



## Breaches of Unsecured Protected Health Information

On August 24, 2009, the Office of Civil Rights (“OCR”) of the Department of Health and Human Services (“HHS”) published an interim final rule specifying when an individual must be notified of unauthorized use or disclosure of the individual’s protected health information (“PHI”). The regulations apply to “covered entities” (most health care providers, health plans, and health care clearinghouses) and their business associates. Currently under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), covered entities, and by contract, their business associates, must keep a record of unauthorized use or disclosure of PHI but are only required to provide the information if asked by the individual. However, HIPAA amendments enacted in the HITECH ACT portion of the American Recovery and Reinvestment Act of 2009 (also known as the Stimulus Bill) require notification if there is a breach of unsecured PHI.

Notice is required when there is an unauthorized use or disclosure (including acquisition or access) of PHI that poses a significant risk of financial, reputational, or other harm to the individual, termed a “breach” of PHI. Because the unauthorized use or disclosure only constitutes a “breach” if there is a significant risk of harm to the individual, if unsecured PHI is improperly accessed, acquired, used or disclosed, a covered entity will have to conduct a risk assessment to determine if there is a significant risk of harm. The rule also includes guidance specifying technology and other methodology that is deemed to render PHI secured.

Breach notifications required by the HITECH ACT are onerous. Notification is expensive and may require public disclosure with the risk of reputational harm to the covered entity and/or business associate. Covered entities and business associates should assess whether their systems meet the technology and methodology specifications and, if not, consider whether it would be prudent to adopt the HHS specifications.

The regulations become effective September 23, 2009, although OCR will not enforce civil monetary penalties for non-compliance until February 22, 2010. Until the February date, OCR will work with covered entities to achieve compliance through technical assistance and voluntary corrective action.

### Notification Requirements

#### *Time for Notice*

If there is a breach of unsecured PHI, affected individuals must be notified “without unreasonable delay” but in no event more than 60 days after discovery of the breach. Discovery is the actual date of discovery or the date on which the covered entity would have known of the breach if it had been diligent. Covered entities and business associates will have to institute system monitoring to know if a breach has occurred. The time period needed to assess the breach does not extend the 60-day time limit for notification and the time runs from the time of the breach and not from the time when the covered entity finishes its assessment of the impermissible use or disclosure.

CHARLOTTE

CHICAGO

GENEVA

HONG KONG

LONDON

LOS ANGELES

MOSCOW

NEW YORK

NEWARK

PARIS

SAN FRANCISCO

WASHINGTON, D.C.

The regulations do not give a covered entity a blanket 60 days in which to provide notice. Because notice must be given without unreasonable delay with a cap of 60 days, notice must be given as soon as the covered entity has sufficient information to provide notification.

The regulations permit a delay beyond the 60-day notice limit if required or requested by law enforcement in order to investigate a crime. If an oral request is made, the covered entity must document the request and if the delay will last more than 30 days, the covered entity must obtain a written request.

### ***Notice Content***

Notification must include a brief description of what happened; a description of the type of unsecured PHI involved (*e.g.*, full name, SSN, date of birth, address, account number, diagnosis); steps the individual should take to protect against potential harm from the breach; a brief description of what the covered entity is doing to investigate the breach, mitigate harm to individuals, and protect against further breaches; and how the individual may contact someone at the covered entity for more information.

### ***Method of Notification***

Notice must be given by first class mail at the individual's last known address (unless email notification is agreed to in advance). If the covered entity does not have current contact information it must use a substitute method for contacting those individuals. For fewer than 10 individuals it may use another reasonable method, such as telephone. If it does not have current contact information for 10 or more individuals, the covered entity must post a notice on its web site for at least 90 days or place a conspicuous notice in a major newspaper or with broadcast media in the area, which must include a toll-free number to call for more information.

In addition to all of the above, if the breach involves more than 500 residents of a state or jurisdiction, the covered entity must notify prominent media outlets. Notice must also be given to HHS. If the breach involves fewer than 500 individuals, the covered entity must maintain a log of the breaches and, within 60 days after the end of each calendar year, notify HHS of these breaches. If 500 or more individuals are affected (no matter the number of jurisdictions), the covered entity must notify HHS at the same time that notice is made to individuals. HHS will post a list of breaches on its web site.

If the breach occurs at the business associate level, the business associate must make notice to the covered entity so that the covered entity may fulfill the notice requirements.

## **Technology and other Methodology to Secure PHI**

HHS has established standards that if followed render PHI secured and not subject to notice if breached.

### ***PHI in Hard Copy Form***

When discarded, PHI that is maintained in paper, film, or other hard-copy form, must be shredded or otherwise destroyed so that it cannot be reconstructed or it will be deemed "unsecured" if breached. Redaction does not suffice. Only upon destruction is hard copy PHI rendered secured.

### ***PHI in Electronic Form***

PHI in electronic form must be encrypted in accordance with standards approved by HHS. Otherwise notice will be required if the electronic PHI is breached. Firewalls, although still advisable, are not sufficient to secure electronic PHI. The regulations divide electronic PHI into three categories for standards: (i) data in motion (data that is being transmitted); (ii) data at rest (*e.g.*, data in a server, on a hard drive, on a flash drive); and (iii) data disposed (data that has been discarded or recycled).<sup>1</sup> To be deemed secured, each category of data must be encrypted consistent with standards established by the National Institute of Standards ("NIST"). Data at rest must be encrypted in accordance with standards in NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices. Data in motion must be encrypted in accordance with standards in NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated. Data that is disposed must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved. All NIST publications are available at <http://www.csrc.nist.gov/>. In addition, encryption keys must be kept on a separate device from the encrypted data.

## **What Constitutes a Breach**

In order for there to be a breach, what is disclosed or acquired must be PHI; the use or disclosure must be unauthorized; and it must compromise the security or privacy of the PHI.

### ***Unauthorized Use or Disclosure***

A breach only may occur if the unauthorized use or disclosure violates the HIPAA Privacy Rule. OCR cautions that if a covered entity or business associate discloses more than the minimum necessary PHI, a violation would occur, and, depending on

<sup>1</sup> The rule introduces a fourth category, data in use, which is data in the process of being created, retrieved, updated, or deleted, but does not provide a standard for encryption.

the circumstances, it may constitute a breach. In contrast, an incidental disclosure, that occurs in conjunction with a permitted use or disclosure, even with reasonable safeguards in place, would not be a violation of the Privacy Rule and, therefore, not a breach. For example, if a physician asks a nurse to call a patient, and the physician has taken reasonable precautions to assure that the conversation will not be overheard, if despite these precautions someone overhears the conversation, there would not be a violation of the Privacy Rule and, therefore, a breach would not occur. In addition, a violation of the Privacy Rule by itself would not be a breach, unless it led to an impermissible use or disclosure that would constitute a breach. For example, if a patient's chart is left on a desk but no unauthorized person reads it, there is no breach.

### ***Exceptions to a Breach***

Even if the use or disclosure is impermissible, the regulations create three further exceptions to the definition of "breach." The first is the acquisition, access, or use made by an employee, or someone else under the authority of the covered entity or business associate that was unintentional and made in good faith within the scope of employment or other relationship, and without any further use or disclosure not permitted by the Privacy Rule. An example is misdirected emails within the covered entity. In contrast, access by an employee curious about a neighbor's condition would not meet the exception.

The second is an inadvertent disclosure by an individual at a covered entity, business associate, or organized health care arrangement who is authorized to have access to the disclosed PHI, made to another individual at the same covered entity, business associate, or organized health care arrangement, who is also authorized to access PHI (even if not authorized to access that PHI) if the PHI is not further used or disclosed in a manner not permitted by the Privacy Rule. An example would be a physician at a hospital inadvertently giving the wrong chart to a nurse whose responsibilities do not include that patient.

The third exception pertains to situations where the covered entity or business associate has a good faith belief that the unauthorized recipient of the PHI would not have been able to retain the PHI. An example given is an EOB sent to the wrong individual that is returned unopened.

### ***Risk Assessment***

In order to determine whether notification of individuals is required, the covered entity or business associate will have to engage in a four-part risk assessment. If challenged, the covered entity will bear the burden of proof that notification was not required. Therefore, it is important to document the risk assessment. First, a determination of whether there is an impermissible use or

disclosure of PHI; second, whether the PHI was secured; third, whether any of the breach exceptions apply; and fourth, whether there is a significant risk of financial, reputational, or other harm to the individual.

In considering the fourth part of the test, HHS advises that among the factors to consider are the following: (i) who improperly used or received the PHI (receipt by another covered entity subject to HIPAA likely would not pose much risk); (ii) whether the harm can be mitigated (*e.g.*, through some sort of confidentiality agreement with the recipient); (iii) whether the PHI is returned prior to access (*e.g.*, mail is returned unopened, a lost laptop is not opened or otherwise accessed); (iv) whether the PHI is returned before it is used for an improper purpose; (v) whether the covered entity or business associate can mitigate the risk by receiving satisfactory assurances that there will be no further use or disclosure or that the PHI will be destroyed; (vi) whether the type or amount of information would not pose significant risk (*e.g.*, if the information were the name of the individual and the fact that she had a cavity filled or a root canal would not seem to meet the threshold for harm); and (vii) if the PHI disclosed is a limited data set, the likelihood that any individual in the database could be identified. The preamble also suggests looking at OMB Memorandum M-07-16, which is available at <http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf>, for factors to be considered in determining significant risk of harm to the individual.

### **State Law Pre-emption**

Unlike most federal law, HIPAA does not pre-empt (take the place of) state privacy law. It is important to note that state law pre-emption still applies if the state law is more stringent than HIPAA or if the state law imposes additional requirements. If HIPAA does not require notification, it may be required by state law. Some state laws require notification of the state attorney general, others require notification of the media in circumstances that are different from the HIPAA requirement, and some states require additional information in the notice. State law is only pre-empted if it is impossible to meet both HIPAA requirements and the state law requirements, and then, only to those parts that conflict.

### **Submission of Comments**

Because this is an interim final rule, OCR will accept comments. As required, OCR estimates the time burden on covered entities to collect information required by the regulations. We have not provided that information in this briefing but will provide that information on request. Comments on those estimates are due by September 8, 2009. All comments on the substance of the rule are due by October 23, 2009.

The Health Care Practice Group of Winston & Strawn represents a broad range of health care entities on all regulatory matters. If you have any questions regarding the matters discussed in this briefing, if you need assistance in preparing comments to HHS regarding the interim final rule, or if you need assistance in developing and/or reviewing compliance plans, systems, controls and/or procedures relating to the matters covered in this briefing, please contact either of the Winston & Strawn attorneys listed below or your usual Winston & Strawn contact:

Tom Mills	<a href="mailto:tmills@winston.com">tmills@winston.com</a>	(202) 282-5714
Marion Kristal Goldberg	<a href="mailto:mgoldberg@winston.com">mgoldberg@winston.com</a>	(202) 282-5788

---

*These materials have been prepared by Winston & Strawn LLP for informational purposes only. These materials do not constitute legal advice and cannot be relied upon by any taxpayer for the purpose of avoiding penalties imposed under the Internal Revenue Code. Receipt of this information does not create an attorney-client relationship. No reproduction or redistribution without written permission of Winston & Strawn LLP.*

© 2009 Winston & Strawn LLP.

---