HHS Guidance on Encryption

The HITECH Act of 2009 required Health and Human Services to publish and update annually specific methodologies that could be used to render health information unusable and unreadable. If the data is protected in the approved manner it will provide a safe haven from the reporting requirements defined for a breach in the event the data is lost, stolen, misplaced or an attempt made to hack the data.

A covered entity can be in compliance with the Security Rule and not use the approved encryption methods but if a breach occurs, notification will be required unless the approved encryption method is used.

II. Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals

Section 13402 of the HITECH Act requires breach notification following the discovery of a breach of unsecured protected health information. Section 13402(h) of the Act defines ''unsecured protected health information'' as ''protected health information that is not secured through the use of a technology or methodology specified by the Secretary in guidance'' and requires the Secretary to specify in the guidance the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals. As required by the Act, this guidance was issued on April 17, 2009, and later published in the **Federal Register** on April 27, 2009 (74 FR 19006).

The guidance specified encryption and destruction as the technologies and methodologies for rendering protected health information, as well as PHR identifiable health information under section 13407 of the Act and the FTC's implementing regulation, unusable, unreadable, or indecipherable to unauthorized individuals such that breach notification is not required. The RFI asked for general comment on this guidance as well as for specific comment on the technologies and methodologies to render protected health information unusable, unreadable, or indecipherable to unauthorized individuals.

Many commenters expressed concern and confusion regarding the purpose of the guidance and its impact on a covered entity's responsibilities under the HIPAA Security Rule (45 CFR part 164, subparts A and C). We emphasize that this guidance does nothing to modify a covered entity's responsibilities with respect to the Security Rule nor does it impose any new requirements upon covered entities to encrypt all protected health information. The Security Rule requires covered entities to safeguard electronic protected health information and permits covered entities to use any security measures that allow them to reasonably and appropriately implement all safeguard requirements.

Under 45 CFR 164.312(a)(2)(iv) and (e)(2)(ii), a covered entity must consider implementing encryption as a method for safeguarding electronic protected health information; however, because these are addressable implementation specifications, a covered entity may be in compliance with the Security Rule even if it reasonably decides not to encrypt electronic protected health information and instead uses a comparable method to safeguard the information

Therefore, if a covered entity chooses to encrypt protected health information to comply with the Security Rule, does so pursuant to this guidance, and subsequently discovers a breach of that encrypted information, the covered entity will not be required to provide breach notification

because the information is not considered ''unsecured protected health information'' as it has been rendered unusable, unreadable, or indecipherable to unauthorized individuals. On the other hand, if a covered entity has decided to use a method other than encryption or an encryption algorithm that is not specified in this guidance to safeguard protected health information, then although that covered entity may be in compliance with the Security Rule, following a breach of this information, the covered entity would have to provide breach notification to affected individuals. For example, a covered entity that has a large database of protected health information may choose, based on their risk assessment under the Security Rule, to rely on firewalls and other access controls to make the information inaccessible, as opposed to encrypting the information.

While the Security Rule permits the use of firewalls and access controls as reasonable and appropriate safeguards, a covered entity that seeks to ensure breach notification is not required in the event of a breach of the information in the database would need to encrypt the information pursuant to the guidance.

We also received several comments asking for clarification and additional detail regarding the forms of information and the specific devices and protocols described in the guidance. As a result, we provide clarification regarding the forms of information addressed in the National Institute of Standards and Technology (NIST) publications referenced in the guidance.

We clarify that ''data in motion'' includes data that is moving through a network, including wireless transmission, whether by e-mail or structured electronic interchange, while ''data at rest'' includes data that resides in databases, file systems, flash drives, memory, and any other structured storage method. ''Data in use'' includes data in the process of being created, retrieved, updated, or deleted, and ''data disposed'' includes discarded paper records or recycled electronic media.

Additionally, many commenters suggested that access controls be included in the guidance as a method for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals. We recognize that access controls, as well as other security methods such as firewalls, are important tools for safeguarding protected health information. While we believe access controls may render information inaccessible to unauthorized individuals, we do not believe that access controls meet the statutory standard of rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals. If access controls are compromised, the underlying information may still be usable, readable, or decipherable to an unauthorized individual, and thus, constitute unsecured protected health information for which breach notification is required. Therefore, we have not included access controls in the guidance; however, we do emphasize the benefit of strong access controls, which may function to prevent breaches of unsecured protected health information from occurring in the first place.

Other commenters suggested that the guidance include redaction of paper records as an alternative to destruction. Because redaction is not a standardized methodology with proven capabilities to destroy or render the underlying information unusable, unreadable or indecipherable, we do not believe that redaction is an accepted alternative method to secure paper-based protected health information. Therefore, we have clarified in this guidance that only destruction of paper protected health information, and not redaction, will satisfy the requirements to relieve a covered entity or business associate from breach notification. We note, however, that covered entities and business associates may continue to create limited data sets or de-identify protected health information through redaction if the removal of identifiers results in the

information satisfying the criteria of 45 CFR 164.514(e)(2) or 164.514(b), respectively. Further, a loss or theft of information that has been redacted appropriately may not require notification under these rules either because the information is not protected health information (as in the case of deidentified information) or because the unredacted information does not compromise the security or privacy of the information and thus, does not constitute a breach as described in Section IV below.

In response to comments received, we also make two additional clarifications in the guidance. First, for purposes of the guidance below and ensuring encryption keys are not breached, we clarify that covered entities and business associates should keep encryption keys on a separate device from the data that they encrypt or decrypt. Second, we also include in the guidance below a note regarding roadmap guidance activities on the part of the NIST pertaining to data storage on enterprise-level storage devices, such as RAID (redundant array of inexpensive disks), or SAN (storage-attached network) systems.

For ease of reference, we have published this updated guidance in this document below; however, it will also be available on the HHS Web site at *http://www.hhs.gov/ocr/privacy/.* Any further comments regarding this guidance received in response to the interim final rule will be addressed in **the first annual update to the guidance, to be issued in April 2010**.

B. Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals
Protected health information (PHI) is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:

(a) 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'' 2 and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged 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*.3 4
(ii) Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800–52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations;* 800–77, http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf

Guide to IPsec VPNs; or *800–113, http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf*

Guide to SSL VPNs, http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf

or others which are Federal Information Processing Standards (FIPS) 140–2 validated.5(b) The media on which the PHI is stored or recorded have 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. Redaction is specifically excluded as a means of data destruction.
(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.