

Interim Final Rule: Breaches of Unsecured Protected Health Information (PHI)

On August 24, 2009, the Department of Health and Human Services (HHS) published an interim final rule with a request for comments that requires *covered entities* and their *business associates* [as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)] to notify affected individuals, the Secretary of HHS, and the media of a breach of unsecured protected health information (PHI) under specified conditions. In light of this rule, health care providers and entities working with PHI will need to revise their policies and procedures and train their employees and contractors on the notification requirements set by HHS. You will also need a strategy for media notification should any breach ever occur. These notification requirements are effective for any breach occurring on or after September 23, 2009 and are publicly available [here](#).

The interim final rule adopts definitions for *breach* and *unsecured protected health information*, while providing specific requirements for notification of a breach of unsecured PHI. A *breach* includes the acquisition, access, use, or disclosure of PHI that is not permitted under HIPAA and poses a significant risk of financial, reputational, or other harm to an individual. The rule recognizes limited exceptions for *unintentional* and *inadvertent* acquisition, use, access, or disclosure of PHI in certain circumstances, as well as an exception for unauthorized disclosures in which an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information. Discovery of a *breach* is deemed to occur when it is known or should have been known by the covered entity if reasonable diligence had been exercised.

All notifications required by the interim final rule must be made “without unreasonable delay” which is further explained as within 60 days of discovery of a breach. Affected individuals and the Secretary of HHS must always be notified by a covered entity after discovery of a breach, although the manner of notification differs between the two. In contrast, the media (specifically a “prominent media outlet” in the State or jurisdiction of affected residents) need only be alerted if a breach involved 500 or more affected individuals and only the media serving the State or jurisdiction of affected residents must be notified.

Notice of such a breach to an individual can be written and sent by first-class mail or, in some cases, by electronic mail; when written notice cannot be provided, notification may be made by appropriate substitute notice (Web site posting of notification, telephone, or other means). The rule also requires notice to the Secretary of a breach of unsecured PHI depending on whether the breach involves 500 or more individuals. When the breach involves 500 or more individuals, notification to the Secretary must be made contemporaneously with notification to the individual. When the breach involves less than 500 individuals, a covered entity may maintain a log of such breaches and provide notification of all such breaches to the Secretary within 60 days of the end of each calendar year. The rule states that covered entities must provide notice in the manner

specified on HHS's Web site. The rule also requires business associates to notify a covered entity of a breach of unsecured PHI without unreasonable delay (less than 60 days). Law enforcement can delay notification or posting under this rule if such would impede a criminal investigation or "cause damage to national security."

A covered entity has the opportunity to mitigate its exposure to required breach notifications by ensuring that all PHI is appropriately *secured*, meaning that the covered entity has rendered the PHI unusable, unreadable, or undecipherable by an unauthorized individual. The commentary to the interim final rule provides some guidance on the technologies and methodologies that a covered entity may use to render PHI unusable, unreadable, and/or undecipherable to unauthorized individuals.

If you would like more information about the new HIPAA breach notification requirements and the legal issues they raise, please contact the Womble Carlyle lawyer with whom you usually work, or one of the following attorneys:

[Kim Licata \(KLicata@wcsr.com\)](mailto:KLicata@wcsr.com), 919-484-2313) in our [Life Sciences Industry Group](#), or [Jill Girardeau \(JGirardeau@wcsr.com\)](mailto:JGirardeau@wcsr.com), 404-879-2426) in our [Health Care Group](#).

For more information about Womble Carlyle's capabilities in working with the media or crisis management applicable to breaches of unsecured PHI, please contact [Henry Fawell](#) at 410-545-5830 or another member of our [Strategic Communications](#) or [Privacy Teams](#).

Womble Carlyle client alerts are intended to provide general information about significant legal developments and should not be construed as legal advice regarding any specific facts and circumstances, nor should they be construed as advertisements for legal services.

IRS CIRCULAR 230 NOTICE: *To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. tax advice contained in this communication (or in any attachment) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed in this communication (or in any attachment).*