Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

Reporting HIPAA Breaches: Annual Deadline Approaches

Publication — 01/09/2018

The HIPAA breach notification rule requires covered entities to report breaches of unsecured protected health information ("PHI") to affected individuals, HHS and, in some cases, local media. (45 CFR § 164.400 *et seq.*). The notice must be sent to individuals as soon as reasonably possible but no later than 60 days after it was discovered. (45 CFR § 164.404). The timing of notice to HHS depends on the number of persons affected by the breach: if the breach involves 500 or more persons, the covered entity must notify HHS at the same time it notifies the individual; if the breach involves less than 500 persons, the covered entity must report the breach to HHS until no later than 60 days after the end of the calendar year, *i.e.*, by March 1. (45 CFR § 164.408(b)-(c)).

Is Your HIPAA Breach Reportable? Under the breach notification rule, covered entities are only required to self-report if there is a "breach" of "unsecured" PHI. (45 CFR § 164.400 *et seq.*).

1. Unsecured PHI. "Unsecured" PHI is that which is "not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology" specified in HHS guidance. (45 CFR § 164.402). Currently, there are only two ways to "secure" PHI: (1) in the case of electronic PHI, by encryption that satisfies HHS standards; or (2) in the case of e-PHI or PHI maintained in hard copy form, by its complete destruction. (74 FR 42742). Breaches of "secured" PHI are not reportable. Most potential breaches will involve "unsecured" PHI.

2. Breach. The unauthorized "acquisition, access, use, or disclosure" of unsecured PHI in violation of the HIPAA Privacy Rule is presumed to be a reportable breach unless the covered entity or business associate determines that there is a low probability that the data has been compromised or the action fits within an exception. (45 CFR § 164.402; see 78 FR 5641). Thus, the covered entity or business associate must determine the following:

a. **Was there a violation of the Privacy Rule?** Breach notification is required only if the acquisition, access, use or disclosure results from a Privacy Rule violation; no notification is required if the use or disclosure is permitted by the Privacy Rule. (45 CFR § 164.402). For example, a covered entity may generally use or disclose PHI for purposes of treatment, payment, or healthcare operations without the individual's authorization unless the covered entity has agreed otherwise. (45 CFR § 164.506). Disclosures to family members and others involved in the individual's care or payment for their care is generally permitted if the patient has not objected and the provider otherwise determines that disclosure is in the

patient's best interest. (45 CFR § 164.510). HIPAA allows certain other disclosures that are required by law or made for specified public safety or government functions. (45 CFR § 164.512). Disclosures that are incidental to permissible uses or disclosures do not violate the Privacy Rule if the covered entity employed reasonable safeguards. (45 CFR §§ 164.402 and 164.502(a)(1)(iii)). When in doubt as to whether a disclosure violates the Privacy Rule, you should check with your privacy officer or a qualified attorney.

b. **Does the violation fit within a breach exception?** The following do not constitute reportable "breaches" as defined by HIPAA:

    1. An unintentional acquisition, access, or use of PHI by a workforce member if such acquisition, access, or use was made in good faith and within the scope of the workforce member's authority and does not result in further use or disclosure not permitted by the Privacy Rule. (45 CFR § 164.402). For example, no notification is required where an employee mistakenly looks at the wrong patient's PHI but does not further use or disclose the PHI. (74 FR 42747).

    2. An inadvertent disclosure by a person who is authorized to access PHI to another person authorized to access PHI at the same covered entity or business associate, and the PHI is not further used or disclosed in a manner not permitted by the Privacy Rule. (45 CFR § 164.402). For example, no notification is required if a medical staff member mistakenly discloses PHI to the wrong nurse at a facility but the nurse does not further use or disclose the PHI improperly. (74 FR 42747-48).

    3. A disclosure in which the person making the disclosure has a good faith belief that the unauthorized recipient would not reasonably be able to retain the PHI. (45 CFR § 164.402). For example, no notification is required if a nurse mistakenly hands PHI to the wrong patient but immediately retrieves the information before the recipient has a chance to read it. (74 FR 42748).

c. **Is there a "low probability that the data has been compromised?"** No report is required if "there is a low probability that the [PHI] has been compromised based on a risk assessment" of at least the following factors listed in 45 CFR § 164.402:

    1. **The nature and extent of the PHI involved**, including the types of identifiers and the likelihood of re-identification. For example, PHI involving financial data (*e.g.*, credit card numbers, social security numbers, account numbers, *etc.*), sensitive medical information (*e.g.*, mental health, sexually transmitted diseases, substance abuse, *etc.*), or detailed clinical information (*e.g.*, names and addresses, treatment plan, diagnosis, medication, medical history, test results,

etc.) create a higher probability that data has been compromised, and must be reported. (78 FR 5642-43). In the Interim Breach Notification Rule, HHS gave the following additional examples:

> 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.

(74 FR 42745). Although the Final Breach Notification Rule changed the "significant risk" test to the "low probability" standard, HHS's commentary may still be helpful in evaluating whether there is a reportable breach.

2. **The unauthorized person who impermissibly used the PHI or to whom disclosure was made.** For example, disclosure to another health care provider or a person within the entity's organization would presumably create a lower risk because such persons are more likely to comply with confidentiality obligations and are unlikely to misuse or further disclose the PHI. HHS offered the following example in the Omnibus Rule commentary:

> if a covered entity misdirects a fax containing protected health information to the wrong physician practice, and upon receipt, the receiving physician calls the covered entity to say he has received the fax in error and has destroyed it, the covered entity may be able to demonstrate after performing a risk assessment that there is a low risk that the protected health information has been compromised.

(78 FR 5642). Similarly, there is a lower risk of compromise if the entity who receives the PHI lacks the ability to identify entities from the limited information disclosed. (78 FR

5643).

3. **Whether the PHI was actually acquired or viewed.** For example, there is likely a low risk if a misdirected letter is returned unopened or a lost computer is recovered and it is confirmed that PHI was not accessed. Conversely, there is a higher risk where the recipient opens and reads a misdirected letter even though she reports the letter to the covered entity. (78 FR 5643).

4. **Whether the risk to the PHI has been mitigated.** For example, there may be a lower risk if a fax is directed to the wrong number, but the recipient confirms that they returned or destroyed the PHI; the PHI has not been and will not be further used or disclosed; and the recipient is reliable. (78 FR 5643). This factor highlights the need for covered entities and business associates to immediately identify and respond to potential breaches to reduce the probability that PHI is compromised and the necessity of breach reporting.

   The risk assessment should involve consideration of all of these factors in addition to others that may be relevant. One factor is not necessarily determinative, and some factors may offset or outweigh others, depending on the circumstances. (*See* 78 FR 5643). If you conclude that the risk assessment demonstrates a low probability that the PHI has been compromised, you should document your analysis and you may forego breach notification. On the other hand, if the risk assessment fails to demonstrate a low probability that the PHI has been compromised, you are required to report the breach to the affected individual and HHS as described below.

How Do I Report? If the breach is reportable, the covered entity and business associate must make the required reports; HHS has indicated that failure to do so will likely constitute "willful neglect", thereby triggering mandatory penalties if discovered. (75 FR 40879).

1. Notice to the Covered Entity. Business associates must notify the covered entity within 60 days after discovery so that the covered entity may provide the required notices to others. (45 CFR § 164.410(c)). Covered entities may want to ensure their business associate agreements shorten the time for business associate reports to, *e.g.*, three days, thereby allowing the covered entity to respond promptly to suspected breaches and minimize liability.

2. Notice to the Individual. Covered entities must notify the affected individual or their personal representative without unreasonable delay, but in no event longer than 60 days following discovery. (45 CFR § 164.404(b)). In general, the notice must be sent by first class mail and contain the following information: a brief description of the breach, including the dates of the breach and its discovery; a description of the types of unsecured PHI involved; steps the individual should take to

protect themselves from resulting harm; a description of the covered entity's actions to investigate, mitigate and protect against future violations; and the procedures the individual may take to contact the covered entity for more information. (45 CFR § 164.404(c)-(d)). There are alternative notice procedures if the covered entity does not know the identity or contact information for affected persons. (*Id.*).

3. Notice to HHS. Breaches of unsecured PHI must also be reported to HHS: breach reports involving more than 500 persons must made within 60 days; breaches involving 500 or less must be reported within 60 days after the end of the calendar year. Covered entities submit the report electronically using the form available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html. The OCR posts the names of entities with breaches involving more than 500 persons on the OCR's wall of shame, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

4. Notice to Media. If the breach involves more than 500 persons in a state, the covered entity must also notify local media within 60 days of discovery. (45 CFR § 164.406). The notification must contain information similar to that provided to individuals. (*Id.* at 164.408(c)).

Documentation. A covered entity is required to maintain documentation concerning its breach analysis and/or reporting for six years. (45 CFR §§ 164.414 and 164.530(j)).

Accounting Logs. Whether or not the breach is reportable to the individual or HHS, covered entities and business associates are still required to record impermissible disclosures in their accounting of disclosure logs as required by 45 CFR § 164.528. The log must record the date of the disclosure; name and address of the entity who received the PHI; a brief description of the PHI disclosed; and a brief statement of the reason for the disclosure. (45 CFR § 164.528(b)). If requested, the covered entity must disclose the log to the individual or the individual's personal representative within 60 days. (*Id.* at 164.528(c)).

Avoid Reports by Avoiding Breaches. Of course, it is better to avoid a breach rather than respond to one. To that end, covered entities and business associates should ensure that they practice preventive medicine by, among other things, encrypting PHI when possible and implementing other required policies and administrative, technical, and physical safeguards to protect PHI. They should train and regularly remind workforce members concerning HIPAA obligations, periodically monitor compliance, and respond promptly to correct weaknesses.

For questions regarding this update, please contact:
Kim C. Stanger
Holland & Hart, 800 W Main Street, Suite 1750, Boise, ID 83702
email: kcstanger@hollandhart.com, phone: 208-383-3913