

Management Alert

HIPAA Breach Notification Interim Final Rule

The American Recovery and Reinvestment Act of 2009 (“the Act”) made several changes to the HIPAA privacy rules—including adding a requirement for notice to affected individuals of any breach of unsecured protected health information. On August 24, 2009, the Department of Health and Human Services (HHS) published an interim final rule (the “Rule”) that lays out the specific steps that HIPAA-covered entities and their business associates must take. This Management Alert will summarize the Rule, which becomes effective September 23, 2009. HHS has stated that while it expects covered entities to comply with this Rule as of September 23, it will not impose sanctions for failure to provide the required notifications for breaches discovered through February 22, 2010. Instead, during such period it will work with covered entities to achieve compliance through technical assistance and voluntary corrective action.

Summary of Interim Rule

The new requirements apply if all of the following are present:

- **There is a “breach.”** The Rule defines “breach” to mean (subject to exceptions discussed below) the unauthorized acquisition, access, use, or disclosure of protected health information (“PHI”).
- **The PHI is “unsecured.”** The Rule defines “unsecured protected health information” to mean PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS guidance.
- **The breach “compromises the security of the PHI.”** Under the Rule, this occurs when there is a significant risk of financial, reputational, or other harm to the individual whose PHI has been compromised.

What is Secured PHI?

On April 27, 2009, HHS issued the HITECH Breach Notification Guidance specifying the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals. That guidance creates a safe harbor so that covered entities and business associates would not be required to provide the breach notifications required by the Act for PHI meeting these standards. PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals only if one or more of the following methods are used:

(1) *Encryption.* Electronic PHI is only secured where it has been encrypted. The HIPAA Security Rule specifies encryption to mean the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning

without use of a confidential process or key. The Rule identifies the various encryption processes which are judged to meet this standard. Further, such confidential process or key that might enable decryption must not have been breached. To avoid a breach of the confidential process or key, decryption tools should be kept on a separate device or at a location separate from the data they are used to encrypt or decrypt.

(2) *Destruction.* Hard copy PHI, such as paper or film media, is only secured where it has been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed.

Determining Whether a Breach of Unsecured Protected Health Information Has Occurred

The Rule envisions that covered entities and their business associates will analyze the following in determining whether a breach of unsecured PHI has occurred:

(1) Determine whether the use or disclosure of PHI violates the HIPAA Privacy Rule. For an acquisition, access, use, or disclosure of PHI to constitute a breach, it must constitute a violation of the HIPAA Privacy Rule. For example, if information is de-identified in accordance with 45 CFR 164.514(b), it is not PHI and any inadvertent or unauthorized use or disclosure of such information will not be considered a breach under the notification requirements of the Act and the Rule.

(2) Analyze whether there is a use or disclosure that compromises the security and privacy of PHI. HHS clarifies that a use or disclosure that “compromises the security and privacy of PHI” means a use or disclosure that “poses a significant risk of financial, reputational, or other harm to the individual.” Thus, in order to determine whether a breach has occurred, covered entities and business associates will need to conduct a risk assessment to determine whether the potential breach presents a significant risk of harm to individuals as a result of an impermissible use or disclosure of PHI. The Rule provides a number of factors which should be taken into account when conducting a risk assessment. A covered entity should consult its legal counsel with respect to the impact of the presence of such factors.

(3) Assess Whether any Exceptions to the Breach Definition Apply. The Rule discusses a number of exceptions to the definition of breach. The following three situations are excluded from the definition of “breach” under the Act:

(i) The unintentional acquisition, access, or use of PHI by any workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the Privacy Rule.

(ii) The inadvertent disclosure of PHI by an individual otherwise authorized to access PHI at a facility operated by a covered entity or business associate to another person at the same covered entity or business associate, or at a organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.

(iii) An unauthorized disclosure where a covered entity or business associate has a good faith belief that an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.

The covered entity or business associate has the burden of proving why a breach notification was not required and must document why the impermissible use or disclosure fell under one of the exceptions. Covered entities should document the risk and other breach assessments accordingly.

Notification Requirements to Individuals and/or Media in the Event of a Breach of Unsecured PHI

The breach notifications required by the Act and the Rule are significant and are triggered by the “discovery” of the breach of unsecured PHI. A breach is treated as “discovered” by a covered entity as of the first day the breach is known, or reasonably should have been known, to the covered entity. Given that knowledge of a breach may be imputed, a covered entity should implement reasonable breach discovery procedures.

- **Notification to Individuals.** A covered entity must send the required notification to each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of the breach, without unreasonable delay and in no case later than 60 calendar days after the date the breach was first discovered by the covered entity. The Act and the Rule specify the content requirements and the methodology required for providing such breach notices.

For covered entities that do not have sufficient contact information for some or all of the affected individuals, the Rule requires that substitute notice be provided as soon as reasonably possible. If a covered entity has insufficient contact information for 10 or more individuals, then substitute notice must be provided via a posting for a period of 90 days on the home page of its web site or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. In such instances, the covered entity is also required to have an active toll-free number for 90 days so that an individual can find out whether his or her unsecured PHI may be included in the breach.

- **Notification to Media.** If a covered entity discovers a breach affecting more than 500 residents of a state or jurisdiction, it must provide notice to prominent media outlets serving that state or jurisdiction without unreasonable delay and in no case later than 60 calendar days after the date the breach was discovered by the covered entity
- **Notification to HHS.** If more than 500 individuals are involved in the breach, regardless of whether the breach involved more than 500 residents of a particular State or jurisdiction, then the covered entity must notify HHS concurrently with the individual notifications. For breaches involving fewer than 500 individuals, the covered entity must maintain an internal log or other documentation of such breaches and annually submit such log to HHS. For calendar year 2009, the covered entity is only required to submit the log for breaches occurring on or after September 23, 2009.
- **Notification by a Business Associate.** Following the discovery of a breach of unsecured PHI, a business associate is required to notify the covered entity of the breach so that the covered entity can, in turn, notify the affected individuals. To the extent possible, the business associate should identify each individual whose unsecured PHI has been, or is reasonably believed to have been, breached. Such notice should be given without unreasonable delay and no later than 60 days following discovery of a breach.

- **Delay Required by Law Enforcement.** The Act provides that a breach notification may be delayed if a law enforcement official determines that such notification would impede a criminal investigation or cause damage to national security.

Interaction of Interim Final Rule with FTC, HIPAA Rules, and Other State Laws

On August 17, 2009, the FTC issued companion breach notification requirements for vendors of personal health records (PHRs) and their third party service providers following the discovery of a breach of unsecured PHR identifiable health information. Entities operating as HIPAA-covered entities and business associates are not subject to these FTC breach notification rules. But in certain instances where a breach involves an entity providing PHRs to customers of HIPAA-covered entity through a business associate arrangement, and directly to the public, the FTC will deem compliance with the HHS Rule as compliance with its own breach notification rules.

HHS has emphasized that this Rule does not modify a covered entity's responsibilities with respect to the HIPAA Security Rule; nor does it impose any new requirements upon covered entities to encrypt all PHI. A covered entity may still be in compliance with the Security Rule even if it decides not to encrypt electronic PHI so long as it utilizes another method to safeguard information in compliance with the Security Rule. However, if such method is not in compliance with the requirements of the Rule with respect to securing PHI, then the covered entity will be required to provide a breach notification to affected individuals upon a breach of unsecured PHI. The Rule preempts contrary State breach notification laws. A covered entity must still comply with requirements of State law which are in addition to the requirements of the Rule, but not contrary to such requirements (such as additional elements required to be included in a notice).

For more information about the Rule, please contact the Seyfarth attorney with whom you work, or any Employee Benefits or Healthcare attorney on our website (www.seyfarth.com/EmployeeBenefits or www.seyfarth.com/Healthcare).



Breadth. Depth. Results.

www.seyfarth.com