Definitions for Breach Notification Requirements

Breach means 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.

Breach excludes:

1. Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

2. Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

3. A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

"Discovery" of a Breach

Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, §§164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the

person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

Incident

An Incident involves a possible unauthorized or impermissible disclosure or use of Protected Health Information or Personally Identifiable Information but may not meet the definition of a Breach.

Protected Health Information (PHI)

Under HIPAA means any information that identifies an individual and relates to at least one of the following:

1. The individual's past, present or future physical or mental health.
2. The provision of health care to the individual.
3. The past, present or future payment for health care.

The health-related information types above are deemed to identify an individual, and hence become PHI, if they include any of the following 18 information attributes that could enable someone to determine the individual's identity:

1. Name
2. Address (all geographic subdivisions smaller than state, including street address, city, county, zip code)
3. All elements (except years) of dates related to an individual (including birth date, admission date, discharge date, date of death and exact age if over 89)
4. Telephone numbers
5. Fax number
6. Email address
7. Social Security number
8. Medical record number
9. Health plan beneficiary number
10. Account number
11. Certificate/license number

12. Any vehicle or other device serial number
13. Device identifiers or serial numbers
14. Web URL
15. Internet Protocol (IP) address numbers
16. Finger or voice prints
17. Photographic images
18. Any other characteristic that could uniquely identify the individual

Risk Assessment

An acquisition, access, use, or disclosure of protected health information in a manner not permitted under the Privacy Rule is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

Unsecured protected health information

Means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5 of Pub. L. 111-5.*

***Federal Register /Vol. 74, No. 79 /Monday, April 27, 2009 /Rules and Regulations 19009**

Data comprising PHI can be vulnerable to a breach in any of the commonly recognized data states: ''data in motion'' (i.e., data that is moving through a network, including wireless transmission 7); ''data at rest'' (i.e., data that resides in databases, file systems, and other structured storage methods 8); ''data in use'' (i.e., data in the process of being created, retrieved, updated, or deleted 9); or ''data disposed'' (e.g., discarded paper

records or recycled electronic media). Protected health information in each of these data states (with the possible exception of ''data in use'' 10) may be secured using one or more methods. In consultation with information security experts at the National Institute of Standards and Technology (NIST), we have identified two methods for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals: encryption and destruction. Both of these methods are discussed below.

Encryption is one method of rendering electronic protected health information unusable, unreadable, or indecipherable to unauthorized persons. The successful use of encryption depends upon two main features: The strength of the encryption algorithm and the security of the decryption key or process. The specification of encryption methods in this guidance includes the condition that the processes or keys that might enable decryption have not been breached. This guidance also addresses the destruction of protected health information both in paper and electronic form as a method for rendering such information unusable, unreadable, or indecipherable to unauthorized individuals.

If protected health information is destroyed prior to disposal in accordance with this guidance, no breach notification is required following access to the disposed hard copy or electronic media by unauthorized persons.

Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals

Protected health information is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:

1. *Electronic protected health information 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" (45 CFR 164.304 definition of encryption) 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 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.*

(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.*

2. *The media on which the protected health information 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 protected health information 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 protected health information cannot be retrieved.*