the entity has a good faith belief that the recipient would not be able to retain the information. HHS provides the example of a nurse who inadvertently hands discharge papers to the wrong patient. If the nurse quickly recognizes her mistake and retrieves the papers before the patient had an opportunity to read and retain the information within them, breach has not occurred, and notification is not necessary.

If an incident violates the Privacy Rule in a manner that compromises the privacy or security of an individual's protected health information, and does not fall within one of these stated exceptions, then it constitutes a breach. The covered entity or business associate must then follow the rule's notification requirements.

Notification Requirements

Discovery by a Covered Entity

Following discovery of a breach, a covered entity must notify all individuals whose information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used or disclosed as a result of the breach. A breach is deemed to be discovered on the first day on which the breach is known by the covered entity, or, by exercising reasonable diligence, would have been known by the covered entity. Written notification must be made in plain language by first-class mail, unless the consumer has agreed to notification by e-mail.

Notice must include, to the extent possible:

- an explanation of the breach,
- a description of the types of unsecured PHI that likely were involved in the breach,
- steps individuals should take to protect themselves from harm resulting from the breach,
- an explanation of what the entity is doing to investigate the breach, mitigate its harm and protect against further breaches, and
- contact information individuals can use to ask questions or learn more.

If the entity lacks sufficient contact information to affect notice, the entity must provide substitute notice reasonably calculated to reach the individual. If the entity lacks contact information for 10 or more individuals, substitute notice must come in the form of:

- a posting on the home page of the entity's Web site for a period of 90 days or conspicuous notice in major print or broadcast media in the geographic areas where affected individuals reside, and must include a toll-free number that remains active for 90 days and through which an individual can learn if his/her information is likely included in the breach.

Covered entities must notify individuals promptly, without "unreasonable delay," and in no case more than 60 calendar days after discovery of the breach.

In addition, covered entities must notify major media outlets in all states or jurisdictions in which 500 or more residents were compromised by the breach.

Likewise, if a breach involves 500 or more individuals, a covered entity must notify HHS contemporaneously with its notification to individuals. If fewer individuals were involved in the breach, covered entities can wait to notify HHS at the end of the calendar year.

Discovery by a Business Associate

If a business associate discovers a breach, it must notify the covered entity of the breach in a timely manner, in no case more than 60 days after discovery of the breach. A business associate must include the identity of all individuals believed to be compromised by the breach, and should include all of the information that the covered entity will need to relay notice of the breach to the impacted individuals.

If, as a matter of agency law, a business associate is an "agent" of the covered entity, knowledge of the breach by the business associate will be imputed to the covered entity. In such a case, the covered entity's timeline for notification to individuals starts on the day when the business associate discovered the breach.

If, on the other hand, the business associate serves only as an "independent contractor" of the covered entity, knowledge will not be imputed to the covered entity, and the clock for notifying individuals will not start until the covered entity receives notice of the breach from the business associate.

Interaction with State Laws

The rule's notification requirements preempt contrary state laws. State law

is contrary to this rule if it would be impossible to comply with both the state law and the rule, or if the state law is an impediment to enforcement of the rule. If state law is consistent with this rule, then entities must comply with both.

Many states have laws governing notification of individuals in the event of a breach of security. Covered entities will have to analyze relevant state law to identify conflicts in the event of a breach.

Effective Date and Sunset of The Rule

The rule will take effect on the date 30 days after the date of publication of this rule in the Federal Register (September 23, 2009) and applies to breaches of security discovered on or after that date. HHS will not begin enforcement until 180 days after publication, the middle of February 2010.

Application of this rule is expected to be temporary, as HITECH commits Congress to enact legislation on

health breach notification. Congress is currently awaiting recommendations by FTC and HHS and will then begin to consider federal legislation on this subject matter.

If you have any questions about this *Client Alert*, please contact one of the authors listed below or the Latham attorney with whom you normally consult:

W. Andrew H. Gantt III

+1.202.637.2259
andrew.gantt@lw.com
Washington, D.C.

Micah Schwartz*

+1.202.637.2362
micah.schwartz@lw.com
Washington, D.C.

**Licensed to practice law in Virginia only; all work directly supervised by a member of the District of Columbia Bar.*

Client Alert is published by Latham & Watkins as a news reporting service to clients and other friends. The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the attorney whom you normally consult. A complete list of our *Client Alerts* can be found on our Web site at www.lw.com.

If you wish to update your contact details or customize the information you receive from Latham & Watkins, please visit www.lw.com/LathamMail.aspx to subscribe to our global client mailings program.

Abu Dhabi

Barcelona

Brussels

Chicago

Doha

Dubai

Frankfurt

Hamburg

Hong Kong

London

Los Angeles

Madrid

Milan

Moscow

Munich

New Jersey

New York

Orange County

Paris

Rome

San Diego

San Francisco

Shanghai

Silicon Valley

Singapore

Tokyo

Washington, D.C.