[buck research]

fyi® for your information®

Volume 32 | Issue 53 | September 4, 2009

HHS Issues Regulations on Security Breach Notification Requirements

The American Reinvestment and Recovery Act (ARRA), enacted earlier this year, significantly expanded the health information privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and added new breach notification requirements. The Department of Health and Human Services (HHS) has issued interim final regulations on these requirements, which apply to HIPAA covered entities and business associates, effective September 23, 2009.

Background

Along with its portability provisions, HIPAA provides important rules for protecting the privacy and security of an individual's protected health information (PHI). Major changes to HIPAA were included in the Health Information Technology for Economic and Clinical Health Act (HITECH), a section of ARRA. HITECH added new notification requirements for covered entities and business associates that have a breach with respect to unsecured PHI, or reasonably believe a breach has occurred. Importantly, the requirements do not apply to secured PHI (i.e., information that is properly encrypted or completely destroyed) or to information that has been de-identified in accordance with federal regulations.

HHS has now issued interim final regulations implementing the breach notification requirements under HITECH. The Federal Trade Commission (FTC), which has enforcement authority over breach notification requirements for vendors of personal health records and related entities, has issued similar regulations, but these are not discussed in this *For Your Information*.

HHS Interim Final Regulations

The HHS interim regulations define what constitutes a breach, and explain what steps covered entities and their business associates must take when they discover a breach of the PHI that they maintain.

Breach Defined

The regulations define breach as "the acquisition, access, use or disclosure" of PHI in a manner not otherwise permitted under the HIPAA privacy rule and "which compromises the security or privacy" of the PHI. Security or privacy would be compromised if the individual whose PHI was improperly accessed would be at serious risk of financial, reputational or other harm. The regulations provide exceptions for unintentional access or use or inadvertent disclosure.

BUCK COMMENT. *Entities will want to assess whether a potential acquisition, access, use or disclosure is permitted under the privacy rule, and if not, determine whether it actually poses a significant risk of harm to affected individuals or is otherwise excepted.*

When Notification of a Breach is Required

Importantly for plan sponsors, the regulations clarify that not every impermissible acquisition, access, use or disclosure of PHI will be considered a breach subject to the notification procedures. In analyzing whether notification is required, a plan can take into account several factors.

Security. If the PHI is held in a manner deemed to be "secure" under the regulations, notification of the breach is not required. PHI will be considered secured if –

- Electronic data is protected by specified encryption technology.
- Paper or film records have been shredded or destroyed.
- Electronic media have been purged in accordance with National Institute of Standards and Technology Guidelines for Medical Sanitation.

For example, if a laptop protected by whole disk encryption is lost or stolen, no notification would be required for any PHI stored on the laptop.

BUCK COMMENT. *The regulations make clear that the use of firewalls and access controls alone would not be sufficient to render the data secure.*

Adequate Retrieval. HHS has provided examples of situations in which notification would not need to be given because proper retrieval occurred before any improper use –

- A stolen laptop is retrieved and forensic analysis shows that the PHI was not opened, altered, transferred or otherwise compromised.
- EOBs are mailed to the wrong address and are returned (unopened) to the sender.

Disclosure to Another Covered Entity. The new rules suggest that if data is misdirected to a HIPAA covered entity (such as where a vendor sends data files to the wrong client), there will be no notification required if the covered entity whose data was misdirected takes immediate steps to mitigate any impermissible use or disclosure.

Insignificant Risk. An example of a PHI breach that provides so little information about a patient's care that the disclosure will be deemed an insignificant risk is the disclosure of a list of persons treated at a particular hospital. However, HHS notes that the risk could increase to significant if the type of services rendered, Social Security numbers (SSNs), or other identifiers were included.

BUCK COMMENT. *These examples provide welcome guidance on actions plan sponsors can take to mitigate HIPAA breaches.*

Notification Requirements

If notification is required, it must be provided to each individual whose unsecured PHI has been breached or is believed to have been compromised. Additional notification requirements apply if the breach affects 500 or more individuals, or involves more than 500 residents of a state or smaller geographic area. In each of these circumstances, the burden of proving compliance with the notice requirements is on the covered entity or business associate.

Timing. The notice must be provided to individuals of a breach of their unsecured PHI without unreasonable delay and no later than 60 days after the breach is first discovered or reasonably should have been known by the covered entity. Discovery is deemed to occur on the first day that it is known to any member of the covered entity (other than the one responsible for the breach).

A business associate is required to notify the covered entity upon discovery of the breach. When the business associate is an independent contractor, it must notify the covered entity within 60 days of the discovery of the breach, and the covered entity, in turn, would have up to 60 days to notify the individual. If, however, the business associate is an "agent" of the covered entity, discovery by the business associate will be considered discovery by the covered entity, starting the 60 day clock to notify the affected individual.

Content. The notice must include –

- a brief description of the breach, the date of the breach and the date of the discovery of the breach
- a description of the types of unsecured PHI involved (e.g., full name, SSN, etc.), but not the actual information
- steps individuals can take to protect themselves from potential harm
- a brief description of what the covered entity is doing to remedy and mitigate the effects of the breach
- contact procedures, including a toll-free telephone number, email address, website or postal address, for questions and further information.

For a business associate, the notice to the covered entity should identify each individual affected by the breach.

Form of Notice. The notice must be written in plain language, and may be in electronic form, by agreement. However, if the need for a notice is urgent because of "possible imminent misuse" of the information, then notice may be provided via telephone or other appropriate means.

When there is insufficient contact information for affected individuals, the regulations allow a substitute notification process – i.e., a 90-day posting on the entity's website home page or conspicuous notice in major print or broadcast media in the area where most affected individuals are likely to reside. The covered entity must also maintain a toll-free telephone number for at least 90 days so an individual can learn whether his or her PHI may be included in the breach.

Breaches Involving More than 500 Residents of a State. The regulations provide that for breaches involving more than 500 residents of a state or jurisdiction, the covered entity must notify "prominent media outlets" serving the state or jurisdiction within 60 days of discovery of the breach. The content noted above should be included.

Notification to HHS. HHS is to be notified of breaches as follows –

- When the security of 500 or more individuals' information is breached, notice must be provided to HHS contemporaneously with notice to the individuals (within 60 days after the breach is discovered).
- When less than 500 individuals are involved, the covered entity is to maintain a log of the breaches and provide notice to HHS within 60 days after the end of each calendar year. The first filing will be required by March 1, 2010, and must include any breaches occurring on or after September 23, 2009.

State Laws

Consistent with the construction of HIPAA generally, the regulations indicate that state notification laws will not be preempted unless they stand "as an obstacle" to the purposes of HITECH. Thus, as long as it is possible to meet a more generous state law provision, it would have to be followed.

Effective Date

The breach notification requirements take effect on September 23, 2009. Although HHS has adopted a non-enforcement policy that will generally allow HIPAA covered entities and their business associates an additional five months, or until February 22, 2010, to come into compliance, they should begin working toward compliance now.

Conclusion

The latest regulations provide useful guidance. If they have not already done so, covered entities should inventory whatever protected health information they maintain to assess whether it is secured or unsecured and identify the compliance issues they may face over the next few months. Plans should establish notice procedures as well as procedures to capture and maintain necessary data in breach logs. Covered entities and business associates should reach clear understandings with respect to what the new regulations require, and their respective compliance roles. Personnel should be trained and privacy policies updated for the new rules.

Buck's consultants would be pleased to discuss these rules with you, and assist in your compliance efforts.