What you need to know about the HIPAA breach notification rule

HIPAA-covered entities (i.e, health plans, health care clearinghouses, and physicians and other health care providers who transmit any health information electronically in connection with a HIPAA standard transaction) are currently bound by the 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.[1] These breach notification requirements were subsequently changed as a result of new regulations that were published in January as part of the HIPAA Omnibus Rule. The following summarizes the requirements that apply as of September 23, 2013. These requirements apply in addition to any notification obligations imposed by state law and also supplement the obligations imposed by the HIPAA Privacy and Security Rules.

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 HIPAA Breach Notification Rule only concerns the unauthorized acquisition, access, use or disclosure of unsecured PHI as a result of a security breach. This Rule does not replace the existing HIPAA Privacy Rule that permits covered entities, including physicians, to use and disclose PHI, within certain limits and protections for treatment, payment, and health care operations activities.

Breach notification requirements

What constitutes a breach

A breach is defined as the acquisition, access, use, or disclosure of ***unsecured*** PHI that is not permitted by the HIPAA Privacy Rules and compromises the security or privacy of the PHI. The simplest thing physicians can do to minimize their risk of a breach is to ***secure*** their PHI by ensuring that they and their business associates encrypt all their electronic PHI (ePHI). See discussion below.

Determining whether a breach occurred

Effective September 23, 2013, the obligation to notify patients if there is a breach of their PHI is expanded and clarified under the new rules. Breaches will be presumed reportable unless, after completing a risk analysis applying at least the following four factors, it is determined that there is a "low probability of PHI compromise." The four factors to be considered are:

- The nature and extent of the PHI involved, including the type and sensitivity of the identifiers and the likelihood the information can be re-identified;
- The person who obtained the unauthorized access and whether that person has an independent obligation to protect the confidentiality of the information;
- Whether the PHI was actually acquired or viewed; and

[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.

- The extent to which the risk has been mitigated, such as by obtaining a signed confidentiality agreement from the recipient.

This rebuttable presumption of breach and four factor assessment replaces the previous, more subjective "significant risk of financial, reputational, or other harm" analysis for establishing a breach. The new rules further clarify that there is no need to have an independent entity conduct the risk assessment and indeed, no risk assessment need be conducted at all if the breach notification is made (although, physicians will want to undertake an appropriate review and steps to mitigate the harm and reduce the likelihood of future breaches in any case).

What constitutes unsecured PHI

Unsecured PHI is any PHI that is not secured through a technology or methodology specified by HHS that renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals. The only technologies or methodologies HHS has approved to secure PHI are encryption and destruction. As noted above, physicians would be well advised to encrypt all their *e*PHI, and ensure their business associates (BAs) do so as well. For further information on encryption see the AMA publication ***"****HIPAA Security Rule: Frequently asked questions regarding encryption of personal health information*." Unsecured PHI (e.g., 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 physician or other 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, who acquired, accessed, or used the PHI in good faith and within the scope of his/her authority, and if that PHI is not further used or disclosed in a manner not permitted by the HIPAA Privacy Rules. For example, breach notification may 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 arrangement[2] in which the covered entity participates, and the PHI is not further used or disclosed in violation of the HIPAA Privacy Rules;
- 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 (e.g., 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);
- Encryption and destruction are deemed as the technologies and methodologies for securing PHI. Covered entities that have thus secured their PHI through appropriate encryption or destruction 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

[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.

stored at a location separate from the encrypted data. For further information, see the AMA publication ***"****HIPAA Security Rule: Frequently asked questions regarding encryption of personal health information*." 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 to individuals

HIPAA-covered entities (e.g., 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.

Discovery of breaches

Breaches are treated as discovered as of the first day on which the breach is known or, by exercising reasonable diligence, would have been known to the physician (or where the BA is acting as their agent, their BA).

Delay of notification

If law enforcement determines that notification would impede a criminal investigation or cause damage to national security, covered entities or business associates 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***.

Business associates

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. Effective September 23, 2013, these reporting obligations are extended to those who subcontract with BAs to perform some or all of the BA's obligations. In addition, physicians are responsible to ensure that all breach notifications are made, regardless of whether the breach was caused by one of their BAs or their BA's subcontractors. Physicians must make sure that their agreements with BAs and subcontractors address these breach notification requirements, including the timing of BA notification to a physician following a breach and responsibility for paying costs resulting from a breach. However, any necessary amendments to BA agreements may not need to be completed until September 23, 2014, pursuant to the transition provisions governing BA agreements generally. Finally, the new rules further confirm that the breach notification requirement may be delegated to a business associate, and physicians are encouraged to coordinate with their BAs so that patients receive only one notification of the breach.

How to provide notice to individuals

Physicians should send written notification via first-class mail to each affected individual (or if deceased, the individual's next of kin or personal representative) 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 contact information is unknown or out-of-date 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 information is unknown or out-of-date for 10 or more individuals, then a substitute notice must be provided by either a conspicuous posting on the entity's web homepage (for 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.

Additional notice if 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.

Contents of written notice

The written notice provided to affected individuals and the media, if applicable, 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 (e.g., 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 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.

Notice to HHS

In addition, the physician must notify HHS, in the manner specified on the HHS website, contemporaneously with the notice sent to the individuals for breaches involving 500 or more individuals. The HHS website maintains a list that identifies the covered entities involved in such a breach. 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 in which the breach was discovered).

Compliance with federal and state laws on breach notifications

The 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 the HIPAA breach notification requirements (e.g., a state law that 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) 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:

- Revise the practice's policies and procedures and Notice of Privacy Practices (NPP) to reflect the HIPAA Breach Notification Rule. Effective September 23, 2013, NPPs must include a statement of the right of individuals to be notified following a breach of their unsecured PHI. To the extent physicians did not previously amend their NPPs, this addition will be considered a material change, and notification must be provided as required by the HIPAA Privacy Rules. Physicians should make sure that their practice's HIPAA compliance program, including record retention practices, addresses determining whether a breach of unsecured PHI has occurred;
- Train their workforce members on the practice's policies and procedures with respect to the notification requirements;
- Allow individuals to complain about those policies and procedures, or whether the notification requirements have been violated;
- Sanction workforce members who violate the notification requirements; and
- Refrain from intimidating or retaliating against those who exercise their rights.