GROOM LAW GROUP

Christy Tinnes, Groom Law Group
202-861-6603 / cat@groom.com

CHART YOUR HIPAA COURSE . . .

HHS ISSUES GUIDANCE ON PHI THAT WILL BE SUBJECT TO SECURITY BREACH NOTIFICATION RULES

On April 27, 2009, the Department of Health and Human Services (HHS) issued guidance on what type of protected health information (PHI) will be considered "secure," and thus, exempt from the new HIPAA security breach notification requirements under the HITECH Act. The HITECH Act was passed on February 17, 2009 as part of President Obama's stimulus bill. The HITECH Act makes significant changes to the HIPAA privacy and security rules, including requiring a HIPAA covered entity (or a personal health records vendor) to notify an individual if there has been a security breach involving the individual's PHI.

The Act required HHS to issue guidance within 60 days of enactment that specifies which technologies will be considered "secure" and thus, not subject to the notification rule. This guidance was published in the Federal Register on April 27, 2009. *See* 74 Fed. Reg. 19006.

The HHS guidance sets out the technologies that will be considered "secure" and asks a number of specific questions about other types of technologies HHS should consider "secure." In addition, the guidance requests comments on the security breach notification requirement in general (for which HHS is required to issue regulations by August 16, 2009). The security breach notification rules will be effective 30 days after interim final regulations are issued.

Below is a summary of the technologies HHS has determined will produce "secure" PHI (and thus be exempt from the security breach notification requirements). Also below is a list of the questions on which HHS specifically has requested comments.

Comments must be submitted on or before May 21, 2009.

A. Guidance on "Secure PHI"

The HHS guidance provides "the functional equivalent of a safe harbor" from the new security breach notification requirement to the extent a covered entity holds "secure PHI." HHS says "secure PHI" is PHI that has been rendered by technology to be "unusable, unreadable, or indecipherable."

HHS provides two methods that would meet this requirement and says that this list is "intended to be exhaustive and not merely illustrative" (meaning that these technologies would be the only means by which PHI would be considered "secure" and thus, exempt from the security breach notification requirements).

The two methods are:

1. Encryption – PHI will be considered rendered unusable, unreadable, or indecipherable if it has been encrypted by an algorithmic process to transform data into a form where there is low probability of assigning meaning without use of a confidential process or key, and such confidential process or key has not been breached. HHS identifies specific encryption processes that it believes meet this standard. *See* NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices, and Federal Information Processing Standards (FIPS) 140-2.

2. Destroyed PHI – PHI also will be considered unusable, unreadable, or indecipherable if it has been shredded or destroyed such that it cannot be read or otherwise reconstructed (for paper or hard copy) or has been cleared, purged, or destroyed consistent with specific NIST standards (for electronic media). *See* NIST Special Publication 800-99, Guidance for Media Sanitization.

B. HHS Request for Comments

Other Methodologies to Create "Secure PHI"

HHS specifically asked for comments on the following questions concerning other methodologies that would create "secure" PHI:

1. Other Media Configurations - Are there particular electronic media configurations that may render PHI unusable, unreadable, or indecipherable to unauthorized individuals, such as a fingerprint protected Universal Serial Bus (USB) drive, which are not sufficiently covered by the above and to which guidance should be specifically addressed?

2. Paper PHI - With respect to paper PHI, are there additional methods the Department should consider for rendering the information unusable, unreadable, or indecipherable to unauthorized individuals?

3. Other Methods Generally - Are there other methods generally the Department should consider for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals?

4. Circumstances When Adopted Methods Would Fail - Are there circumstances under which the methods discussed above would fail to render information unusable, unreadable, or indecipherable to unauthorized individuals?

5. Limited Data Set Risk of Re-Identification - Does the risk of re-identification of a limited data set warrant its exclusion from the list of technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals? Can risk of re-identification be alleviated such that the creation of a limited data set could be added to this guidance?

6. Limited Data Set & Compliance with Notification Rules - In the event of a breach of protected health information in limited data set form, are there any administrative or legal concerns about the ability to comply with the breach notification requirements?

7. Off-the-Shelf Products - Should future guidance specify which off-the-shelf products, if any, meet the encryption standards identified in this guidance?

Breach Notification Provisions Generally

HHS also asked for comments on the breach notification requirement generally and said it would use this information to develop its interim final regulations on breach notification.

1. Conflicts with State Breach Notification Law - Based on experience in complying with state breach notification laws, are there any potential areas of conflict or other issues the Department should consider in promulgating the federal breach notification requirements?

2. Multiple Notices Under State Laws - Given current obligations under state breach notification laws, do covered entities or business associates anticipate having to send multiple notices to an individual upon discovery of a single breach? Are there circumstances in which the required federal notice would not also satisfy any notice obligations under the state law?

3. States Not Recognizing "Secure PHI" Standard - Considering the methodologies discussed in the guidance, are there any circumstances in which a covered entity or business associate would still be required to notify individuals under state laws of a breach of information that has been rendered secured based on federal requirements?

4. Exceptions to "Breach" Definition - The Act's definition of "breach" provides for a variety of exceptions, including: (1) where unauthorized access is "unintentional" and made by an individual acting under authority of the plan if such access was made in good faith and within the course and scope of employment, and such information was not further accessed or disclosed; and (2) where information is "inadvertently" disclosed by an individual who is authorized to access PHI at a facility operated by a plan to another similarly situated individual at the same facility, as long as the PHI is not further accessed or disclosed. To what particular types of circumstances do entities anticipate these exceptions applying?

+ + +