The Four Things You Need to Know and Do to Comply with the New HIPAA Breach Notification Rules

Sep 03 2009

Practice Area: Health Law & Health Information Privacy and Security

Effective September 23, 2009, if you are a health care provider, clearinghouse, or health plan that is a "Covered Entity" under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), you must notify affected individuals of certain breaches of their individually identifiable health information by you or your Business Associates.

This new "Rule" goes into effect on September 23, 2009; however, sanctions will not be imposed until after February 22, 2010.

#1 WHAT TO KNOW: If a breach involves encrypted or de-identified information, you don't have to notify anyone.

WHAT TO DO: Find out if NIST-level encryption is on, or available for the systems and applications on which you and your Business Associates store or transmit PHI.

The Rule applies only to protected health information ("PHI") that is "unsecured"; which is defined as "[PHI] that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by [HHS]."

For now, the Rule specifies three methodologies that would render PHI no longer "unsecured":

- encryption of electronic data per National Institute Standards and Technology (NIST) standards
- destruction of electronic media as per NIST standards, and
- the destruction or shredding of paper, film or other hard copy media.

This means a stolen laptop containing NIST-level encrypted PHI would not trigger a notification obligation, because the approved encryption renders the PHI "unusable, unreadable, or indecipherable." A stolen laptop containing merely login username and password protection of PHI would be unsecured, and the Rule's breach notification provisions would apply.

Breaches of de-identified health information (as defined in HIPAA) would not trigger a notification obligation, because de-identified health information is not considered PHI.

Special Note: Business Associates must notify the Covered Entity, not the individual, of a breach. You may want to revisit the Business Associate Agreement and develop a joint breach determination and notification provision. Business Associates must notify covered entities no later than 60 calendar days after discovery of a breach, but Covered Entities will want this to be shorter so that they have time to react. The Covered Entity must then notify the affected individuals. A Business Associate will go through the same analysis and process applicable to covered entities in determining whether to notify the Covered Entity. The notice to the Covered Entity must include the identification of each person whose unsecured PHI has been accessed, acquired, used, or disclosed, and any other available information that the Covered Entity is required to include in its notification to the affected individual.

#2 WHAT TO KNOW: If a breach falls into certain narrow exceptions, you don't have to notify anyone.

WHAT TO DO: Change your privacy and security policies to include these exceptions, and document when an exception determination is made.

The Rule provides the following three exceptions to the definition of breach:

- Unintentional acquisition, access, or use of PHI by workforce members acting under authority of Covered Entity or (Business Associate), if done in good faith and provided the PHI is not further used or disclosed in any manner that violates the Privacy Rule.
- Inadvertent disclosures of PHI from a person authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the same Covered Entity, Business Associate or Organized Health Care Arrangement, provided the PHI is not further used or disclosed in any manner that violates the Privacy Rule.
- Unauthorized disclosures where the Covered Entity or Business Associate has good faith belief that the unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.
- Example: A Covered Entity sends a number of explanations of benefits (EOBs) to the wrong individuals. Some of the EOBs are returned by the post office, unopened, marked undeliverable. The Covered Entity may conclude that the improper addressee could not have reasonably retained the information. However, the EOBs actually delivered and opened could constitute a potentially reportable breach.

The burden of demonstrating an exception applies lies with the Covered Entity. The Covered Entity must document that notification was not required.

#3 WHAT TO KNOW: If a breach does not pose a risk to the individual, you don't have to notify anyone.

WHAT TO DO: Change your privacy and security policies to include the risk analysis steps, and document the risk determination for each breach that does not meet #1 or #2.

If an unauthorized disclosure of unsecured PHI occurs that does not fit into an exception or the disclosure does not meet the following definition of breach, the Covered Entity does not need to fulfill the notification requirements of the Rule. A Breach is the "acquisition, use, or disclosure of PHI in a manner not permitted under [HIPAA's Privacy Rule] that compromises the security or privacy of the PHI." The Covered Entity must undertake a risk assessment to determine whether the disclosure poses a significant risk of financial, reputational, or other harm to the individual whose PHI was breached. To do so, HHS recommends considering the following factors:

- Who impermissibly used the PHI or to whom was the PHI impermissibly disclosed?
- PHI disclosure to another Covered Entity = less risk of harm.
- PHI disclosure to a non-Covered Entity = greater risk of harm.
- What immediate steps were taken to mitigate the impermissible use or disclosure?
- Did the Covered Entity obtain the recipient's satisfactory assurances that the information would not be used or further disclosed? (i.e., obtain confidentiality agreement).
- Was the PHI returned prior to being accessed for an improper use? i.e., forensic analysis of stolen laptop reveals PHI not opened, altered, transferred or otherwise compromised = no breach.
- What type and amount of PHI was involved in the impermissible use or disclosure?
- PHI that includes patient's name and fact that he received hospital services = less risk of harm.
- PHI that includes patient's name and fact that he received mental health services = greater risk of harm.

#4 WHAT TO KNOW: For a reportable breach, you must notify HHS and the individuals; individuals must be notified in writing (if you can find them) and on your web site and in the media (if you cannot find them, or if more than 500 individuals are impacted).

WHAT TO DO: Create, implement and maintain a breach notification plan that includes keeping a log of all breaches.

Covered Entity's must notify HHS of all reportable breaches. If such breaches involve more than 500 people in a particular state/jurisdiction, the Covered Entity must notify both a "prominent media outlet" and HHS. [1]

For breaches involving fewer than 500 individuals, a Covered Entity must maintain a log of each breach and notify HHS not later than 60 calendar days after the end of each calendar year.

Covered Entities must notify affected individuals within 60 calendar days from the date of discovery of the breach (by the Covered Entity or the Business Associate). The notice must be in writing and be sent (a) via first-class mail to the individual's last known address, or (b) via e-mail if the individual has agreed to receive electronic notice via e-mail. It must be written in plain language and contain the following elements:

- A brief description of what happened, including the date of the breach and the date of discovery of the breach.
- The types of PHI involved (i.e., name, social security number, date of birth, diagnosis, etc).
- Steps individuals should take to protect themselves from potential harm.
- A description of the steps taken to investigate, mitigate harm, and protect against further breaches.
- Contact information for further information, such as a toll-free number, e-mail address, web site, or postal address.

If an individual's contact information is missing or out of date, the Covered Entity must provide a "substitute notice." If the breach involved fewer than 10 people, the notice must be sent via e-mail or telephone. If it involved 10 or more individuals, the notice must be either (a) posted on the patient / participant home page of the Covered Entity's web site for 90 days, or (b) published in major print or broadcast media where the affected individuals are likely to reside.

Special note for entities that provide personal health record services as Covered Entities: Comply with HIPAA, not the new FTC Rules. One day after the Rule takes effect, new Federal Trade Commission breach notification requirements will require personal health record (PHR) vendors and their third-party service providers to notify affected individuals of breaches. [2]

The intent of the FTC Rule is to govern entities that do not have to comply with HIPAA, such as occupational health vendors that host employee health records and vendors who sell devices that are able to upload data to a personal record. If an entity is subject to both the HHS and FTC rules, such as vendors that offer PHRs to customers of a Covered Entity as a Business Associate and also offer PHRs directly to the public, the FTC will deem compliance with certain provisions of the HIPAA breach notification rule as compliance with the FTC's Rule.

[1] The Rule states that the HHS Secretary will post instructions on its web site for submitting notifications.

[2] The FTC breach notification form can be accessed at http://www.ftc.gov

---