Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

HIPAA Breach Notification: When and How to Self-Report

Publication — 01/08/2019

So you just discovered that protected health information ("PHI") from your organization was improperly accessed or disclosed. Are you required to self-report the violation to the affected individual and HHS?

HIPAA Breach Notification Rule. Not all HIPAA violations are required to be reported to the relevant patient or HHS. 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: (i) in the case of electronic PHI, by encryption that satisfies HHS standards; or (ii) 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 rules. (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. (*Id.* at § 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. (*Id.* at § 164.510). HIPAA allows certain other disclosures that are required by law or made for specified public safety or government functions. (*Id.* at § 164.512). Disclosures that are incidental to permissible uses or disclosures do not violate the privacy

rule if the covered entity employed reasonable safeguards. (*Id.* at §§ 164.402 and .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 breach exception?* The following do not constitute reportable "breaches" as defined by HIPAA:

    i. 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 rules. (*Id.* at § 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).

    ii. 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 rules. (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).

    iii. 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:

    i. 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).

ii. 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. 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).

iii. 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).

iv. 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.

d. *When in doubt, it is likely safer to report.* When in doubt, it is safer to report the breach because the failure to report may

constitute willful neglect, thereby exposing the covered entity or business associate to mandatory penalties under the HIPAA enforcement penalties. (75 FR 40879).

3. **Reporting the Breach.** If the breach notification rule requires a report, the covered entity and business associate must make the required reports to both the individual and HHS.

    a. *Notice to 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.

    b. *Notice to 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. (*Id.* at § 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.*).

    c. *Notice to HHS.* The timing of notice to HHS depends on the number of persons affected by the breach. If the breach involves less than 500 persons, the covered entity may wait to report the breach to HHS until no later than 60 days after the end of the calendar year. (45 CFR § 164.408(c)). If the breach involves 500 or more persons, the covered entity must notify HHS at the same time it notifies the individual. (*Id.* at § 164.408(b)). Covered entities should submit the report electronically using the form available here. 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.

    d. *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)).

4. **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)).

5. **Log the disclosure in accounting log.** Whether or not the unauthorized disclosure 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)).

6. **Don't forget state breach reporting requirements.** Most if not all states have their own breach reporting statutes that apply to certain breaches of specified confidential information. They usually apply if there is a potential misuse of computerized data involving names in connection with social security numbers, account numbers, personal identification numbers, etc. Covered entities and business associates should consider whether state laws apply in addition to HIPAA.

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