

Legislative Brief

Changes to HIPAA Rules: HHS Guidance on Securing PHI for Breach Notification Requirements



On February 17, 2009, the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act" or "Act") was passed as part of the American Recovery and Reinvestment Act of 2009 (ARRA). The HITECH Act included a requirement that certain breaches of unsecured Protected Health Information (PHI) be reported. On April 17, 2009, as directed by the Act, the Department of Health and Human Services (HHS) issued guidance (the "HHS Guidance") regarding whether PHI is unsecured. The HHS Guidance specifies the technologies and methodologies that render PHI "unusable, unreadable, or indecipherable to unauthorized individuals."

HHS also issued interim final regulations regarding the reporting requirements (the "Breach Notification Rule") on August 24, 2009. The Breach Notification Rule updates the HHS Guidance. The Breach Notification Rule and the HHS Guidance are effective for breaches occurring on or after **September 23, 2009**.

This issue of the Midlands Financial Benefits, Inc. Legislative Brief provides you with an overview of ARRA's security breach notification requirements and the related HHS regulations and guidance.

SECURITY BREACH NOTIFICATION REQUIREMENT

What is the Security Breach Notification Requirement?

The Health Insurance Portability and Accountability Act (HIPAA) did not originally require Covered Entities to report breaches of privacy or security of PHI. The HITECH Act and the Breach Notification Rule now require Covered Entities to notify individuals whose "unsecured PHI" has been breached. If the breach involves PHI held by a Business Associate, the Business Associate must notify the Covered Entity.

The Act did not specify when PHI is considered to be "secure" or "unsecure." Instead, it directed HHS to issue guidance regarding which technologies and methodologies are considered secure by April 18, 2009. The guidance was to specify the technologies and methodologies that render PHI "unusable, unreadable or indecipherable to unauthorized individuals."

What is a Security Breach?

For purposes of the Breach Notification Rule, a breach is the unauthorized acquisition, access, use or disclosure of PHI that compromises the security or privacy of the information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

There are exceptions to this definition for the following situations, if the information is not further acquired, accessed, used or disclosed:

- The unauthorized acquisition, access or use of PHI is unintentional and made by an employee or individual acting under authority of a Covered Entity or Business Associate if the acquisition, access or use was made in good faith and within the course and scope of the employment or other professional relationship; or
- An inadvertent disclosure occurs by an individual who is authorized to access PHI at a facility operated by a Covered Entity or Business Associate to another similarly situated individual at the same facility.

Legislative Brief

Changes to HIPAA Rules: HHS Guidance on Securing PHI for Breach Notification Requirements

When Must the Notification of a Security Breach be Provided?

Notification must be made without unreasonable delay and no later than 60 days after the discovery of the breach. However, notification must be delayed if a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security.

How Must the Notification of a Security Breach be Provided?

The Act specifies the following methods of providing the notice:

- Written notice by first-class mail (or by e-mail, if specified by the individual).
- If there is insufficient or out-of-date contact information, substitute notice, such as conspicuous posting on the Covered Entity's website or notice in major print or broadcast media.
- In urgent cases where there is a possibility of imminent misuse of the unsecured PHI, notice by telephone or other method (in addition to the above methods).
- Notice to "prominent media outlets" within the state or jurisdiction if the breach affects more than 500 individuals of that state or jurisdiction.
- Notice to HHS of all breaches. Notice must be provided immediately for breaches involving more than 500 individuals and annually for all other breaches. HHS will post breaches involving more than 500 individuals on its website (www.hhs.gov).

What Information Must the Notification Include?

The Act requires the notice to include the following information:

- A description of the breach, including the date of the breach and date of discovery;
- The type of PHI involved (such as full name, Social Security number, date of birth, home address or account number);
- Steps individuals should take to protect themselves from potential harm resulting from the breach;
- Steps the Covered Entity is taking to investigate the breach, mitigate losses and protect against future breaches; and
- Contact procedures for individuals to ask questions or learn additional information, including a toll-free telephone number, e-mail address, website or postal address.

HHS GUIDANCE REGARDING UNSECURED PHI

What Does the HHS Guidance Say About Unsecured PHI?

The HHS Guidance states that, if PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals by one or more of the methods identified in the HHS Guidance, then that information is not "unsecured" PHI. Because the breach notification requirements apply only to breaches of unsecured PHI, the HHS Guidance provides information

Legislative Brief

Changes to HIPAA Rules: HHS Guidance on Securing PHI for Breach Notification Requirements

for Covered Entities and Business Associates to use to determine whether the notification obligations apply to a particular breach.

What Methods are Identified in the HHS Guidance for Securing PHI?

The new HHS Guidance states that HHS has identified two methods for rendering PHI in paper or electronic form unusable, unreadable or indecipherable to unauthorized individuals: **encryption and destruction**. These technologies and methodologies are intended to be exhaustive and not merely illustrative. However, HHS may issue guidance regarding additional technologies and methodologies in the future.

Encryption

Under the HHS Guidance, electronic PHI has been rendered unusable, unreadable or indecipherable to unauthorized individuals if it is encrypted by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” and the confidential process or key has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt.

The following encryption processes meet this standard:

- Valid encryption processes for data at rest are those that are consistent with the National Institute of Standards and Technology (NIST) Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices* (available at www.csrc.nist.gov); and
- Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2.¹

HHS has clarified in the updated guidance that “data in motion” includes data that is moving through a network, including wireless transmission, whether by e-mail or structured electronic interchange. “Data at rest” includes data that resides in databases, file systems, flash drives, memory and any other structured storage method.

Destruction

If PHI is destroyed prior to disposal in accordance with the HHS Guidance, no breach notification is required following access to the disposed hard copy or electronic media by unauthorized persons.

PHI is considered destroyed in accordance with the HHS Guidance if the media on which the PHI is stored or recorded has been destroyed in one of the following ways:

- Paper, film or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed (this does not include redaction); or
- Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitation*, such that the PHI cannot be retrieved.

¹ These include, as appropriate, standards described in NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, 800-77, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs*, and may include others that are FIPS 140-2 validated.

Legislative Brief

Changes to HIPAA Rules: HHS Guidance on Securing PHI for Breach Notification Requirements

Are Covered Entities Required to Follow the HHS Guidance?

No, Covered Entities and Business Associates are not required to follow the HHS Guidance. However, the security breach notification rules apply only to unsecured PHI. Therefore, if Covered Entities and Business Associates use the specified technologies and methodologies to secure PHI, they do not have to provide notification if there is a security breach involving that PHI.

Does the HHS Guidance Apply to De-Identified Information?

No, the HHS Guidance does not address the use of de-identified information as a way to render PHI unusable, unreadable or indecipherable to unauthorized individuals. Once PHI has been de-identified in accordance with the HIPAA Privacy Rule, it is no longer PHI and no longer subject to the HIPAA Privacy and Security Rules.

However, HHS specifically states that nothing in the HHS Guidance should be construed as discouraging Covered Entities and Business Associates from using de-identified information to the maximum extent practicable.

Does the HHS Guidance Address How to Protect PHI?

No, the HHS Guidance is not intended to inform Covered Entities and Business Associates how to prevent breaches involving PHI. The HHS Guidance states that it does not change a Covered Entity's Privacy and Security Rule obligations. Covered Entities must comply with the HIPAA Privacy and Security Rules by conducting risk analyses and implementing physical, administrative and technical safeguards that are reasonable and appropriate.

What is the Effective Date of the HHS Guidance?

The Breach Notification Rule and the HHS Guidance apply to breaches that occur on or after **September 23, 2009**.

Please contact your Midlands Financial Benefits, Inc. representative with any questions.

This Midlands Financial Benefits, Inc. Legislative Brief is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice.

Content copyright © 2009 Zywave, Inc. Images copyright © 2000 Getty Images, Inc. All rights reserved.

4/09; EM 9/09