Breach Notification Involving Protected Health Information

Save to myBoK

by Peter Adler

The American Recovery and Reinvestment Act (ARRA), previously known as the stimulus bill, offers new challenges to health information privacy professionals. Today guest author Peter Adler, attorney at law for Pepper Hamilton LLP, looks at new provisions requiring organizations to provide notice in the event of a breach.

The portion of ARRA known as the HITECH Act amends HIPAA with new notice of breach provisions that apply to covered entities and business associates. A breach generally is an unauthorized acquisition, access, use, or disclosure of unsecured protected health information (PHI) which compromises the security or privacy of such information.

The term "unsecured" essentially means that the PHI is unencrypted. Encryption guidelines are to be specified by the secretary of Health and Human Services or otherwise meet standards that are developed or endorsed by the American National Standards Institute.

Breaches Discovered by a Covered Entity or Business Associate

Breaches will be treated as "discovered" by a covered entity or a business associate the day the breach is known or reasonably should have been known to have occurred. Unless delayed for law enforcement purposes, notifications are to be provided without unreasonable delay and in no case later than 60 days after discovery of the breach.

Breaches Involving a Covered Entity

Once discovered, a covered entity shall notify each individual whose unsecured PHI has been or may have been breached. Notice provided by a covered entity shall include the following:

- what happened, including the date of the breach and the date of the discovery of the breach, if known;
- the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code);
- steps that may be taken by individuals to protect themselves from potential harm resulting from the breach;
- what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches; and
- procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number and e-mail address, Web site, or postal address.

Notice may be provided in a number of ways. First, a written notification may be sent by mail or e-mail. If mailing or e-mail addresses are unknown for 10 or more individuals, substitute notice may be provided. This is accomplished by the covered entity conspicuously posting notice on the home page of its Web site or by using major print or broadcast media.

When the possible imminent misuse of unsecured PHI creates urgency, notice may be provided to individuals by telephone or other appropriate means. Notice to the media is acceptable when the breach is likely to have included more than 500 individuals.

Breaches involving more than 500 individuals are to be reported immediately to the HHS secretary and will be posted on the HHS Web site. Breaches of fewer than 500 individuals will be logged by the covered entity and annually submitted to the secretary. Annual reports of all reported breaches will be provided by the secretary to specified House committees.

Breaches Involving a Business Associate

The legislation provides that following discovery, a business associate must notify the covered entity of the breach. The content of the notice is to include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during the breach.

Effective Date

Interim final regulations on breach notifications are to be published no later than August 16, 2009. The provisions will become effective September 15, 2009.

Original source:
Adler, M. Peter. "Breach Notification Involving Protected Health Information" (Journal of AHIMA website), April 2009.
