

HHS Issues Rule Requiring Individuals Be Notified of Breaches of Their Health Information

New regulations requiring health care professionals, health plans, and other entities covered by the Health Insurance Portability and Accountability Act (HIPAA) to notify individuals when their health information is breached were issued by the U.S. Department of Health and Human Services (HHS). The regulations are effective September 23, 2009.

The regulations, developed by the HHS Office for Civil Rights (OCR), require health care professionals and other HIPAA covered entities to promptly notify affected individuals of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.

The regulations were developed after considering public comment received in response to an April 2009 request for information and after close consultation with the Federal Trade Commission (FTC), which has issued companion breach notification regulations that apply to vendors of personal health records and certain others not covered by HIPAA.

To determine when information is “unsecured” and notification is required by the HHS and FTC rules, HHS is also issuing in the same document as the regulations an update to its guidance specifying encryption and destruction as the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Entities subject to the HHS and FTC regulations that secure health information as specified by the guidance through encryption or destruction are relieved from having to notify in the event of a breach of such information.

For more information, visit the HHS Office for Civil Rights web site at <http://www.hhs.gov/ocr/hipaa/>

The Health Information Technology for Economic and Clinical Health (HITECH) Act, was enacted on February 17, 2009. Subdivision D of Division A of the HITECH Act, among other provisions, requires the Department of Health and Human Services (DHHS) to issue interim final regulations for breach notification by covered entities subject to the “Administrative Simplification” provisions of HIPAA and their business associates. The breach notification provisions are found in section 13402 of the Act and apply to HIPAA covered entities and their business associates that access, maintain, retain, modify, record, store, destroy or otherwise hold, use, or disclose unsecured health information. The Act incorporates the definitions of “covered entity”, “business associates” and “protected health information” used under the HIPAA regulations.

I. Definitions

“Covered Entity” – A health plan, health care clearinghouse, or health care provider that transmits any health information electronically in connection with a covered transaction (see “Are You a Covered Entity Under HIPAA?”

http://www.mssny.org/mssnyip.cfm?c=f&nm=Covered_Entities)

Business Associate - A person or entity that performs functions or activities on behalf of, or certain services for, a covered entity that involve the use for disclosure of individually identifiable health information. Examples: Claims Processing or billing companies, transcription companies, persons who perform legal, actuarial, accounting, management, or administrative services for covered entities and who require access to protected health information. A medical society may be a business associate if a physician discloses protected health information to the medical society.

(A business associate does not include a workforce member of a covered entity such as an employee, volunteer, trainees or other person whose conduct in the performance of work for a covered entity, is under the direct control of the covered entity, whether or not they are paid by the covered entity).

“Protected Health Information” – Individually identifiable health information held or transmitted in any form or medium by HIPAA covered entities and business associates, subject to certain exceptions.

Definition of “Breach”

Sections 164.402 of the HITECH regulations define the work “Breach” as follows:

“Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted . . . which compromises the security or privacy of the protected health information.”

- (1) (i) For purpose of the definition compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational or other harm to the individual.
- (ii) A use or disclosure of protected health information that does not include the identifiers listed at 164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.
- (2) Breach Excludes:
 - (i) 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.
 - (ii) Any inadvertent disclosures 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.
 - (iii) 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.

The term “Unsecured protected health information” is defined by section 164.402 to mean “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 of DHHS (listed on DHHS website).

The breach notification requirements arise following the discovery of a breach of unsecured protected health information. Section 13402(h) of HITECH requires the Secretary of HHS to issue guidance that specifies the technologies and methodologies that render protected health information “unusable, unreadable, or indecipherable” to unauthorized individuals. The Secretary issued guidance April 17, 2009 which is published in the Federal Register on April 27, 2009. The guidance specified (1) encryption and (2) destruction as the two technologies and methodologies for rendering protected health information “unusable unreadable and indecipherable”, to unauthorized individuals.

A. Encryption

Interplay between HIPAA Security Rule (45 CFR part 164 subparts A and C) and Breach Notification requirements. The HIPAA 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 using encryption as a method for safeguarding electronic protected health information; however, because encryption is an “addressable” implementation specification, encryption is not mandatory.

For purposes of the Breach Notification requirements, if a covered entity chooses to encrypt protected health information, 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”.

For purposes of the Breach Notification requirements, it is strongly recommended that a medical practice that maintains or stores patient information in electronic form should consider encryption. The Breach Notification requirements may be very onerous, and encryption will enable the medical practice to avoid the Breach Notification requirements.

If a covered entity has decided to use a method other than encryption or an encryption algorithm that is not specified in the DHHS guidance to safeguard protected health information, then, although the covered entity may be in compliance with the Security Rule, if there is a breach of this information, the covered entity would have to provide breach notification to the affected individuals.

DHHS has offered the following guidance regarding encryption processes:

- (i) Valid encryption processes for data at rest are consistent with the National Institute of Standards Technology (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 with NIST Special Publications 800-52, Guidelines for 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. <http://www.csrc.nist.gov/>

Guidance: To avoid a breach of the confidential process or key, the decryption tools should be stored on a device or at a location separate from the data they are used to encrypt.

B. Destruction

The second method specified in the April 27, 2009 Federal Register is the destruction of the media on which the protected health information is stored or recorded.

- (i) Paper, film or other hard copy media have been shredded or destroyed;
- (ii) Electronic Media have been cleared, purged or destroyed consistent with NIST Special Publication 800-88 Guidelines for Media Sanitization, such that PHI cannot be retrieved; available at <http://www.csrc.nist.gov/>

2) Analysis

Based upon the definitions of “Breach” and “Unsecured Protected Health Information”, there is a three Part Analysis:

Step 1 – The covered entity or business associate must determine whether there has been an impermissible use or disclosure of protected health information under the Privacy Rule.

Step 2 – The covered entity or business associate must determine, and document, whether the impermissible use or disclosure compromises the security or privacy of the protected health information. This occurs when there is a significant risk of financial, reputational, or other harm to the individual.

Step 3 – The covered entity or business associate may need to determine whether the incident falls under one of the exceptions in paragraph (2) of the “Breach” definition.

Step 1 – A “breach” is an unauthorized acquisition, access, use, or disclosure of protected health information. “Unauthorized” means an impermissible use or disclosure of protected health information.

One of the first steps in determining whether notification is necessary is to determine whether a use or disclosure violates the HIPAA Privacy Rule.

- Uses or disclosures that impermissible involve more than the “minimum necessary” information in 164.502(b) and 164.514(d) may qualify as breaches
- In contrast, a use or disclosure of protected health information that is “incident to” or otherwise permissible use and disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not violate the Privacy Rule pursuant to 45 CFR 164.502(a)(1)(iii), and, therefore, would not qualify as a potential breach.

Step 2 – Once it is determined that the use or disclosure violates the Privacy Rule, the covered entity or business associate must determine whether the violation compromises the security or privacy of the protected health information.

The term “compromise the security or privacy of the protected health information” means that the covered entity or business associate must perform some type of risk assessment to determine if there is a risk of harm to the individual.

The term “poses a significant risk of financial, reputational or other harm to the individual” means that covered entities and business associates will need to perform a risk assessment to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure.

Covered entities and business associates should consider who impermissibly used or to whom the information was impermissibly disclosed when evaluating the risk of harm to individuals.

If the nature of the protected health information does not pose a significant risk of financial, reputational, or other harm, then the violation is not a breach.

For example, if a covered entity improperly discloses protected information that merely included the name of an individual and the fact that he/she received services, then this would violate the Privacy Rule, but it may not constitute a significant risk of financial or reputational harm to the individual.

In contrast, if the information indicates the type of services that the individual received (such as oncology services), or that the individual received services from a specialized facility (e.g. substance abuse treatment), or if the risk of identity theft (such as social security number, account number, or mother's maiden name) then there is a higher likelihood that the impermissible use or disclosure compromised the security or privacy of the information.

According to the DHHS, the risk assessment should be fact specific, and the covered entity or business associate must keep in mind that many forms of health information, and not just information about sexually transmitted diseases or mental health, should be considered sensitive for purposes of risk of reputational harm – especially in light of fears about employment discrimination.

“Limited Data Sets”

A Limited Data Set is created by removing 16 direct identifiers listed in 45 CFR 164.514(e)(2) from the protected health information.

- (1) names;
- (2) postal address information, other than town or city, State and zip code;
- (3) telephone numbers;
- (4) tax numbers;
- (5) email addresses;
- (6) social security numbers;
- (7) medical record numbers;
- (8) health plan beneficiary numbers;
- (9) account numbers;
- (10) certificate/license plate numbers;
- (11) vehicle identifiers and serial numbers;
- (12) device identifiers and serial numbers;
- (13) web URLs;
- (14) internet Protocol (IP) address numbers;
- (15) biometric identifiers, including finger and voice prints; and
- (16) full face photographs images or any comparable images.

DHHS has stated that because of the risk of re-identification, the creation of a limited data set is not comparable to encrypting information, and therefore, is NOT included as a method to render protected health information “unusable, unreadable or indecipherable”.

Therefore, creation of a Limited Data Set is not treated the same as Encryption.

Does this mean that a breach of a Limited Data Set must lead to a Breach Notification? Not necessarily. The covered entity must perform a risk assessment described in Step 2. In performing the risk assessment to determine the risk of harm caused by an impermissible use or disclosure of a limited data set, the covered entity or business associate should take into

consideration the risk of re-identification of the protected health information contained in the limited data set.

Through a risk assessment, a covered entity or business associate may determine that the risk of identifying a particular individual is so small that use or disclosure poses not significant harm to any individual. If, however, the covered entity or business associate determines that the individual can be identified based on the information disclosed, and there is otherwise a significant risk of harm to the individual, then breach notification is required, unless an exception applies.

Narrow Exception: DHHS deems that information that excludes the 16 identifiers listed in 45 CFR 164.514(e)(2) as well as dates of birth and zip codes would pose a low level risk.

Step 3 – What are the Breach Exceptions? The definition of the term “breach” at 164.402(2) provides three exceptions:

(2)(i). The exception at (2)(i) applies to unintentional acquisition, access, or use of protected health information. This provision excepts from the definition of “breach” the unintentional acquisition, access or use of protected health information by an employee or individual acting under the authority of a covered entity or business associate, if the acquisition, access or use was in good faith, within the course of employment or other professional relationship, and does not result in further use or disclosure.

For example, a billing employee receives and opens email containing protected health information about a patient which a nurse mistakenly sent to the billing employee. The billing employee notices that he is not the intended recipient, alerts the nurse of the misdirected email, and then deletes it.

(2)(ii). The second exception at (2)(ii) covers inadvertent disclosures from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or a business associate to another similarly situated individual at the same facility if the information is not further used or disclosed without authorization.

This exception encompasses circumstances in which a person who is authorized to use or disclose protected health information within a covered entity, business associate, or organized health care arrangement inadvertently discloses the information to another person who is authorized to use or disclose protected health information within the same covered entity, business associate or organized health care arrangement, as long as the recipient does not further use or disclose the information in violation.

The term “organized health care arrangement” is defined by HIPAA Rules at 164.103 to mean, among other things, a clinically integrated setting in which individuals typically receive health care from more than one provider.

For example, a physician who has authority to use or disclose protected health information at a hospital by virtue of participating in an organized health care arrangement with the hospital is similarly situated with a nurse or billing employee at the hospital.

(2)(iii). The third exception at (2)(iii) except from the definition of “breach” situations in which an unauthorized person to whom protected health information has been disclosed would not have reasonably been able to retain the information.

For example, a nurse mistakenly hands a patient the discharge papers belonging to another patient but she quickly realizes her mistake and recovers the protected health information from the patient. If the nurse can reasonably conclude that the patient could not have read or otherwise retained the information, then this would not constitute a breach.

Definition: “Unsecured Protected Health Information”. Protected Health Information that is not rendered unusable, unreadable or indecipherable to authorized individuals through the use of a technology or methodology specified by the Secretary in guidance.

The term “unsecured protected health information can include information in any form or medium, including electronic, paper or oral form.

II. Notification 164.404

1. General Rule – A covered entity must follow the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used or disclosed as a result of the breach.

Section 164.404(a)(2). A breach is treated as discovered by a covered entity on the first day the breach is known to the covered entity, or by exercising reasonable diligence, would have been known to the covered entity.

A covered entity is 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.

Guidance: Thus, covered entities should ensure their workforce members and other agents are adequately trained and aware of the importance of timely reporting of privacy and security incidents and of the consequences of failing to do so.

2. Timeliness – A covered entity is required to send the required notification without unreasonable delay and in no case later than 60 calendar days after the breach was discovered.

3. Content – 164.404(c) The Notification should include, to the extent possible, the following elements:

- (A) a brief description of what happened, including the date of the breach and the date of discovery of the breach if known;
- (B) a description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);
- (C) any steps individuals should take to protect themselves from potential harm resulting from the breach;
- (D) a brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; and

- (E) contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an email address, website, or postal address.

4. Methods of Notification – 164.404(d)

- (1) Written notice by first class mail at the last known address of the individual;

Email – Written notice may be in the form of electronic mail, provided the individual has agreed to receive notices by electronic means and such agreement to receive notifications by email has not been withdrawn.

Recommendation: Medical Practice should make sure it has current updated patient contact information including home address and email address if possible. Also, if possible, routinely obtain patient agreement to receive notifications by email.

Minor Patient – If the individual is a minor or otherwise lacks capacity, notice to the parent or other personal representative will satisfy requirements. See Privacy Rule at 164.502(g).

Individuals deceased – If the individual is deceased, written notice by first class mail either to the next of kin or personal representative.

- (2) Substitute Notice – 164.404(d)(2)

If a covered entity does not have sufficient information for some or all of the affected individuals, or if some notices are returned as undeliverable, the covered entity must provide substitute notice.

a) Fewer than 10 individuals. If there are fewer than 10 individuals for whom the covered entity has insufficient or out-of-date contact information to provide written notice, the covered entity may provide substitute notice to such individuals through an alternative form of written notice, by telephone, or other means.

For example, If the covered entity learns that the home address it has for a patient is out-of-date but it has the patient's email address, it may provide substitute notice by email even if the patient has not agreed to electronic notice.

Insufficient or Out-of-Date Contact Information for 10 or more individuals:

- A) the covered entity must provide substitute notice through either a conspicuous posting for a period of 90 days on the home page of its website or conspicuous notice in major print or broadcast media in geographic areas where the individual affected by the breach likely reside; and
- B) the covered entity must have a toll-free phone number, active for 90 days, where an individual can learn whether the individual's unsecured

protected health information may be included in the breach and to include the number in the notice.

Recommendation: Requirements for Substitute Notice underscore importance of having up-to-date patient contact information

Urgent Situations

Notice by telephone or other means may be made in addition to written notice, in cases deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information.

(3) Notification to the Media - 164.406

Notice must be provided to prominent media outlets serving a state or jurisdiction following the discovery of a breach if the unsecured protected health information of more than 500 residents in the state or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach.

The media notice differs from the substitute media notice described in 164.404(d)(i)(2) in that it is directed “to” the media and is intended to supplement, but not substitute for, individual notice.

The term “jurisdiction” refers to a geographic area smaller than a state, such as a county, city or town.

For example, if laptops containing the unsecured protected health information of more than 500 residents of a particular city were stolen from a covered entity, notification should be provided to prominent media outlets serving that city.

If a breach involves 500 or more residents across a state and not within any one particular county or city of the state, the prominent media outlet chosen must serve the entire state.

If a breach involves 600 individuals, but fewer than 500 residents in any particular state or jurisdiction, then notification pursuant to 164.406 is not required.

(4) Notification to the Secretary of DHHS – 164.408

For breaches involving 500 or more individuals, the covered entity must notify the Secretary of DHHS immediately.

The term “immediately” means “without unreasonable delay”, but in no case later than 60 calendar days following discovery of the breach.

A covered entity must notify the Secretary of discovered breaches involving 500 or more individuals generally, without regard to whether the breach involved more than 500 residents of a particular state or jurisdiction.

For example, if a breach involves 600 individuals but fewer than 500 residents in any particular state or jurisdiction, then notification to a media outlet pursuant to 164.406 is not required, but notification to the Secretary is required.

(5) Breach involving less than 500 individuals

A covered entity must maintain a log or other documentation of breaches and to submit information annually to the Secretary for breaches occurring during the preceding calendar year.

DHHS will specify on its website the information to be submitted and how to submit such information.

Although covered entities need only provide notification to the Secretary of breaches involving less than 500 individuals annually, they must still provide notification of such breaches to different individuals pursuant to 164.404.

III. Notification By a Business Associate – 164.410

A business associate of a covered entity that accesses, maintains, retains, modifies, records, destroys or otherwise holds, uses or discloses unsecured protected health information must notify the covered entity when it discovers a breach of the information.

Timeliness – A business associate must provide the notification to the covered entity without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.

A breach is deemed to be discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate.

Content of Notification – The business associate, to the extent possible, must provide the covered entity with the identity of each individual whose unsecured protected health information that has been, or is reasonably believed to have been, breached.

The business associate is required to provide the covered entity with other available information that the covered entity is required to include in the notification to the individual under 164.404(c), either at the time it provides notice to the covered entity of the breach or promptly thereafter as information becomes available.

IV. Law Enforcement Delay – 164.412

If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting would impede a criminal investigation or cause damage to national security:

- a) If the statement is in writing and specifies the time for which the delay is required, the covered entity or business associate should delay such notification, notice or posting for the time period specified by the official; or

- b) If the statement is made orally, the covered entity or business associate should document the statement, including the identity of the official making the statement, and delay making the notification, notice or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

V. Administrative Requirements and Burden of Proof – 164.414

a) Covered Entities must comply with the administrative requirements of the HIPAA Privacy Rule. These provisions, for example, require covered entities and business associates to develop and document policies and procedures, train workforce members and have sanctions for failure to comply with these policies and procedures, permit individuals to file complaints regarding failure to comply with policies and procedures, and require covered entities to refrain from intimidating or retaliatory acts.

b) Burden of Proof – Following an impermissible use or disclosure, covered entities and business associates have the burden of proof to demonstrate compliance with these rules.

VI. Training – 164.530

A covered entity must train all members of the workforce on policies and procedures with respect to the Breach Notification Requirements.

September 23, 2009