PUBLICATION

HHS Issues Guidance on Unsecure PHI and Requests Comments on Guidance and Breach Notification Rules

April 30, 2009

On April 17, 2009, the United States Department of Health & Human Services (HHS) issued guidance specifying the technologies and methodologies that can be used to secure protected health information (PHI), making paper or electronic PHI unusable, unreadable, or indecipherable to unauthorized individuals. The guidance provides a safe harbor to the new breach notification requirements mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act portion of the American Recovery and Reinvestment Act of 2009 (ARRA or Stimulus Package). In the same document, HHS also solicited public comments to the guidance and to the new breach notification requirements. Comments must be submitted on or before May 21, 2009.

The guidance is a first step in understanding how the Obama administration will continue to develop the handling of the privacy and security of PHI and the notification requirements should a breach occur. The guidance is effective upon issuance; however, it will apply to breaches 30 days after the Interim Final Regulations on the same subject are issued by HHS. HHS will update the guidance as needed (based on public comments) prior to or concurrently with the forthcoming regulations.

Background

The HITECH Act, signed into law on February 17, 2009, was enacted as part of the Stimulus Package. The HITECH Act dramatically altered the requirements of the Health Insurance Portability and Accountability Act of 1996 Privacy Rule and Security Standards (HIPAA).

Among other new HIPAA requirements, the HITECH Act mandates patient notification for breaches of unsecured PHI – similar to many state consumer protection or financial data laws. Unsecured PHI is defined in the HITECH Act to mean PHI that is not secured (i.e., has not been rendered "unusable, unreadable, or indecipherable") through the use of a technology or methodology specified in the HHS guidance.

HHS Guidance

The new HHS guidance establishes that PHI is rendered "unusable, unreadable, or indecipherable" (and is thereby secure) to unauthorized individuals if one or more of the following applies:

1) Electronic PHI has been encrypted as specified in the HIPAA Security Rule 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 such confidential process or key that might enable decryption has not been breached. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and are judged by HHS to meet this standard.

i) Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*.

ii) Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140- 2. 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 which are FIPS 140-2 validated.

2) The media on which the PHI is stored or recorded has been destroyed in one of the following ways:

i) Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed.

ii) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*, such that the PHI cannot be retrieved.

Covered entities and business associates are not required to follow the HHS guidance, but compliance with the guidance provides a functional safe harbor to the breach notification requirements – meaning that entities that comply with the guidance will be deemed to have secure PHI. In other words, if an entity that is otherwise subject to the notification requirements applies the NIST technologies and methodologies specified in the HHS guidance in order to secure paper and electronic PHI, that entity will not be required to provide the notifications in the event paper or electronic information is breached.

The HHS guidance also reiterates that de-identified information is not subject to HIPAA; therefore, deidentified information is deemed secure and exempt from notification requirements.

The HHS guidance correlates with two breach notification regulations – one to be issued by HHS for HIPAA covered entities and their business associates (Sec. 13402 of HITECH Act) and one recently proposed by the Federal Trade Commission (FTC) for vendors of personal health records and other non- HIPAA covered entities (Sec. 13407 of HITECH Act). The HITECH Act requires these regulations to be published within 180 days of February 17, 2009.

Public Comments and Information Requested

In addition to the HHS guidance, HHS has concurrently issued a request for information (RFI) soliciting public comment on the breach notification provisions of the HITECH Act to inform future rulemaking and updates to the HHS guidance. Once published in the Federal Register, the guidance and RFI will also be available for public comment at www.regulations.gov.

HHS has specifically requested comments be made on the following HHS guidance questions.

1. 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 With respect to paper PHI, are there additional methods HHS should consider for rendering the information

. unusable, unreadable, or indecipherable to unauthorized individuals?

3. Are there other methods generally HHS should consider for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals?

4. Are there circumstances under which the methods discussed above would fail to render information unusable, unreadable, or indecipherable to unauthorized individuals?

5. 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. In the event of a breach of PHI in limited data set form, are there any administrative or legal concerns about the ability to comply with the breach notification requirements?

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

In addition to public comment on the HHS guidance, HHS also requests comments concerning any other areas or issues pertinent to the development of its Interim Final Regulations for breach notification. In particular, HHS is interested in comment on the following areas:

1. Based on experience in complying with state breach notification laws, are there any potential areas of conflict or other issues HHS should consider in promulgating the federal breach notification requirements?

2. 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. Considering the methodologies discussed in HHS 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. The HITECH Act's definition of "breach" provides for a variety of exceptions. To what particular types of circumstances do entities anticipate these exceptions applying?

Potential Action Items:

- *Covered entities should add provisions to their Business Associate Agreements requiring business associates to comply with the NIST standards and other safe harbors noted in the April 17, 2009 guidance.*
- *Confirm that PHI held by your entity meets NIST standards/safe harbor.*
- *Comment on breach notice requirements.*
- *Comment on HHS guidance.*
- *Watch for HHS breach notification proposed rules.*