

“Unsecured PHI” Breach Notification Guidance Issued

April 2009

On April 17, 2009 the U.S. Department of Health & Human Services (HHS) issued a “Breach Notification Guidance and Request for Public Comment.” The Guidance was issued jointly by the Office for Civil Rights (OCR), the Office of the National Coordinator for Health Information Technology (ONC), and the Centers for Medicare & Medicaid Services (CMS). The Guidance is to be published in the April 27, 2009 edition of the Federal Register. 74 Fed. Reg. 19006 (April 27, 2009).

HITECH Background—The Guidance and Breach Notification Obligations

The Health Information Technology for Economic & Clinical Health Act (HITECH) amends the HIPAA Privacy and Security Rules and requires, among other things, notification to the individual whose protected health information (PHI) has been breached and, in some instances, it also requires notification to both the media and the federal government. The breaches subject to notification are breaches of “unsecured PHI” by unauthorized persons. There are some exceptions for when a breach of “unsecured PHI” does not trigger the notification rules, but as a practical matter the question of when covered entities and business associates must follow the notification rules turns on whether the PHI that was “breached” was unsecured PHI. Congress required HHS to publish guidance that defines “unsecured PHI.”

The Guidance is very broad and essentially defines “unsecured PHI” as any PHI that is not encrypted or destroyed. The Guidance also clarifies that it covers both paper and electronic PHI. This will render as “unsecured PHI” an enormous amount of individually identifiable health information maintained by covered entities and business associates.

The Guidance essentially defines ‘unsecured PHI’ as any PHI that is not encrypted or destroyed.

Significantly, if there is a breach of PHI that has been encrypted or destroyed, then the covered entity or business associate will have no notification requirements. Conversely, if there is a breach of PHI and the PHI has not been encrypted or destroyed, then most breaches will be subject to the notification rules (some exceptions related to inadvertent internal breaches exist). Consequently, as a practical matter, it will be important for covered entities and business associates to determine whether they can implement the recommended methodologies and technologies to ensure that they do not have “unsecured PHI.”

The breach notification rules will go into effect 30 days after HHS publishes interim final regulations on breach notification.

HHS is required to publish the regulations by mid-August 2009. This means that the breach notification obligations will go into effect likely in mid-September 2009.

The Guidance

The structure of the Guidance is important to review in order to understand how broad a net HHS has cast. The Guidance does not provide a definition of “secured PHI,” but sets out a type of “safe harbor” as to when PHI will not be considered “unsecured PHI.” This is a subtle point, but it suggests how broadly HHS will consider the breach notification rules to apply.

The Guidance does not require covered entities and business associates to encrypt or destroy PHI; though the Guidance warns organizations that by not encrypting or destroying, the organizations must pay careful attention to the breach notification obligations.

The HITECH Act gave instructions to HHS to set out a guidance around what methodologies HHS would consider

PHI sufficiently secure so that the PHI was rendered “unusable, unreadable, or indecipherable” to unauthorized individuals. HHS chose to approve extraordinarily narrow methodologies.

In thinking through security measures and the feasibility of encryption and destruction, the Guidance encourages covered entities and business associates to analyze the security of PHI from the perspective of four “states” - data at rest, data in motion, data in use, and data disposed. Breach vulnerabilities should be assessed from the perspective of all of those “states.”

HHS acknowledges in its Guidance that it may be impossible to encrypt certain “states” of PHI. For example, when PHI is “in use,” encryption may never be possible and organizations must be particularly vigilant for possible breaches.

For the technical methodologies that can be employed to ensure that PHI is not “unsecured,” HHS defers to documents published by the National Institutes of Standards & Technology (NIST). The NIST publications for encryption that are referenced are: (i) NIST 800-111 (Guide to Storage Encryption Technologies for End User Devices) which covers “data at rest;” and (ii) NIST 800-52 (Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations), 800-77 (Guide to IPsec VPNs) and 800-113 (Guide to SSL VPNs) (which cover “data in motion”) and incorporate the requirements of Federal Information Processing Standards (FIPS) 140-2. These documents are available at www.csrc.nist.gov.

The second method for ensuring that PHI is not “unsecured,” is “destruction” of PHI in paper and electronic form. If PHI is destroyed prior to disposal, and there is unauthorized access, acquisition or disclosure of the disposed hard copy or electronic media, then the breach notification rules are not triggered. For standards of electronic media destruction, HHS also defers to the NIST. Destruction methods for electronic media should follow NIST Special Publication 800-88 (Guidelines for Media Sanitation).

Significantly, the Notice specifies that the technologies and methodologies set forth in the Guidance are “intended to be exhaustive and not merely illustrative” (emphasis added).

Next Steps/Action Plan

The following are three actions covered entities and business associates can take to prepare for the breach notification rules that will be issued later this year:

1. Examine the organization’s data at rest and data in motion encryption processes, if any. Download the NIST documents referenced in the Guidance and consider the specified encryption methods with your information technology managers. Explore the costs (both financial and operational) of adopting the specified encryption methodologies and the attendant benefit, versus having to comply with the breach notification obligations for “unsecured PHI.”
2. Examine your destruction of PHI methods. Download the NIST electronic media destruction document and begin to analyze your policies and procedures against this document. Remember the “recommended” standard for destroying electronic PHI and the attendant NIST publication is definitive and not merely illustrative.
3. To the extent your organization is unable to implement the recommended methodologies and technologies for ensuring that its PHI is not “unsecured,” prepare now for the breach notification obligations. The HITECH Act’s breach notification sections provide the basic outline and structure of what HHS will cover in the regulations later this summer. Understand when notification will be required to the individual, to media, and to HHS. There are also requirements for posting notice of breaches on an organization’s website. It’s important to start thinking about this now because covered entities and business associates will only have 30 days from the publication of the regulations to comply.

If you have any questions about clinical research compliance, please contact:

Brian D. Annulis at 773.907.8343 or
BAnnulis@MeadeRoach.com

Ryan D. Meade at 312.498.7004 or
RMeade@MeadeRoach.com

Michael C. Roach at 312.255.1773 or
MRoach@MeadeRoach.com

Steven W. Ortquist at 312.285.4850 or
SOrtquist@MeadeRoach.com