



# Federal Register

---

Monday,  
August 24, 2009

---

Part II

## Department of Health and Human Services

---

45 CFR Parts 160 and 164  
Breach Notification for Unsecured  
Protected Health Information; Interim  
Final Rule

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 de-identified 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"<sup>2</sup> 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*.<sup>3</sup>

(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, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs*, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.<sup>5</sup>

<sup>2</sup> 45 CFR 164.304, definition of "encryption."

<sup>3</sup> NIST Roadmap plans include the development of security guidelines for enterprise-level storage devices, and such guidelines will be considered in updates to this guidance, when available.

<sup>4</sup> Available at <http://www.csrc.nist.gov/>.

<sup>5</sup> Available at <http://www.csrc.nist.gov/>.

(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*,<sup>6</sup> such that the PHI cannot be retrieved.

### III. Overview of Interim Final Rule

We are adding a new subpart D to part 164 of title 45 of the Code of Federal Regulations (CFR) to implement the breach notification provisions in section 13402 of the Act. These provisions apply to HIPAA covered entities and their business associates and set forth the requirements for notification to affected individuals, the media, and the Secretary of HHS following a breach of unsecured protected health information. In drafting this interim final regulation, we considered the public comments received in response to the RFI described above.

In addition, we consulted closely with the FTC in the development of these regulations. Commenters in response to both the RFI as well as the FTC's notice of proposed rulemaking urged HHS and the FTC to work together to ensure that the regulated entities know with which rule they must comply and that those entities that are subject to both rules because they may operate in different roles are not subject to two completely different and inconsistent regulatory schemes. In addition, commenters were concerned that individuals could receive multiple notices of the same breach if the HHS and the FTC regulations overlapped. Thus, HHS coordinated with the FTC to ensure these issues were addressed in the respective rulemakings. First, the rules make clear that entities operating as HIPAA covered entities and business associates are subject to HHS', and not the FTC's, breach notification rule. Second, in those limited cases where an entity may be subject to both HHS' and the FTC's rules, such as a vendor that offers PHRs to customers of a HIPAA covered entity as a business associate and also offers PHRs directly to the public, we worked with the FTC to ensure both sets of regulations were harmonized by including the same or similar requirements, within the constraints of the statutory language. See *Section IV.F.* below for a more

detailed discussion and an example of our harmonization efforts.

### IV. Section-by-Section Description of Interim Final Rule

The following discussion describes the provisions of the interim final rule section by section. Those interested in commenting on the interim final rule can assist the Department by preceding discussion of any particular provision or topic with a citation to the section of the interim final rule being discussed.

#### A. Applicability—Section 164.400

Section 164.400 of the interim final rule provides that this breach notification rule is applicable to breaches occurring on or after 30 days from the date of publication of this interim final rule. See *Section IV.K. Effective/Compliance Date* of this rule for further discussion.

#### B. Definitions—Section 164.402

Section 164.402 of the interim final rule adopts definitions for the terms "breach" and "unsecured protected health information."

##### 1. Breach

Section 13402 of the Act and this interim final rule require covered entities and business associates to provide notification following a breach of unsecured protected health information. Section 13400(1)(A) of the Act defines "breach" as the "unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of the protected health information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information." Section 13400(1)(B) of the Act provides several exceptions to the definition of "breach." Based on section 13400(1)(A), we have defined "breach" at § 164.402 of the interim final rule as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information." We have added paragraph (1) to the definition to clarify when the security or privacy of information is considered to be compromised. Paragraph (2) of the definition then includes the statutory exceptions, including the exception within section 13400(1)(A) that refers to whether the recipient would reasonably have been able to retain the information.

### Protected Health Information

We note that the definition of "breach" is limited to protected health information. With respect to a covered entity or business associate of a covered entity, protected health information is individually identifiable health information that is transmitted or maintained in any form or medium, including electronic information. 45 CFR 160.103. If information is de-identified in accordance with 45 CFR 164.514(b), it is not protected health information, and thus, any inadvertent or unauthorized use or disclosure of such information will not be considered a breach for purposes of this subpart. Additionally, § 160.103 excludes certain types of individually identifiable health information from the definition of "protected health information," such as employment records held by a covered entity in its role as employer. If individually identifiable health information that is not protected health information is used or disclosed in an unauthorized manner, it would not qualify as a breach for purposes of this subpart—although the covered entity should consider whether it has notification requirements under other laws. Further, we note that although the definition of "breach" applies to protected health information generally, covered entities and business associates are required to provide the breach notifications required by the Act and this interim final rule (discussed below) only upon a breach of unsecured protected health information. See also Section II of this document for a list of the technologies and methodologies that render protected health information secure such that notification is not required in the event of a breach.

#### Unauthorized Acquisition, Access, Use, or Disclosure

The statute defines a "breach" as the "unauthorized" acquisition, access, use, or disclosure of protected health information. Several commenters asked that we define "unauthorized" or that we clarify its meaning. We clarify that "unauthorized" is an impermissible use or disclosure of protected health information under the HIPAA Privacy Rule (subpart E of 45 CFR part 164). Accordingly, the definition of "breach" at § 164.402 of the interim final rule interprets the "unauthorized" acquisition, access, use, or disclosure of protected health information as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part." We emphasize that not all violations of the Privacy Rule will be

<sup>6</sup> Available at <http://www.csrc.nist.gov/>.

ends here