

Benefit Brief



SUBJECT: HIPAA Breach Notification and Business Associate Requirements

DATE: September 16, 2009

This Benefit Brief applies to employers whose health plans are subject to HIPAA Privacy and Security regulations and to all business associates.

In our April 2009 *BeneFlash*, we informed you that the privacy and security rules of the Health Insurance Portability and Accountability Act (HIPAA) have been expanded under the American Recovery and Reinvestment Act of 2009 (ARRA). The section of ARRA that deals with privacy and security of personal health information is known as the Health Information Technology for Economic and Clinical Health (HITECH) Act. The Department of Health and Human Services (HHS) recently issued guidance and implemented breach notification requirements as required by the HITECH Act. HIPAA-covered entities must notify individuals when their protected health information (PHI) is breached beginning September 23, 2009.

What is a breach?

This definition of "breach" is limited to PHI. Breach means the "unauthorized acquisition, access, use, or disclosure" of PHI in a manner not permitted by HIPAA privacy rules that "compromises the security or privacy" of the PHI. Security and privacy are considered to be compromised when a breach poses a "significant risk of financial, reputational, or other harm" to an individual.

What are the Notification Requirements?

Notices are only required when "unsecured" PHI is breached. PHI is "unsecured" if it has not been destroyed under an approved method, or secured by a technology developed or accredited by the American National Standards Institute which makes the PHI unusable, unreadable, or indecipherable to unauthorized individuals. (HHS will annually issue guidance specifying the approved technology and methodology to make PHI secure.) If a breach occurs, the HIPAA-covered entity (health plan) must send the following notices:

- **Notice to Individuals:** HIPAA-covered entities must notify individuals that their health information was, or is believed to have been, breached. Notices must be provided "without unreasonable delay" and within 60 days of "discovery" (the actual knowledge of the breach or when the breach would have been discovered by exercising reasonable diligence). Notices should be sent by first-class mail to the last known address or by email if the individual has agreed to receive information electronically. Notices must be written in plain language and include:
 - a brief description of the breach, including the date of the breach and date of discovery;
 - the type of PHI involved (full name, SSN, date of birth, home address, account number, diagnosis, disability code, etc.);
 - steps affected individuals should take to protect themselves;
 - a brief description of steps the covered entity is taking to investigate, alleviate damage, and protect against future breaches; and
 - contact information for affected individuals to ask questions.
- **Notice to the Media:** If a breach affects more than 500 residents of one state or jurisdiction, prominent media serving the area must be notified in a press release. This notice should contain the same information as the individual notice and be provided within the same timeframe.

- **Notice to HHS:** HIPAA-covered entities must notify HHS of any breach of unsecured PHI. If the breach involves 500 or more individuals, HHS must be notified when the individuals are notified. If the breach involves fewer than 500 individuals, HHS must be notified within 60 days of the end of the calendar year.

How are Business Associates Affected?

A business associate (broker, third party administrator, consultant, or advisor) provides a service to health plans that involves the use or disclosure of PHI. The HITECH Act has made HIPAA privacy and security rules applicable directly to business associates. Previously, only covered entities such as health plans and health care providers were subject to HIPAA rules. Business associates are now subject to the following requirements:

- **Administrative safeguards:** implement policies and procedures to prevent, detect, contain, and correct security violations. This includes risk analysis and management, regular review of records, employee training, sanctions for employees who violate policies, designating a security official, implementing workforce security, establishing a contingency plan, and developing plans for data backup, disaster recovery, and emergency mode operation.
- **Physical safeguards:** implement policies and procedures to limit physical access to electronic information systems and facilities in which they are housed. This includes developing a facility security plan, controlling employees' access to facilities based on role or function, controlling receipt and disposal of hardware and PHI, and documenting repairs.
- **Technical safeguards:** implement policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights. This includes assigning unique names or numbers for identifying and tracking user identities, establishing procedures for obtaining necessary electronic PHI during an emergency, and implementing a mechanism to encrypt and decrypt electronic PHI.
- **Policies, procedures, and documentation requirements:** implement reasonable and appropriate policies and procedures to comply with the requirements, and maintain those policies and procedures in written form. Retain the documentation for six years from the date of its creation or the date it was last in effect, whichever is later. Make documentation available to those responsible for implementing the procedures.
- **Civil and criminal penalties:** business associates who violate any HIPAA privacy and security rules shall be subject to the same penalties that apply to covered entities that violates such rules.
- **Notification to health plan (employer) of a breach:** business associates who discover a breach of unsecured PHI must notify the covered entity without unreasonable delay and within 60 days of discovery. The covered entity will notify the affected individuals as noted above.

How Can You Avoid the Notification Requirement?

HIPAA-covered entities and business associates should take necessary steps to secure PHI. The two methods approved by HHS to secure health information are encryption and destruction. Electronic PHI must be encrypted according to HHS-approved standards to be considered secure under HIPAA security rules and exempt from the notification requirement. Paper, film, or other hard PHI must be completely destroyed so that it cannot be read or reconstructed.

What are the Penalties?

ARRA increases enforcement and penalties for violations of the HIPAA privacy and security rules. HHS is required to conduct periodic audits to ensure that covered entities and business associates comply with privacy and security rules. Civil penalties increased from \$100 per violation to \$1,000 or more per violation. Criminal penalties can apply to individuals who wrongfully obtain or disclose PHI maintained by a covered entity. HHS has said it will not impose penalties for failing to provide notification for breaches that are discovered before February 2010. However, HHS still expects covered entities and business associates to comply with the rule and will work with them through technical assistance and voluntary corrections.

What Do Employers and Business Associates Need to Do?

Employers and business associates who have electronic or paper PHI should take necessary steps to encrypt or destroy the information to avoid a breach. Employers should update HIPAA privacy and security

policies and procedures to determine when a breach has occurred and comply with the new notification rules. Breach notices should be developed and employees who have access to PHI should be trained on the requirements. Business associate agreements should be revised to include their responsibility to notify the employer of a breach and timing of notification. Business associates should prepare and adopt privacy and security policies and procedures by February 17, 2010, if they don't already have them.

If Benecon prepared your HIPAA policies and documents, we will make the necessary revisions for you.

If you have questions about the breach notification or business associate requirements, please contact Danielle Omans at The Benecon Group at domans@benecon.com or the number below.

This Benefit Brief is provided for informational purposes only and does not constitute legal advice. The Benefit Brief contains only a summary of the applicable legal provisions and does not purport to cover every aspect of any particular law, regulation or requirement. Depending on the specific facts of any situation, there may be additional or different requirements. Please use this Benefit Brief as a guide and not as a definitive description of your compliance obligations.