

Summary of the HHS interim final rule to require notification of breaches of unsecured protected health information

Editors Note:

This summary consists principally of edited text taken directly from the discussion section of the HHS interim final regulations published August 24th in the Federal Register. The editors have removed some of the discussion (for example discussion of comments received) in an attempt to simplify the review and focus on content and HHS comments most helpful in assisting a Covered Entity or Business Associate in implementing the policies and procedures necessary to comply with these regulations. Statutory and Regulatory references have, for the most part, been removed and replaced by generic terms (i.e. “as defined by HIPAA”) for the sake of clarity. Full regulatory and statutory references and additional commentary is included in the full text of the HHS interim final rule. Exclusion of some text from this summary in no way implies that the information is not relevant or important. A link to the full text can be found on our website at www.wjflynnandassociates.com.

-The Editors

While every effort has been taken in compiling this information to ensure that its contents are totally accurate, neither the publisher nor the author can accept any liability whatsoever for any inaccuracies or changed circumstances of any information herein or for the consequences of any reliance placed upon it. This publication is distributed on the understanding that the publisher is not engaged in rendering legal, accounting or other professional advice or services. Readers should always and without exception seek professional advice before entering into any commitments.

Background

The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted on February 17, 2009. Subtitle D of Division A of the HITECH Act (the Act), entitled “Privacy,” among other provisions, requires the Department of Health and Human Services (HHS or the Department) to issue interim final regulations for breach notification by covered entities subject to the Administrative Simplification provisions of HIPAA and their business associates.

These breach notification provisions are found in § 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 protected health information. The Act incorporates the definitions of “covered entity,” “business associate,” and “protected health information” used in the HIPAA regulations.

The Act requires HIPAA covered entities to provide notification to affected individuals and to the Secretary of HHS following the discovery of a breach of unsecured protected health information. In addition, in some cases, the Act requires covered entities to provide notification to the media of breaches.

In the case of a breach of unsecured protected health information at or by a business associate of a covered entity, the Act requires the business associate to notify the covered entity of the breach.

Finally, the Act requires the Secretary to post on an HHS web site a list of covered entities that experience breaches of unsecured protected health information involving more than 500 individuals.

Section-by-Section Description of Interim Final Rule

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.

- The interim final rule was published in the Federal Register on Monday August 24th, making the effective date of these regulations September 23rd, 2009.

B. Definitions—Section 164.402

Section B contains regulatory definitions of the two principal definitions related to the requirements;

1. What is a Breach
2. What is Unsecured Protected Health Information

1 – Breach

The interim final rule defines breach as “the acquisition, access, use, or disclosure of protected health information in a manner not permitted under HIPAA which compromises the security or privacy of the protected health information.”

Protected Health Information

The definition of “breach” is limited to protected health information. If information is de-identified in accordance with HIPAA regulations, 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.

- Covered entities and business associates are required to provide the breach notifications only upon a breach of unsecured protected health information (see section 2 below).

Unauthorized Acquisition, Access, Use, or Disclosure

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 HIPAA.”

For an acquisition, access, use, or disclosure of protected health information to constitute a breach, it must constitute a violation of the Privacy Rule. Therefore, one of the first steps in determining whether notification is necessary is to determine whether a use or disclosure violates the Privacy Rule.

- Not all violations of the Privacy Rule will be breaches, and therefore, covered entities and business associates need not provide breach notification in all cases of impermissible uses and disclosures.
- Violations of administrative requirements, such as a lack of reasonable safeguards or a lack of training, do not themselves qualify as potential breaches under this subpart (although such violations certainly may lead to impermissible uses or disclosures that qualify as breaches).

Compromises the Security or Privacy of Protected Health Information

The Act and regulation limit the definition of “breach” to a use or disclosure that “compromises the security or privacy” of the protected health information. Accordingly, once it is established that a use or disclosure violates the Privacy Rule, the covered entity must determine whether the violation compromises the security or privacy of the protected health information.

- The definition that “compromises the security or privacy of the protected health information” means “poses a significant risk of financial, reputational, or other harm to the individual.”

To determine if an impermissible use or disclosure of protected health information constitutes a breach, 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. In performing the risk assessment, covered entities and business associates may need to consider a number or combination of factors.

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, for example, protected health information is impermissibly disclosed to another entity governed by the HIPAA Privacy and Security Rules or to a Federal agency that is obligated to comply with the Privacy Act of 1974 and the Federal Information Security Management Act of 2002, there may be less risk of harm to the individual, since the recipient entity is obligated to protect the privacy and security of the information it received in the same or similar manner as the entity that disclosed the information. In contrast, if protected health information is impermissibly disclosed to any entity or person that does not have similar obligations to maintain the privacy and security of the information, the risk of harm to the individual is much greater.

There may be circumstances where a covered entity takes immediate steps to mitigate an impermissible use or disclosure.

- For example, by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed. If such steps eliminate or reduce the risk of harm to the individual to a less than "significant risk," then the security and privacy of the information has not been compromised and, therefore, no breach has occurred.

There may be circumstances where impermissibly disclosed protected health information is returned prior to it being accessed for an improper purpose.

- For example, if a laptop is lost or stolen and then recovered, and a forensic analysis of the computer shows that its information was not opened, altered, transferred, or otherwise compromised, such a breach may not pose a significant risk of harm to the individuals whose information was on the laptop. Note, however, that if a computer is lost or stolen, we do not consider it reasonable to delay breach notification based on the hope that the computer will be recovered.

In performing a risk assessment, covered entities and business associates should also consider the type and amount of protected health information involved in the impermissible use or disclosure. 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 health information that merely included the name of an individual and the fact that he received services from a hospital, then this would constitute a violation of 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), that the individual received services from a specialized facility (such as a substance abuse treatment program), or if the protected health information includes information that increases the risk of identity theft (such as a 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 and privacy of the information.

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

Exceptions to Breach

A covered entity or business associate is not responsible for a breach by a third party to whom it permissibly disclosed protected health information unless the third party received the information in its role as an agent of the covered entity or business associate.

The Act also includes three exceptions to the definition of "breach" that encompass situations Congress clearly intended to not constitute breaches:

- (1) 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;

- Example - A billing employee receives and opens an e-mail 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 e-mail, and then deletes it. The billing employee unintentionally accessed protected health information to which he was not authorized to have access. However, the billing employee's use of the information was done in good faith and within the scope of authority, and therefore, would not constitute a breach and notification would not be required, provided the employee did not further use or disclose the information accessed in a manner not permitted by the Privacy Rule. In contrast, a receptionist at a covered entity who is not authorized to access protected health information decides to look through patient files in order to learn of a friend's treatment. In this case, the impermissible access to protected health information would not fall within this exception to breach because such access was neither unintentional, done in good faith, nor within the scope of authority.

(2) Inadvertent disclosure of protected health information from one person authorized to access protected health information at a covered entity or business associate to another similarly situated person authorized to access protected health information at the covered entity or business associate;

- 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 improperly discloses PHI to a nurse or billing employee at the hospital. In contrast, the physician is not similarly situated to an employee at the hospital who is not authorized to access protected health information, thus an improper disclosure to a security worker not authorized to access the PHI would be a breach subject to these regulations.

(3) Unauthorized disclosures in which an unauthorized person to whom protected health information is disclosed would not reasonably have been able to retain the information.

- For example, a covered entity, due to a lack of reasonable safeguards, sends a number of explanations of benefits (EOBs) to the wrong individuals. A few of the EOBs are returned by the post office, unopened, as undeliverable. In these circumstances, the covered entity can conclude that the improper addressees could not reasonably have retained the information. The EOBs that were not returned as undeliverable, however, and that the covered entity knows were sent to the wrong individuals, should be treated as potential breaches.
- As another 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.

Determining if a Breach Has Occurred

Covered entities and business associates will need to do the following to determine whether a breach occurred.

- First, 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.
- Second, 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.
- Lastly, the covered entity or business associate may need to determine whether the incident falls under one of the exceptions to the breach definition.

2. Unsecured Protected Health Information

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

Background

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.

- 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, unusable, unreadable, or indecipherable to unauthorized individuals such that breach notification is not required.
- Future guidance (on specified technology and methods) will be published on the HHS web site.

Methods to Render PHI Unusable

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” 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.

(b) The media on which the PHI 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 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, 6 such that the PHI cannot be retrieved.

C. Notification to Individuals—Section 164.404

General Rule

A covered entity shall, following 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 such breach.

Breaches Treated as Discovered

A breach shall be treated as discovered by a covered entity as of 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.

- ...it is important for such covered entities to implement reasonable systems for discovery of breaches.
- These provisions attribute knowledge of a breach by a workforce member or other agent, such as certain business associates, to the covered entity itself.
 - This is important, as knowledge of a breach, i.e., when a breach is treated as “discovered,” starts the clock in terms of the period of time a covered entity has to make the notifications required by the interim final rule.
 - 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.

Timeliness

A covered entity shall send the required notification without unreasonable delay and in no case later than 60 calendar days after the date the breach was discovered

- The covered entity may take a reasonable time to investigate the circumstances surrounding the breach, in order to collect and develop the information required to be included in the notice to the individual.
- It may be an “unreasonable delay” to wait until the 60th day to provide notification.
 - For example, if a covered entity has compiled the information necessary to provide notification to individuals on day 10 but waits until day 60 to send the notifications, it would constitute an unreasonable delay despite the fact that the covered entity has provided notification within 60 days.

Content

The Act requires the notification to include, to the extent possible, the following elements:

- (1) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- (2) 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);
- (3) any steps individuals should take to protect themselves from potential harm resulting from the breach;
- (4) a brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
- (5) contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an e-mail address, web site, or postal address.

With respect to indicating in the notification the types of protected health information involved in a breach, this provision requires covered entities to describe only the types of information involved. Covered entities should not include a listing of the actual protected health information that was breached (e.g., list in the notice the individual’s social security number or credit card number that was breached) and generally should avoid including any sensitive information in the notification itself.

Form of Notice

The Act requires a covered entity to provide breach notice to the individual in written form by first-class mail at the last known address of the individual.

- The interim final rule also provides that written notice may be in the form of electronic mail, provided the individual agrees to receive electronic notice and such agreement has not been withdrawn.

- Where the individual affected by a breach is a minor or otherwise lacks legal capacity due to a physical or mental condition, notice to the parent or other person who is the personal representative of the individual will satisfy the requirements
- The statute also requires that, if the individual is deceased, notice must be sent to the last known address of the next of kin or personal representative.

Substitute Notice

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

- Substitute notice should be provided as soon as reasonably possible after the covered entity is aware that it has insufficient or out-of-date contact information for affected individuals.
- Whatever form of substitute notice is provided, the notice must contain all the elements that are required to be included in the direct written notice to individuals.
- If there are fewer than 10 individuals for whom the covered entity has insufficient or out-of-date contact information to provide the written notice, The Act permits the covered entity to 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 one of its patients is out-of-date but it has the patient's e-mail address, it may provide substitute notice by e-mail even if the patient has not agreed to electronic notice.
 - Alternatively, posting a notice on the web site of the covered entity or at another location may be appropriate if the covered entity lacks any current contact information for the patients, so long as the posting is done in a manner that is reasonably calculated to reach the individuals.
- If a covered entity has insufficient or out-of-date contact information for 10 or more individuals,
 - The covered entity to provide substitute notice through either a conspicuous posting for a period of 90 days on the home page of its web site or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside.
 - Substitute notice through the website or media for 10 or more individuals requires the covered entity to have a toll-free phone number, active for 90 days, where an individual can learn whether the individual's unsecured PHI may be included in the breach and to include the number in the notice.
 - If the covered entity chooses to provide substitute notice on the home page of its web site, the notice must be conspicuous and posted for at least 90 days. A covered entity may provide all the information directly on its home page or may provide a hyperlink to the notice containing such information.
 - If a covered entity uses a hyperlink on the home page to convey the substitute notice, the hyperlink should be prominent so that it is noticeable given its size, color, and graphic treatment in relation to other parts of the page, and it should be worded to convey the nature and importance of the information to which it leads.

D. Notification to the Media—164.406

The Act requires that notice 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 of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach.

- The Act requires that notification to the media under this provision be provided within the same timeframe as notice is to be provided to the individual.
- Notification to the media under this provision must include the same information required to be included in the notification to the individual.

To illustrate how these provisions apply, HHS included provided the following examples:

- If laptops containing the unsecured protected health information of more than 500 residents of a particular city were stolen from a covered entity, notification under this section should be provided to prominent media outlets serving that city. In this case, the prominent media outlet may be a major television station or newspaper (or other media outlet) serving primarily the residents of that city or a prominent media outlet serving the entire state. Alternatively, for a breach involving 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 covered entity discovers a breach of 600 individuals, 200 of which reside in Virginia, 200 of which reside in Maryland, and 200 of which reside in the District of Columbia, such a breach did not affect more than 500 residents of any one State or jurisdiction, and as such, notification is not required to be provided to the media.

E. Notification to the Secretary—164.408

For breaches involving 500 or more individuals, the Act requires covered entities to notify the Secretary (HHS) immediately. For breaches involving less than 500 individuals, the Act provides that a covered entity may maintain a log of such breaches and annually submit such log to the Secretary documenting the breaches occurring during the year involved.

Breaches involving more than 500 individuals

- The term “immediately” requires notification be sent to the Secretary concurrently with the notification sent to the individual.
 - HHS will post instructions on its web site for submitting both this notification as well as the annual notification described below.
- The Secretary will post on the HHS web site a list of covered entities that submit reports of breaches of unsecured protected health information involving more than 500 individuals.
- Covered entities must notify the Secretary of discovered breaches involving more than 500 individuals generally, without regard to whether the breach involved more than 500 residents of a particular State or jurisdiction

Breaches involving less than 500 individuals

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

- The interim final rule requires the submission of this information to the Secretary no later than 60 days after the end of each calendar year.
 - Information about breaches involving less than 500 individuals is to be provided to the Secretary in the manner specified on the HHS web site. HHS will specify on its web site the information to be submitted and how to submit such information.
- For calendar year 2009, the covered entity is only required to submit information to the Secretary for breaches occurring after the effective date of this regulation.

F. Notification by a Business Associate—164.410

The Act requires a business associate of a covered entity to notify the covered entity when it discovers a breach of PHI.

- A business associate that maintains the protected health information of multiple covered entities need notify only the covered entity(s) to which the breached information relates. However, in cases in which a breach involves the unsecured protected health information of multiple covered entities and it is unclear to whom the breached information relates, it may be necessary to notify all potential affected covered entities.
- A business associate must provide notice of a breach of unsecured protected health information to a covered entity without unreasonable delay and in no case later than 60 days following the discovery of a breach.
 - If a business associate is acting as an agent (based on the principles of the federal common law of agency) of a covered entity, then, the business associate's discovery of the breach will be imputed to the covered entity. Accordingly, in such circumstances, the covered entity must provide notifications based on the time the business associate discovers the breach, not from the time the business associate notifies the covered entity.
 - In contrast, if the business associate is an independent contractor of the covered entity (i.e., not an agent), then the covered entity must provide notification based on the time the business associate notifies the covered entity of the breach.
- Covered entities may wish to address the timing of the notification in their business associate contracts.
- The Act requires business associates, to the extent possible, to provide covered entities with the identity of each individual whose unsecured protected health information has been, or is reasonably believed to have been, breached.

G. Law Enforcement Delay—164.412

The Act provides that if a law enforcement official determines that a notification, notice, or posting required under this section would impede a criminal investigation or cause damage to national security, such notification, notice, or posting shall be delayed in the same manner as provided under the HIPAA Privacy Rule.

- The Act provides for a temporary delay of notification in situations in which a law enforcement official provides a statement in writing that the delay is necessary because notification would impede a criminal investigation or cause damage to national security, and specifies the time for which a delay is required. In these instances, the covered entity is required to delay the notification, notice, or posting for the time period specified by the official.
- The Act also requires a covered entity or business associate to temporarily delay a notification, notice, or posting if a law enforcement official states orally that a notification would impede a criminal investigation or cause damage to national security.
 - In this case, the covered entity or business associate is required to document the statement and the identity of the official and delay notification for no longer than 30 days.

H. Administrative Requirements and Burden of Proof—164.414

The regulations require covered entities and business associates to develop and document policies and procedures, train workforce members on and have sanctions for failure to comply with these policies and procedures, permit individuals to file complaints regarding these policies and procedures or a failure to comply with them, and require covered entities to refrain from intimidating or retaliatory acts. Thus, a covered entity is required to consider and incorporate the requirements of this subpart with respect to its HIPAA administrative compliance and other obligations.

Burden of Proof

Following an impermissible use or disclosure under the Privacy Rule, covered entities and business associates have the burden of demonstrating that all notifications were made as required.

- As part of demonstrating that all required notifications were made, a covered entity or business associate also must be able to demonstrate that an impermissible use or disclosure did not constitute a breach, in cases where it is determined that notifications were not required.
- When a covered entity or business associate knows of an impermissible use or disclosure of protected health information, it should maintain documentation that all required notifications were made, or, alternatively, of its risk assessment or the application of any exceptions to the definition of “breach” to demonstrate that notification was not required.

For more information or for assistance with HIPAA compliance contact:

Bob Radecki
Principal
W.J. Flynn and Associates, LLC
bob.radecki@wjflynnandassociates.com
www.wjflynnandassociates.com