

Notice Requirements for Breach of Protected Health Information

Beginning on September 23, 2009, federal law titled the Health Information Technology for Economic and Clinical Health (HITECH) Act enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA), requires HIPAA-covered entities (including group health plans, health care providers and many employers) and their business associates (persons or entities that use or disclose PHI on behalf of a covered entity that are not members of the covered entity's workforce) to provide notice to their health plan participants, the Department of Health and Human Services (HHS) and in some cases the media after breaches of unsecured protected health information (PHI). Covered entities must continue to comply with any applicable state law or local law in addition to this new federal requirement.

Breach of Unsecured PHI Defined:

- Breach is the acquisition, access, use or disclosure of PHI in a manner not allowed by HIPAA privacy rules that compromises the security or privacy of the PHI. Security and privacy are compromised when a breach poses a significant risk of financial, reputational or other harm to an individual. =
- Unsecured PHI is information that has not been destroyed under an approved method or secured by technology that makes the PHI unusable, unreadable or indecipherable to unauthorized individuals. Electronic information that has been encrypted according to HIPAA security rules is considered secure.
- Exceptions:
 - Disclosures made where there is a good faith belief that the unauthorized person who received PHI would not reasonably be able to retain the information.
 - Disclosures made in good faith within the course and scope of employment that do not result in further disclosures.
 - Inadvertent disclosures by an authorized individual to another authorized individual at the same covered entity or business associate if the information is not further used or disclosed.

Notice Requirements:

1. **Individuals:** An employer health plan must notify each individual whose unsecured PHI was or is believed to have been improperly used or disclosed. Notices may be sent by first-class mail to the individual's last known address or by e-mail if the individual has agreed to receive electronic notices.
2. **Media:** For breaches affecting more than 500 residents of one state, county, city or town, the media must also be notified. This form of notice is usually done via a press release.
3. **Notices to HHS:** Employer-sponsored health plans must also notify HHS of a breach. If the breach involves 500 or more individuals, HHS must be notified at the same time individuals are notified. For breaches involving fewer than 500 individuals, the plan must track the breaches and notify HHS no later than sixty (60) days after the end of the calendar year. The 500-individual threshold is reached based on the total number of

individuals affected regardless of where they live. HHS will post notice content requirements on their website and employers experiencing a breach should refer to that site for specific instructions.

4. **Notices by Business Associates to Plan:** A third-party administrator, claims administrator, pharmacy benefit manager or other business associate to an employer-sponsored health plan is required to notify the plan itself of a breach.

Timing of Individual, Media and Business Associate Notices: Notices must be sent without unreasonable delays and no later than sixty (60) calendar days after discovery. Discovery occurs when the employer has actual knowledge of the breach by a member of the plan's workforce or an agent of the plan or if the breach would have been discovered had the employer practiced reasonable diligence. The regulations specify that if an employer has the necessary information to notify affected individuals within ten (10) days but do not notify until sixty (60), that employer is in violation of the regulations.

Content of Individual, Media and Business Associate Notices: Notices must be written in plain language and contain the following: date of the breach, a description of the breach, plans to mitigate damages and protect against future breaches, and steps affected participants should take to protect themselves.

Penalties for Noncompliance: Penalties range from \$100 to \$50,000 per violation capped at \$1.5 million per year.

What Employers Should Do:

- Review and revise policies and procedures to ensure PHI is secured. Implement procedures to comply with the breach notification requirements in the event any unsecured PHI is disclosed.
- Review and revise existing business associate agreements to insure that they require business associates to comply with the new notification requirements.
- Be aware of any state laws requiring notification to residents whose personal information was or may have been disclosed.