

## Health Care ADVISORY

April 22, 2009

### HHS Releases Long Awaited Guidance for Securing PHI

On April 17, the Secretary of the Department of Health and Human Services (HHS) issued guidance relating to the technologies and methodologies for rendering protected health information (PHI)<sup>1</sup> secure for purposes of health breach notifications.<sup>2</sup> The guidance identifies technologies and methodologies for ensuring that PHI is unusable, unreadable or indecipherable to unauthorized individuals, as mandated by Section 13402(h)(2) of the American Recovery and Reinvestment Act of 2009 (ARRA).<sup>3</sup> ARRA required that HHS issue such guidance within 60 days of the law's enactment and annually thereafter.

According to HHS, the guidance is effective as of its issuance. However, HHS is seeking comments through May 21, 2009, on the methodologies and technologies specified in the guidance, as well as whether additional methodologies and technologies should be included. Based on the public's comments, HHS may modify and reissue its guidance. This advisory highlights the two methodologies chosen by HHS to secure PHI and the areas where HHS is seeking comments and additional information from the public.

#### Overview

The HHS guidance identifies the technologies and methodologies that can be used to render PHI unusable, unreadable or indecipherable to unauthorized individuals. ARRA defines "unsecured [PHI]" as PHI that is not secured through the use of a technology or methodology specified by the Secretary in guidance.<sup>4</sup> This definition is significant because the breach notification requirements for covered entities subject to the Health Insurance Portability and Accountability Act (HIPAA) and

---

<sup>1</sup> Protected health information (PHI) is individually identifiable health information transmitted or maintained by a covered entity or its business associates in any form or medium. See 45 C.F.R. § 160.103.

<sup>2</sup> Office of the Secretary, "Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for Information," *available at* <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechrfi.pdf>.

<sup>3</sup> American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5.

<sup>4</sup> ARRA at § 13402(h)(1)(A).

This advisory is published by Alston & Bird LLP to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered attorney advertising under court rules of certain jurisdictions.

their business associates are triggered in the event that unsecured PHI is breached.<sup>5</sup> Similarly, non-HIPAA covered entities, such as vendors of personal health records (PHR)<sup>6</sup> and PHR related entities, will be subject to the Federal Trade Commission's (FTC) breach notification requirements for the breach of an individual's PHR.<sup>7</sup>

This guidance, therefore, instructs HIPAA covered entities and their business associates (as well as PHR vendors and PHR related entities) as to the specific technologies and methodologies that secure PHI for purposes of the breach notification requirements. The guidance is intended to be used by these entities as a way of determining whether unsecured PHI has been breached, thereby triggering the notification requirements. According to HHS, if the specified technologies and methodologies are used to secure an individual's health information, these entities are "safe harbored," and, thus, not required to provide notification as otherwise required. Covered entities and business associates, however, will still be required to comply with all other federal and state statutory and regulatory obligations that may apply following a breach of PHI.

## Methodologies

In issuing its guidance, HHS consulted with various stakeholders. In particular, HHS consulted with external experts in health informatics and security, including representatives from several federal agencies. HHS, in consultation with the National Institute of Standards and Technology (NIST), identified two acceptable methods for securing PHI—encryption and destruction.

## Encryption

Encryption is one of the methods for securing electronic PHI from unauthorized access and use. HHS observes that the successful use of encryption depends upon two key features: (1) the strength of the encryption algorithm and (2) the security of the decryption key or process. The guidance provides that encryption requires 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," as specified in the HIPAA Security Rule.<sup>8</sup> In addition, the guidance requires that the confidential processes or keys that might enable decryption have not been breached. NIST has already tested two encryption processes that have been determined to meet this standard.

---

<sup>5</sup> Section 13402(j) of ARRA requires the Secretary to issue interim final regulations for breach notification by entities subject to HIPAA and their business associates within 180 days of ARRA's enactment. The Secretary has not yet issued these regulations.

<sup>6</sup> A personal health record (PHR) is "an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." See 74 *Fed. Reg.* 17914, 17916 (April 20, 2009), available at <http://edocket.access.gpo.gov/2009/pdf/E9-8882.pdf>.

<sup>7</sup> In accordance with Section 13407 of ARRA, the Federal Trade Commission (FTC) recently proposed its health breach notification rule requiring vendors of PHR and related entities to notify individuals when the security of their individually identifiable health information is breached. See 74 *Fed. Reg.* 17914.

<sup>8</sup> 45 C.F.R. § 164.304 (see definition of "encryption").

## ***Destruction***

Destruction is the second methodology identified by HHS to secure PHI. HHS specifies that destruction can occur 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 reconstructed.
- Electronic media have been cleared, purged or destroyed consistent with NIST Special Publication 800-88, *Guidelines of Media Sanitization*, such that the PHI cannot be retrieved.

## **Request for Comments on Guidance**

Given that the identified methodologies and technologies are intended to be exhaustive, and not merely illustrative, HHS is seeking comments regarding its guidance by May 21, 2009. In particular, HHS is requesting comments on the following:

- 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?
- With respect to paper PHI, are there additional methods that should be considered?
- Are there other methods, generally, that HHS should consider for securing PHI?
- Are there circumstances under which the two specified methods discussed above would fail to render the information secure?
- Does the risk of re-identification of a limited data set warrant its exclusion from the list of technologies and methodologies that render PHI secure? Can the risk of re-identification be alleviated such that the creation of a limited data set could be included as an accepted methodology?
- 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?
- Should future guidance specify which off-the-shelf products, if any, meet the encryption standards identified in this guidance?

## Request for Information

In its guidance, HHS also uses this opportunity to request comments relating to any other areas or issues relevant to the development of HHS' forthcoming interim final regulations for breach notification. HHS is particularly interested in comments on the following topics:

- Given state breach notification laws, are there any potential areas of conflict or other issues HHS should consider in promulgating the federal breach notification requirements?
- Do covered entities or business associates anticipate having to send multiple notices to an individual upon discovery of a single breach in light of current state law obligations? Are there circumstances where the required federal notice would not also satisfy any state obligation?
- To what particular circumstances do entities anticipate that the exceptions to the definition of "breach" would apply?

## Conclusion

This guidance document marks the beginning of forthcoming HHS guidance and regulations relating to the HIPAA security and privacy changes that were required under ARRA. Following the issuance of this guidance, HHS is required to issue its interim final regulations implementing the breach notification requirements for covered entities and their business associates by mid-August. The interim final regulations will be effective 30 days after they are issued and will apply to breaches of unsecured PHI thereafter. As such, in the meantime, covered entities and their business associates should prepare themselves to be in compliance with the specified encryption and destruction standards to ensure that PHI is appropriately secured for purposes of the breach notification requirements. Although HHS' guidance is voluntary, compliance with such standards will permit covered entities and business associates to disregard the burdensome notification requirements that will be set forth under the interim final regulations.

If you would like to receive future *Health Care Advisories* electronically, please forward your contact information including e-mail address to [healthcare.advisory@alston.com](mailto:healthcare.advisory@alston.com). Be sure to put “**subscribe**” in the subject line.

For further guidance please contact one of the attorneys or advisors listed below:

## Alston & Bird Health Information Technology (HIT) Task Force

Jacqueline C. Baratian  
202.756.3484  
[jacqueline.baratian@alston.com](mailto:jacqueline.baratian@alston.com)

Robert C. Lower  
404.881.7455  
[bob.lower@alston.com](mailto:bob.lower@alston.com)

Jennifer L. Butler  
202.756.3326  
[jennifer.butler@alston.com](mailto:jennifer.butler@alston.com)

Colin T. Roskey  
202.756.3436  
[colin.roskey@alston.com](mailto:colin.roskey@alston.com)

Timothy J. Hogan  
202.756.3001  
[timothy.hogan@alston.com](mailto:timothy.hogan@alston.com)

Tiffani V. Williams  
202.756.3412  
[tiffani.williams@alston.com](mailto:tiffani.williams@alston.com)

Laura E. Holland  
202.239.3980  
[laura.holland@alston.com](mailto:laura.holland@alston.com)

Marilyn Yager  
Senior Public Policy Advisor  
202.756.3341  
[marilyn.yager@alston.com](mailto:marilyn.yager@alston.com)

Peter M. Kazon  
202.756.3334  
[peter.kazon@alston.com](mailto:peter.kazon@alston.com)

### ATLANTA

One Atlantic Center  
1201 West Peachtree Street  
Atlanta, GA 30309-3424  
404.881.7000

### CHARLOTTE

Bank of America Plaza  
Suite 4000  
101 South Tryon Street  
Charlotte, NC 28280-4000  
704.444.1000

### DALLAS

Chase Tower  
Suite 3601  
2200 Ross Avenue  
Dallas, TX 75201  
214.922.3400

### LOS ANGELES

333 South Hope Street  
16th Floor  
Los Angeles, CA 90071-3004  
213.576.1000

### NEW YORK

90 Park Avenue  
New York, NY 10016-1387  
212.210.9400

### RESEARCH TRIANGLE

Suite 600  
3201 Beechleaf Court  
Raleigh, NC 27604-1062  
919.862.2200

### SILICON VALLEY

Two Palo Alto Square  
Suite 400  
3000 El Camino Real  
Palo Alto, CA 94306-2112  
650.838.2000

### VENTURA COUNTY

Suite 215  
2801 Townsgate Road  
Westlake Village, CA 91361  
805.497.9474

### WASHINGTON, D.C.

The Atlantic Building  
950 F Street, NW  
Washington, DC 20004-1404  
202.756.3300

[www.alston.com](http://www.alston.com)

© Alston & Bird LLP 2009