



What You Need to Know About the New HIPAA Breach Notification Rule¹

New regulations effective September 23, 2009 require all physicians who are covered by HIPAA to notify patients if there are breaches of security involving their medical information. The following summarizes these new requirements. These requirements apply in addition to any notification obligations imposed by state law. These requirements also supplement the obligations imposed by the HIPAA Privacy and Security Rules.

HIPAA covered entities (i.e, health plans, health care clearinghouses, physicians, and other health care providers who transmit any health information electronically in connection with a HIPAA standard transaction) must comply with the new breach notification requirements specified in interim final regulations promulgated pursuant to the “American Recovery and Reinvestment Act of 2009” that was signed into law on February 17, 2009. Following the discovery of a breach of unsecured protected health information (PHI), physicians must provide notification to affected individuals, to the Secretary of the Department of Health and Human Services (HHS), and in some cases, to the media.

The breach notification provisions are effective, and compliance is required for breaches occurring on or after September 23, 2009. However, HHS will use its discretion not to enforce the new breach notice requirements and will not impose sanctions or financial penalties for breaches discovered before February 22, 2010. After the breach notification rule takes effect, but before HHS imposes sanctions, HHS expects compliance with the breach notification requirements. Accordingly, we recommend that physicians (and their business associates) plan immediately to comply with these new breach notification requirements.

This new HIPAA Breach Notification Rule only concerns the unauthorized acquisition, access, use or disclosure of unsecured patient health information as a result of a security breach. This Rule does not replace the existing HIPAA Privacy Rule that permits a covered entity (i.e., physician) to use and disclose patient health information, within certain limits and protections, for treatment, payment, and health care operations activities.

¹ Disclaimer: The information provided in this document does not constitute, and is no substitute for, legal or other professional advice. Users should consult their own legal or other professional advisors for individualized guidance regarding the application of the law to their particular situations, and in connection with other compliance-related concerns. Prepared September 21, 2009 based on available information.

Breach Notification Requirements

What Constitutes a Breach

A breach is defined as the acquisition, access, use, or disclosure of unsecured PHI which is not permitted by the HIPAA Privacy Rules and compromises the security or privacy of the PHI. In order to determine whether a breach of unsecured PHI has occurred, the Rule calls for physicians to perform risk assessments to establish whether a significant risk of financial, reputational, or other harm to the affected individual(s) exists. If the physician performs a risk assessment and determines that there is significant risk of harm to the affected individual(s) as a result of the unauthorized use or disclosure of unsecured PHI, then breach notification(s) are required. For example, a stolen laptop containing patient health records that is not encrypted would constitute a breach and trigger notification requirements, unless the laptop was returned and a forensic analysis demonstrates that the PHI was not accessed or otherwise compromised.

What Constitutes Unsecured PHI

Unsecured PHI is any patient health information that is not secured through a technology or methodology, specified by HHS, that renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals. Unsecured PHI (i.e., patient's full name, patient's address, social security number, diagnosis) can be in any form or medium including electronic, paper, or in oral form.

Exceptions to the Breach Notification Requirements

The law identifies the following circumstances when a breach notification is NOT required:

- Any ***unintentional*** acquisition, access, or use of the PHI by a workforce member (i.e., employees, volunteers, trainees, and other persons whose conduct is under the direct control of a covered entity, whether or not they are paid by the covered entity) or an individual, acting upon the authority of the HIPAA covered entity or a business associate (BA), who acquired, accessed, or used the PHI in good faith and within the normal scope of his/her authority, and if that PHI is not further used or disclosed. For example, breach notification would not be required where a billing employee receives and opens an email containing PHI about a patient which a nurse mistakenly sent to the billing employee but, upon noticing that he/she is not the intended recipient, the billing employee alerts the nurse of the misdirected e-mail, and then deletes it;
- Any ***inadvertent*** disclosure by a person who is authorized to access PHI at a covered entity or BA to another person authorized to access PHI at the same covered entity, BA, or organized health care arrangement² in which the covered entity participates, and the PHI is not further used or disclosed in violation of the HIPAA Privacy Rules;

² An organized health care arrangement is a clinically integrated care setting in which individuals typically receive health care from more than one health care provider such as a hospital and the health care providers who have staff privileges at the hospital.

- A disclosure of PHI where a covered entity or BA has a ***good faith belief*** that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information (i.e., a laptop is lost or stolen and then recovered, and a forensic analysis of the computer shows that information was not opened, altered, transferred, or otherwise compromised);
- If law enforcement determines that notification would impede a criminal investigation or cause damage to national security, covered entities are allowed to delay notification, ***but only for up to 30 days as orally directed by the law enforcement agency, or for such longer period as the law enforcement agency specifies in writing***; and
- Encryption and destruction are deemed as the technologies and methods for securing PHI. Covered entities that have thus secured their PHI through appropriate encryption or destruction methods are relieved of the notification obligation (unless otherwise required by federal or state law or necessary to mitigate the harmful effect of the breach). The encryption must be an algorithmic process with a confidential process or encryption key, and the decryption tools are stored at a location separate from the encrypted data.. With regard to destruction, paper copies of PHI must be shredded or destroyed and electronic media copies of PHI must be cleared, purged, or destroyed such that PHI cannot be retrieved..

Breach Notification

HIPAA covered entities (i.e., physicians) are required to notify the affected individuals of any unauthorized acquisition, access, use, or disclosure of unsecured PHI without unreasonable delay but not later than 60 calendar days after discovery. Thus if the physician has compiled all of the necessary information to provide notification of a breach of unsecured PHI to affected individual(s) by day 10 (10 days from the day the breach was discovered) but waits until day 60 to send notifications, this would constitute an unreasonable delay.

BAs who have access to PHI are required to notify the covered entity of any such breach, including the name of any individual whose unsecured PHI has been released. Physicians should make sure that their agreements with BAs address these new breach notification requirements, including the timing of BA notification to a physician following a breach and responsibility for paying costs resulting from a breach. While HHS has indicated that the parties to BA agreements have flexibility in this regard, it has encouraged the parties to ensure that individuals do not receive notification from both the BA and the covered entity, as this could be confusing.

Discovery of Breaches

Breaches are treated as discovered as of the first day on which the breach is known or should have been known to the physician (or where the BA is acting as their agent).

How to Provide Notice

Physicians should send written notification via first class mail to each affected individual (or if deceased, the individual's next of kin) at the last known address, unless the individual has indicated a preference for e-mail. In situations where a physician deems

possible imminent misuse of unsecured PHI, the physician may provide other forms of notice, such as by telephone or e-mail, in addition to the written notice.

If the address is unknown for fewer than 10 individuals, then a substitute notice must be provided by other means reasonably calculated to reach the affected individual, such as by telephone. If the address is unknown for 10 or more individuals, then a substitute notice must be provided by either a conspicuous posting on the entity's web homepage for a specified period of time (period of time proposed by HHS is 90 days) or a conspicuous publication in major print or broadcast media in the geographic areas where the individuals affected by the breach likely reside. The substitute notice must include a toll-free number that remains active for at least 90 days.

Notice to 500+ Affected Individuals

If the breach of unsecured PHI affects 500 or more individuals, then the notice must also be provided to major media outlets serving the relevant State or jurisdiction. The notice to the media must contain the same information as the written notice to individuals, and must similarly be provided without unreasonable delay, but in no case later than 60 calendar days after discovery of the breach.

Notice to HHS

Additionally, the physician must notify HHS, in the manner specified on the HHS website, contemporaneously with the notice sent to the individuals. The HHS website will have a list that identifies the covered entities involved in a breach in which 500 or more individuals are affected. If less than 500 individuals are affected then the covered entity may maintain a log of the breaches and must submit this log annually to HHS (within 60 days after the end of each calendar year).

Contents of the Written Notice

The written notice must contain the following content:

1. Notification must be written in plain language;
2. A brief description of what happened, including the date of the breach and the date of the discovery of the breach to the extent these dates are known;
3. A description of the types of unsecured PHI that were disclosed in the breach (i.e., full name, social security number, date of birth, home address, account number, diagnosis, disability code, etc.);
4. Steps that the patients should take to protect themselves from potential harm resulting from the breach of unsecured PHI (such as contacting their credit card companies);
5. A brief description of the actions taken by the physician to investigate the breach, mitigate harm to individuals, and to protect against any further breaches; and
6. Contact procedures for individuals to ask questions or learn additional information, including a toll-free number, an e-mail address, website, or postal address.

Compliance with Federal and State Laws on Breach Notifications

The new HIPAA breach notification requirements override any conflicting state laws. However, physicians must comply with both federal and state breach notification laws if the state law does not conflict with these new HIPAA breach notification requirements (i.e., a state law requires the covered entity to send a notice of a breach of unsecured PHI to the affected individual(s) in 30 calendar days (not 60 days), and the physician has all of the necessary information to comply with the state's 30 day requirement. Issuing the notice by day 30 does not conflict with federal law.)

These requirements similarly do not override obligations imposed by other federal laws, such as requirements imposed by Title VI of the Civil Rights Act to take reasonable steps to ensure meaningful access to the notice by those with Limited English Proficiency, and requirements imposed by the Americans with Disabilities Act to ensure effective communication of the notice to individuals with disabilities.

Additional Requirements

In addition to the breach notification requirements, the federal regulations impose additional compliance obligations on physician practices consistent with those imposed by other HIPAA obligations, including the requirement to:

- 1) Revise the practice's policies and procedures and Notice of Privacy Practices to reflect the HIPAA Breach Notification Rule. For example, physicians should make sure that their practice's HIPAA compliance program, including record retention practices, address risk assessments for determining whether a breach of unsecured PHI has occurred;
- 2) Train their workforce members on the practice's policies and procedures with respect to the notification requirements;
- 3) Allow individuals to complain about those policies and procedures, or whether the notification requirements have been violated;
- 4) Sanction workforce members who violate the notification requirements; and
- 5) Refrain from retaliating against those who exercise their rights.