



EMPLOYEE BENEFITS BULLETIN

September 10th, 2009

New HIPAA Breach Notification Requirements-Upcoming Compliance Deadline

The Health Information Technology for Economic and Clinical Health Act, known as the HITECH Act (the Act), was included as part of the American Recovery and Reinvestment Act of 2009 (ARRA). Subtitle D of the Act imposes new requirements under HIPAA that will impact covered entities and business associates. In particular, the Act creates new notification obligations around certain breaches of protected health information. On August 24, 2009, the Department of Health and Human Services (HHS) issued interim final regulations on breach notifications. These requirements will apply to breaches occurring on or after September 23, 2009. However, HHS will not impose sanctions for failure to provide the required notifications in the event of a breach until 180 calendar days from the publication of regulations (or February 20, 2010). The following is a general overview of the requirements.

A copy of the Final Rule is available at <http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>

Highlights

- A breach involves the unauthorized acquisition, access, use or disclosure of unsecured PHI that is in violation of the HIPAA Privacy Rule and compromises the security or privacy of such information. See the discussion of **“Avoiding a breach”**, below, for guidelines on how to secure PHI so as to remove it from the scope of these new rules. Note, however, that those security measures will not always be workable for normal business activities involving PHI, thus leaving covered entities and business associates with the task of complying with the new rules in the event of a breach.
- Covered entities and business associates will need to conduct a risk assessment to determine if a breach occurred and document this process.
- In the event of a breach, the covered entity must notify affected individuals that their information has been breached within 60 days. Business associates (TPAs, brokers, attorneys, etc.) will be required to notify the covered entity in the event of a breach.
- Breaches impacting 500 or more individuals will require media and HHS notification. Breaches impacting fewer than 500 individuals will need to be reported to HHS annually.

What is a breach?

The Act imposes new notification requirements on a covered entity and any business associate in the instance

where unsecured protected health information (PHI) is breached.

A **breach** means the unauthorized acquisition, access, use or disclosure of unsecured PHI that is in violation of the HIPAA Privacy Rule and compromises the security or privacy of such information.

A breach will compromise the security or privacy of PHI if it poses significant risk of financial, reputational, or other harm to the individual.

A breach does not include:

- A use or disclosure of PHI that is a limited data set and also excludes both the date of birth and zip codes of individuals.
- Any unintentional acquisition, access, or use of PHI by a person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure.
- Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
- A disclosure of PHI where a covered entity or business associate 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.

How do I know if PHI has been breached?

A determination of whether a breach occurred will be based on all the facts and circumstances. The guidance provides some steps that covered entities and business associates need to follow when dealing with a potential breach situation:

- Determine whether the use or disclosure of PHI violated the Privacy Rule.
- Determine whether the violation compromises the security or privacy of PHI. In other words, does the violation pose a significant risk of financial, reputational or other harm to an individual?
 - This will require covered entities and business associates to conduct a risk assessment. This assessment will determine whether a significant risk of harm to an individual exists as a result of the impermissible use or disclosure.
- Determine whether an exception applies.
- Document the findings of the risk assessment.

There's been a breach, now what?

Notification required by the Covered Entity

A covered entity must notify each individual whose unsecured PHI has been (or is reasonably believed to have been) accessed, acquired, used or disclosed as a result of a breach.

Timeliness of notification: Notification must be made without unreasonable delay and no later than 60 calendar days after the breach is discovered. An exception applies when law enforcement determines a notification would impede a criminal investigation or threaten national security.

Contents of the notice: Notification of a breach to an individual must include the following:

- Brief description of what happened, including date of breach and the date the breach was discovered, if known;
- Description of the types of unsecured PHI involved (e.g. full name, social security number, date of birth, address, account number, disability code);
- Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- Brief description of what the covered entity is doing to investigate the breach, mitigate harm to individuals, and to protect against future breaches; and
- Contact procedures for individuals to ask questions or to receive more information including a toll-free number, email address, Web site or portal address.

Individual notification

- **Written notice:** The covered entity must provide written notice to the individual's last known address. Notification may be provided in multiple mailings as information develops. Electronic notice (e.g. email) is only permissible in limited situations.
- **Substitute notice:** If there is insufficient or out-of-date contact information that precludes written notice, a substitute form of notice reasonably calculated to reach the individual must be provided. How this notice is provided depends on the number of individuals with insufficient or out-of-date information.
 - *Fewer than 10 individuals:* Telephone, email or other notification means may be used.
 - *10 or more individuals:* A conspicuous posting for 90-days on the covered entity's Web site or notice to major media (print or broadcast) where individuals are likely to reside will be required. Such notice must include a toll-free number for individuals to receive more information.
- **Urgent situations:** In the case of an urgent situation (i.e. possible imminent misuse of unsecured PHI), the covered entity may provide information via phone or other means as appropriate. This is in addition to the written notice requirement.

Media notification

- Applies when the breach involves 500 or more residents of a state or jurisdiction.
- Notice must be provided to prominent media outlets servicing the state or jurisdiction in which the

breach occurred. The same content and timing requirements that apply to the individual notice apply with respect to the media notice.

HHS notification

- In the event a breach involves 500 or more individuals, the covered entity must provide notification to HHS. The notice must be provided concurrent with the individual notice.
- For breaches affecting fewer than 500 individuals, the covered entity must maintain a log of any breaches, and provide this information annually to HHS.
- The content of the notifications to HHS is the same as described in the individual notice. The manner for submitting this notice will be described on the HHS Web site.

Notification required by the Business Associate

Following the discovery of a breach, the business associate must notify the covered entity without unreasonable delay and no later than 60 calendar days after discovery of the breach.

Notification must include, to the extent possible, the identity of each individual affected by the breach and any other available information that will assist the covered entity in satisfying the individual notification obligation.

Generally, the covered entity, and not the business associate, has the obligation to notify the affected individuals in the event of a breach. However, nothing in the law prohibits the covered entity from contractually obligating the business associate to provide the individual notification.

Avoiding a breach

HHS identified Encryption and Destruction as mechanisms to render PHI unusable, unreadable, or indecipherable to unauthorized individuals. PHI that is either encrypted or destroyed, in accordance with the requirements described below, cannot be breached. While these approved methodologies may be helpful in sufficiently securing some forms of PHI, it is likely some PHI will remain vulnerable to a breach.

Encryption

- Encryption applies with respect to electronic PHI (ePHI). The successful use of encryption will depend on two main features: the strength of the encryption algorithm, and the security of the decryption key or process.
- If using encryption, the key to encrypt or decrypt ePHI data should be kept on a separate device from where the ePHI is stored.
- For data in motion (data moving through a network – e.g. email), valid encryption processes would comply with the requirements described in the NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security Implementations*; 800-77, *Guide to IPsec VPNs*; or 800-113m *Guide to SSL VPNs*, and may include others which are FIPS 140-2 validated. (Available at : <http://www.csrc.nist.gov/>)

- For data at rest (data residing on a data system, file system or other structured storage mechanism – e.g. data stored on a server), valid encryption processes are consistent with the NIST Special Publication 800-111, *Guide to Storage Encryption for Technologies for End User Devices*. (Available at: <http://www.csrc.nist.gov/>. NIST Roadmap plans include the development of security guidelines for enterprise-level storage devices, and such guidelines will be considered in updates to this guidance, when available.)

Destruction

- Destruction is the recommended methodology for securing PHI in paper, film, or other hard copy media and for electronic media containing PHI (e.g. hard drives, disks, CDs, tapes, flash drives).
- For paper, film or other hard copy media, destruction means shredding the information or otherwise destroying it so PHI cannot be read or otherwise reconstructed. The regulations specifically exclude redaction as a means of data destruction.
- For electronic media, destruction means the information is purged, cleared, or destroyed so that such PHI cannot be retrieved, consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*. (Available at <http://www.csrc.nist.gov/>)

Implementing either of these methods will likely require coordination with technical resources.

Interaction with state law

State law provisions that are contrary to what is required by the regulations will be preempted. Where state law mirrors federal law or is more favorable, compliance with both state and federal law is required. For example, if state law requires notification within 5 days following detection of a breach, sending notice within that period complies with the 60-day notice requirement described in the new regulations.

Action items

Employers should do all of the following:

- Determine whether the employer and any business associates have PHI that may be vulnerable to a breach;
- Conduct and document a risk assessment if there is a violation of the Privacy Rule;
- Create a breach notification log to record the occurrence of a breach;
- Establish notification procedures;
- Update business associate agreements;
- Update HIPAA policies and procedures and train staff accordingly; and
- Review compliance requirements with carriers and business associates.

The *Employee Benefits Bulletin* is designed to highlight various employee benefit matters of general interest to our readers. It is not intended to interpret laws, regulations or to address specific client situations.