HOLLAND&HART

Responding to HIPAA Breaches

11/06/2015

by Kim Stanger

HIPAA privacy and security breaches can result in fines of $100 to $50,000 to covered entities (including healthcare providers and health plans) and their business associates. (45 CFR 160.404). If the violation resulted from "willful neglect", the Office for Civil Rights ("OCR") must impose a mandatory fine of $10,000 to $50,000. (45 CFR 160.404). To make matters worse, covered entities and their business associates must self-report breaches of unsecured protected health information ("PHI") to the affected individual and to HHS (45 CFR 164.400); failure to do so may constitute "willful neglect" resulting in additional fines. The good news is that the OCR may not impose a fine so long as the covered entity or business associate did not act with "willful neglect" and corrected the problem within 30 days. (45 CFR 160.410(b)).

Responding to Possible Breaches. Given the potential consequences, it is critical that covered entities and business associates respond appropriately to potential HIPAA breaches to avoid or minimize their liability. Below are steps that you may follow to help you identify and timely respond to HIPAA breaches.

1. Stop the breach. Immediate action may help avoid or mitigate the effects of a breach. Terminate improper access to PHI; retrieve any PHI that was improperly disclosed; and obtain assurances from recipients that they have not, or will not, further use or disclose PHI that was improperly accessed. Document your actions.

2. Notify the privacy officer. Each covered entity must have a designated privacy officer who has the training and experience to properly investigate and respond to a potential breach. Deadlines for responding to breaches generally run from the date that anyone in the organization knew of the breach except the person committing the breach (*see* 45 CFR 164.404(b); 78 FR 5647); accordingly, workforce members should be trained to notify the privacy officer as soon as they become aware of a breach.

3. Respond promptly. Swift, appropriate action is critical for at least four reasons. First, covered entities have an affirmative obligation to mitigate the effects of any breach. (45 CFR 164.530(f)). Second, prompt action may help avoid or mitigate further breaches, which is

an important factor in determining whether a breach is reportable. (45 CFR 164.402). Third, as discussed above, a covered entity or business associate may avoid penalties if they correct a violation within 30 days. (45 CFR 160.410(b)). And fourth, the breach notification rule requires that notice of reportable breaches be given "without unreasonable delay," but no later than 60 days after discovery. (45 CFR 164.404).

4. Investigate appropriately. Confirm the "who, what, when, why, and how" with persons involved, including persons who committed the alleged violation; persons who may have received PHI improperly; and other relevant witnesses. Confirm the nature and scope of the PHI that was accessed, used. or disclosed, and why they accessed or disclosed the PHI. Ensure there was no redisclosure or will not be any further redisclosure. In your discussions, ensure that you do not inadvertently disclose additional PHI. Also, beware of jumping the gun: sometimes a full investigation reveals additional facts that confirm no reportable breach occurred. Do not report a suspected breach before you have actually concluded that a reportable breach occurred. Document your investigation, including obtaining witness statements or sending confirming letters as appropriate. For example, you may want to send a letter to alleged recipients confirming the extent of their access or disclosure of PHI, and warning them of the penalties that may apply if they further use or disclose PHI improperly. (*See* 42 USC 1320d-6).

5. Mitigate the effects of the breach. HIPAA requires that a covered entity mitigate any harmful effects of a breach to the extent practicable. (45 CFR 164.530(f)). Mitigation may include retrieving, deleting, or destroying improperly disclosed PHI; terminating access or changing passwords; remote wiping mobile devices; modifying policies or practices; and/or warning recipients of potential penalties for further violations. In some cases, it might include paying for the cost of a credit monitoring service or similar action, and/or notifying affected individuals even if the breach is not reportable under the breach notification rules. The response will depend on the circumstances. If a covered entity knows that a business associate is violating HIPAA, it must either take steps to cure the breach or terminate the business associate agreement. (45 CFR 164.504(e)(1)).

6. Correct the breach. Remember: a covered entity may avoid HIPAA penalties if it did not act with willful neglect and corrects the problem within 30 days. (45 CFR 160.410(b)). Although you may not be able to "unring" the bell, you can ensure that the bell does not continue ringing by, *e.g.*, changing processes; implementing new safeguards; modifying policies; and/or training employees. (*See* 75 FR 40879).

7. Impose sanctions. HIPAA requires that covered entities have, apply, and document appropriate sanctions against workforce members who

violate HIPAA or privacy policies. (45 CFR 164.530(e)). The sanction should fit the crime: it may range from a written warning and additional training to suspension or termination.

8. Determine if the breach is reportable to the individual and 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*.).

a. **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.

b. **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:

    1. **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 164l.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 .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.

2. **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. (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).

    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:

    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).

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. 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.

9. If required, report the breach to the individual and HHS. If the breach notification rule requires a report, 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).

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. (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*.).

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 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.

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)).

e. **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)).

10. Log the breach in accounting log. 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)).

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, implementing required policies and administrative, technical, and physical safeguards to protect PHI, and periodically monitor compliance. Train and regularly retrain or remind workforce members concerning HIPAA obligations. Use past breaches to improve systems and future performance. Consider purchasing appropriate privacy insurance to cover the costs if breaches do occur, and include indemnification or other provisions in business associate agreements to protect yourself and/or shift the costs of potential breaches.

A sample breach notification policy is available here.

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