



BREACH NOTIFICATION FOR UNSECURED PROTECTED HEALTH INFORMATION

November 2009

Summary

On August 24, 2009, the Department of Health and Human Services (HHS) published an interim final rule (the “Rule”) that spells out what to do in the event of a breach of unsecured protected health information (PHI). The Privacy and Security Rules set the standard for how and what to protect, as well as their exceptions, but this interim final rule adds a requirement to notify patients when a breach occurs. The requirements vary based on the magnitude of the breach, but there are steps practices must take if they discover any kind of breach by either the practice or one of their business associates, including notifying HHS, the media, or both, as well as the affected individuals.

Although the rule took effect on September 23, 2009, HHS will not enforce the rule until February 22, 2010. This gives covered entities a grace period to set up policies and procedures related to breach notification.

The new requirements apply if *all* of the following are present:

- There is a “breach.” A “breach” is defined as the unauthorized acquisition, access, use, or disclosure of protected health information (“PHI”). (There are exceptions which are defined below.)
- PHI was “unsecured” at the time of the breach. “Unsecured” is defined as PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals using the technology or a methodology specified by HHS guidance.
- The breach “compromises the security of the PHI.” This occurs when there is a significant risk of financial, reputational, or other harm to the individual whose PHI has been compromised.

This rule does not replace the Privacy or Security Rules but concerns only what to do in the event of a security breach. See ACP’s HIPAA [Privacy and Security Manuals](#) for information on how to comply with these rules.

Exceptions

The rule defines the following exceptions where notification of a breach is NOT required:

1. When a workforce member of the practice or business associate, acting in good faith and within the scope of authority, unintentionally acquires, accesses, or uses PHI, and it doesn't result in further unpermitted uses or disclosures,
2. When an authorized person inadvertently discloses to another authorized person or entity, and the information disclosed is not further used or disclosed in a manner not permissible, or
3. When the unauthorized recipient of the PHI would in good faith not reasonably be able to retain such information.

These exceptions assume that the practice would conduct a risk assessment each time a breach occurs. Did the breach meet one of the exceptions? If not, what is the risk and what type of notification is required to meet the requirements?

Definitions

Breach – The acquisition, access, use, or disclosure of PHI not permitted by the Privacy Rule that “compromises the security and privacy” of the PHI. In this case, “compromises” is defined to mean “poses a significant risk of financial, reputational, or other harm” to the individual(s) whose PHI was breached. As of this writing, it is incumbent on the practice to determine “harm” for each breach that occurs.

Unsecured PHI – PHI that is not rendered unusable, unreadable, or indecipherable by one or more of the following methods:

(1) Encryption. Electronic PHI is only secure if it is encrypted. The HIPAA Security Rule specifies encryption as using an algorithmic process to convert data into a form resulting in a low probability of assigning meaning without a specific process or key. There are various encryption processes that meet this standard. In addition, that decryption process or key also must not have been breached. This applies both to data at rest (as stored) or in motion (such as in email or other transmission).

(2) Destruction. Hard copy PHI is only secured when it has been shredded or destroyed such that the PHI cannot be read or otherwise reconstructed. Likewise, electronic media must be cleared, purged, or destroyed such that PHI cannot be retrieved or accessed.

Requirements

The practice (the covered entity) and its business associate(s) should analyze the following to determine whether a breach of unsecured PHI has occurred:

- (1) Determine whether the use or disclosure of PHI violates the HIPAA Privacy Rule. For an acquisition, access, use, or disclosure of PHI to constitute a breach, it must violate the Privacy Rule. For example, if information is de-identified, it is not PHI

and thus any inadvertent or unauthorized use or disclosure of such information would not be considered a breach.

- (2) Determine whether the use or disclosure compromises the security and privacy of PHI. In other words, if an impermissible use or disclosure “poses a significant risk of financial, reputational, or other harm to the individual,” then it is a breach. The Rule provides a number of factors which should be taken into account when conducting a risk assessment. A covered entity should consult its legal counsel with respect to the impact of the presence of such factors.
- (3) Determine whether any exceptions to the breach definition apply.

The practice or business associate has the burden of proving why a breach notification is not required and must document why the impermissible use or disclosure fell under one of the exceptions. The practice should document the risk and other breach assessments accordingly (Exhibit 1).

Notification

Once it has been determined that a breach did occur and that none of the exceptions apply, the practice should implement reasonable breach discovery procedures. (See Figure 1.)

- Notification to Individuals (Exhibit 2). The practice must send the required notification to each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of the breach no later than 60 calendar days after the date the breach was first discovered by the covered entity. See below for the specific content requirements and the methodology required for providing such breach notices.
 - If insufficient contact information is available for some or all of the affected individuals, a substitute notice (Exhibit 3) is required as soon as reasonably possible. If there is insufficient contact information for 10 or more individuals, then substitute notice must be provided via a 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. In such instances, the covered entity is also required to have an active toll-free number for 90 days so that an individual can find out whether his or her unsecured PHI may be included in the breach.
- Notification to Media. If the breach affects more than 500 residents of a state or jurisdiction, notice must be in prominent media outlets serving that state or jurisdiction without unreasonable delay and no later than 60 calendar days after the date the breach was discovered by the covered entity.
- Notification to HHS. If more than 500 individuals are involved in the breach, regardless of where those individuals live, then the practice must notify HHS at the same time as making the individual notifications. For breaches involving fewer than 500 individuals, the practice must maintain an internal log of such breaches and submit the log annually to HHS.

- Notification by a Business Associate. Following the discovery of a breach of unsecured PHI, a business associate is required to notify the practice of the breach so that the practice can then notify the affected individuals. To the extent possible, the business associate should identify each individual whose unsecured PHI has been, or is reasonably believed to have been, breached. Such notice should be given within 60 days following the discovery of a breach.
- Delay Required by Law Enforcement. A breach notification may be delayed if law enforcement determines that notification would impede a criminal investigation or cause damage to national security.

How this Interim Final Rule relates to HIPAA rules and State Laws

HHS emphasizes that this Rule does not modify a covered entity's responsibilities with respect to the HIPAA Security Rule; nor does it impose any new requirements upon covered entities to encrypt all PHI. A covered entity may still be in compliance with the Security Rule even if it decides not to encrypt electronic PHI as long as it uses another method to safeguard information in compliance with the Security Rule. However, if such method is not in compliance with the requirements of the Rule with respect to securing PHI, then the covered entity will be required to provide a breach notification to affected individuals upon a breach of unsecured PHI. This Rule preempts contrary State breach notification laws. However, a covered entity must still comply with requirements of State law that are *in addition to* the requirements of this Rule, but not contrary to such requirements (such as additional elements required to be included in a notice).

Figure 1

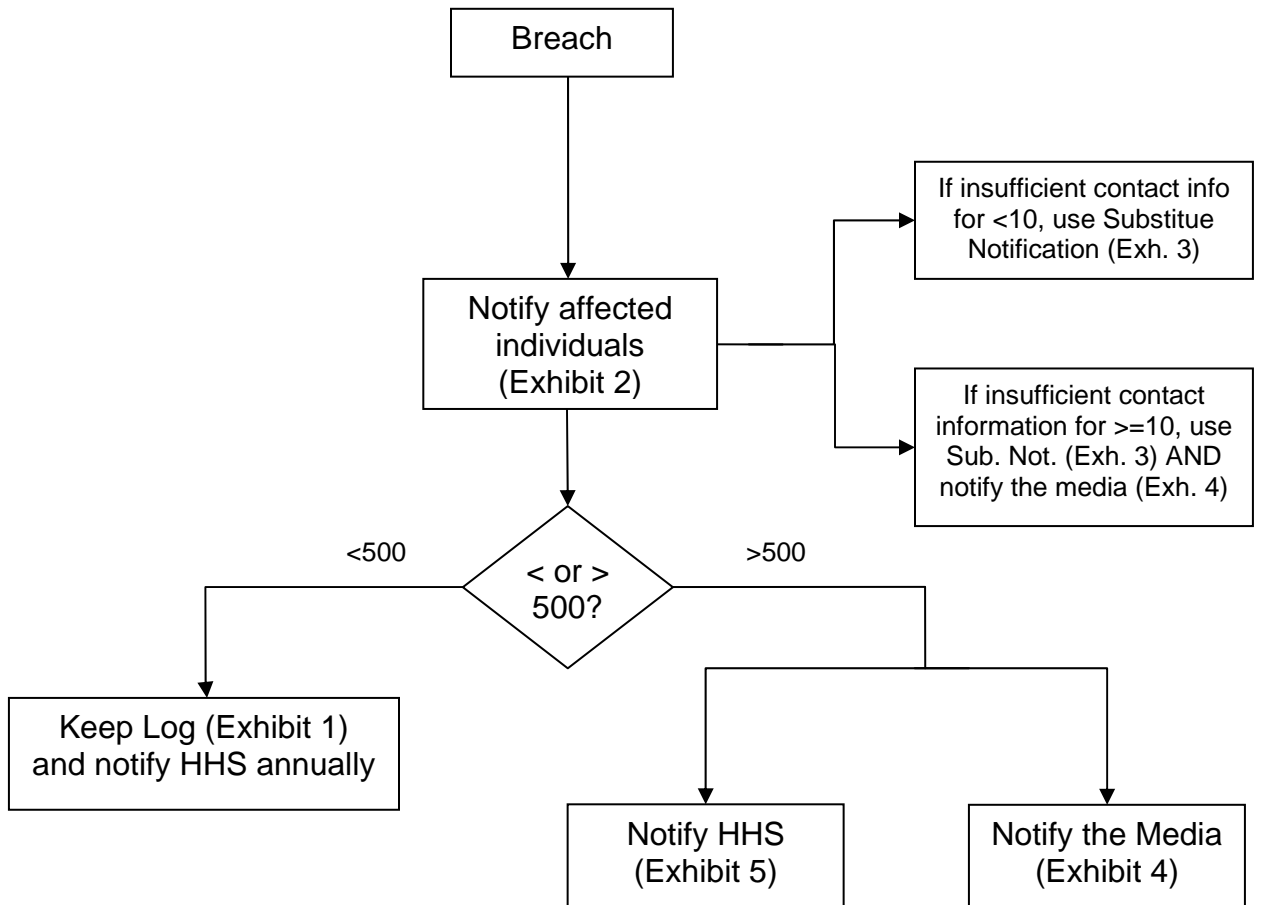


EXHIBIT 2
SAMPLE NOTIFICATION TO PATIENTS

This template should be used in the event of a breach within 60 days of the discovery of a breach. It should be sent by first-class mail to the individual(s) at the last known address. If the individual is deceased, it must be sent to the individual's next of kin or other designated representative, if known. If the affected individual has agreed to receive email notification, then this letter may be sent electronically. If written notification is not possible because there is insufficient or out of date contact information, then substitute notice may be given (see Exhibit 3).

Dear Patient,

In accordance with 45 CFR Parts 160 and 164, this letter is to notify you of a recent occurrence that resulted in a breach of protected health information.

Description of what happened: [insert paragraph describing what the breach was, how it happened, etc.]

Date of the breach: [insert date the breach occurred]

Date of discovery: [insert date you learned of the breach]

Description of the types of unsecured protected health information (PHI) that were involved:

[insert list of data elements that might have been breached, such as name, SSN, DOB, address, diagnosis, or other personal information]

Steps you should take to protect yourself from potential harm resulting from this incident: [insert suggestions on what to do such as be vigilant of bills for services they did not receive, notify their credit card company, or other applicable suggestions based on the circumstances of the situation]

Please know that we are doing everything we can to investigate this breach, to protect you in any way that we can to mitigate any harm to you, and to protect against any further breaches of information. If at any point you discover that your information has been used inappropriately, please notify us and we will work with you to make sure the proper authorities are involved as warranted by the situation.

If you have any questions about this incident, please contact [insert Privacy Officer's name here] at [insert office phone, address, and an email address that is used regularly by the practice and/or Privacy Officer]. Again, we apologize for any inconvenience this might cause or might have caused.

Sincerely,

[insert practice name]

EXHIBIT 3 SUBSTITUTE NOTICE

If the practice cannot provide written notification due to insufficient or incorrect contact information, a substitute notice may be used.

If the number of individuals that cannot be notified is fewer than 10, the practice may use telephone or some other alternate means of notification. If the number of individuals requiring notice is 10 or more, then the substitute notice must:

1. Be conspicuously posted for 90 days on the practice's Web site home page or in a major media outlet in the geographic area where most of the individuals reside.
2. Include a toll-free number that is active for 90 days. Temporary toll free numbers can be set up on a pay per minute basis.

If the situation is urgent because of possible imminent misuse, the practice may contact the affected individuals by telephone or other means, as appropriate.

EXHIBIT 4 NOTIFICATION OF MEDIA

For a breach of unsecured PHI involving more than 500 residents of a particular jurisdiction, the practice must provide notification in a prominent media outlet serving that jurisdiction.

- Such notification must occur within 60 days after the discovery of the breach.
- The notification must meet the same requirements as shown in Exhibit 1.

EXHIBIT 5 NOTIFICATION OF THE SECRETARY OF HHS

The practice shall notify the Secretary ANY breach regardless of how many individuals are affected. The HHS Web site will provide specifics regarding reporting requirements.

- For breaches involving 500 or more individuals, the practice will notify the Secretary at the same time as notifying the individuals (Exhibit 2) and the media (Exhibit 4).
- For breaches involving fewer than 500 individuals, the practice will keep a log (Exhibit 1) and report annually.