Explanation of Sample HIPAA Privacy Policy Number 9: Breach Notification

Covered entities, including physician practices, are required by the Privacy Rule to report any "Breach" of unsecured protected health information. This explanation and sample HIPAA Privacy Policy 9 discuss the obligations of practices to comply with the Breach Notification Rule.

Breach Notification Rule Background

The Breach Notification Rule was mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act and required covered entities, including physician practices to provide notification to the individual, the government, and in some cases the media in the event of a "breach of unsecured health information." This provision was implemented by an interim final regulation which was published in August 2009 and later amended by the Final Omnibus Rule in 2013. The Final Omnibus Rule removed much of the subjectivity of the interim final rule.

What is a Breach?

A "Breach" for purposes of the Breach Notification Rule is defined as an impermissible use or disclosure (i.e., a violation of the Privacy Rule) which compromises the security or privacy of the protected health information.

There are three exceptions where an impermissible use or disclosure will not be considered a breach. They are:

(1) An unintentional acquisition, access or use of protected health information by a member of the practice's workforce or an individual under authority of the workforce that was made in good faith and under the scope of authority and does not result in further impermissible uses or disclosures. (For example, this exception would be applicable to violations of the minimum necessary policy that were inadvertent and in good faith, but would not cover employees who are "snooping" into a record where they do not have a need to know the information).

(2) An inadvertent disclosure from a person who is authorized to access PHI to another person who is similarly authorized to access PHI at the covered entity or as part of an organized health care organization, provided that no further inappropriate uses or disclosures follow. (For example, this exception would be applicable to a disclosure of information on the wrong patient to a doctor who is part of a hospital's medical staff). This exception will rarely apply to an inadvertent disclosure involving a physician practice.

(3) A disclosure of protected health information where the practice has a good faith belief that an unauthorized person who received the information would not have been able to retain the information. (For example, the wrong results are handed to a patient but taken back before the patient has a chance to look at them).

When is Protected Health Information "Unsecured"?

It is important to note that an improper use or disclosure is only considered a "Breach" when the Protected Health Information that is wrongly disclosed is "unsecured." If Protected Health Information is rendered unusable, unreadable or indecipherable then it is no longer considered "unsecured." In general, Protected Health Information is rendered unusable, unreadable and indecipherable by either destroying it (such shredding in a manner where it cannot possibly be read or destroying electronic information in accordance with Department of Defense standards) or by encrypting the information.

Specific guidance on how to render Protected Health Information unusable, unreadable and indecipherable is available on the Office of Civil Rights website and is to be updated annually. The link to the guidance is:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html

Breach Notification

When it has been determined, through the risk assessment that an impermissible use or disclosure does meet the definition of "Breach", then the individual whose Protected Health Information was breached must be notified without unreasonable delay and no later than sixty (60) days from the date of discovery. The clock starts "running" when the practice (or an agent of the practice) discovers the breach. The individual must be notified via first class mail (or email, but only if the individual has agreed to receive such notices electronically).

If the practice does not have current information for more than 10 individuals, then the practice must post the notice on the home page of its website or put a notice in a major print or broadcast medium where the individuals are likely to reside. (In lieu of doing this, the practice can also do some research to update the contact information for the individuals at issue). This "substitute notice" must be posted for a period of at least ninety days. The posting should not include names of individuals, but should include a toll free number that will remain active for ninety days for individuals to call to find out if they were part of the breach.

If there is a situation where an individual may be subjected to harm because of the breach, then the practice is expected to also alert the individual by telephone or other appropriate means, in addition to the individual or substitute notice.

Where greater than 500 residents of a state or jurisdiction have been impacted by the Breach, then, in addition to the individual notice set forth above, the practice must also provide notice in a prominent media outlet serving the affected area. This notice must be provided without reasonable delay and no later than sixty days following the discovery of the breach by the practice or an agent of the practice.

All breaches must also be reported to the Secretary of the Department of Health and Human Services. If the breach involves more than 500 individuals, then the notice must be made without unreasonable delay or no later than 60 days. Smaller breaches (involving less than 500 individuals) must be maintained in a log and reported through the Office of Civil Rights website no later than 60 days after the end of the calendar year in which the breach occurred.