Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

New HIPAA Breach Notification Standard

New HIPAA Breach Notification Standard

Insight — 2/4/2013

On January 25, 2013, the Department of Health and Human Services ("HHS") officially published its new HIPAA omnibus rule. Among other things, the new rules and accompanying commentary reaffirm a lower standard for reporting privacy breaches to patients and HHS than many providers had previously applied. The new standard will require providers to self-report more breaches, thereby exposing providers to more patient complaints, government investigations, and potential penalties for HIPAA violations.

Old Standard. Under HHS's interim rule, covered entities were not required to report breaches of PHI that did not pose "a significant risk of financial, reputational or other harm to the individual." (45 C.F.R. § 164.402, definition of "breach"). This "no harm, no foul" standard allowed covered entities to avoid reporting many if not most privacy breaches. It also drew the ire of privacy advocates and some members of Congress, who claimed that the HITECH Act did not authorize a "harm" standard. HHS capitulated to their objections by removing the former "harm" standard from the omnibus rule.

New Standard. Under the new standard, the acquisition, access, use or disclosure of PHI in violation of the privacy rules is presumed to be a reportable breach unless the covered entity or business associate demonstrates that

> there is a low probability that the [PHI] has been compromised based on a risk assessment of at least the following factors:
> (i) The nature and extent of the [PHI] involved…;
> (ii) The unauthorized person who used the [PHI] or to whom the disclosure was made;
> (iii) Whether the [PHI] was actually acquired or viewed; and
> (iv) The extent to which the risk to the [PHI] has been mitigated.

(45 C.F.R. § 164.402, definition of "breach", emphasis added).

When is PHI "Compromised"? Unfortunately, the new regulation does not define "compromised." For purposes of breach notification, the mere acquisition, use or disclosure of PHI alone does not necessarily mean that the PHI has been compromised. HHS noted that a contrary rule would overburden both covered entities and individual recipients with reports of "inconsequential" breaches. (78 FR 5641-42). Instead, "whether the [PHI] was actually acquired or viewed" is just one factor in assessing the risk that PHI may be compromised; it is not the sole factor. (45 C.F.R. § 164.402). For data to be "compromised," there must be something else—

some risk of misuse or adverse consequences to the individual. For example, HHS commented that "[c]onsidering the type of [PHI] involved in the impermissible use or disclosure will help entities determine the probability that the [PHI] could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipient's own interests." (78 F.R. 5642). Although ill-defined, this new standard appears to focus on the potential for the recipient's unauthorized use or misuse of the data rather than subjective harm to the individual. This seems consistent with the common definition of "compromise", which means: "[a] to expose to suspicion, discredit, or mischief…; [b] to reveal or expose to an unauthorized person and especially to an enemy." (www.merriam-webster.com/dictionary/compromise).

Risk Assessment. To determine the probability that PHI has been "compromised" (whatever that means), entities must conduct a risk assessment of the following factors:

- **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 F.R. 5642-43).
- **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 F.R. 5643).
- **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. (*Id.*).
- **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. (*Id.*). 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 F.R. 5643). If the entity concludes that the risk assessment demonstrates a low probability that the PHI has been compromised, the entity should document its analysis and may forego breach notification. On the other hand, if the risk assessment fails to demonstrate a low probability that the PHI has been compromised, the entity is required to report the breach unless one of the regulatory exceptions applies.

Exceptions to Breach Notification. 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, including disclosures that are incidental to a permissible use or disclosure despite the use of reasonable safeguards ("incidental disclosures"). (45 C.F.R. §§ 164.402 and .502(a)(1)(iii)). Also, notification is only required for breaches of "unsecured" PHI; it is not required for breaches of electronic data that has been encrypted consistent with HHS standards. (*Id.* at § 164.402). Even if there is a breach, no notification is required in the following situations:

- **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 C.F.R. § 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.
- **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. (*Id.*). 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.
- **A disclosure where the person making the disclosure has a good faith belief that the unauthorized recipient would not reasonably be able to retain the PHI.** (*Id.*). 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.

Even if there is no reportable breach, however, covered entities and business associates may still be required to record impermissible disclosures in their accounting of disclosure logs as required by 45 C.F.R. § 164.528.

Conclusion. In issuing the new breach rule, HHS confirmed that:

> breach notification is necessary in all situations except those in which the covered entity or business associate, as applicable, demonstrates that there is a low probability that the

> [PHI] has been compromised (or one of the other exceptions to the definition of breach applies).

(78 F.R. 5641). Given the presumption in favor of disclosure and the "low probability" of avoiding notification if there is a breach, covered entities should reexamine and renew their efforts to avoid breaches. If a potential breach occurs, covered entities should carefully evaluate whether the breach notification rule applies since reporting breaches to patients and HHS may result in complaints, investigations, and potential penalties. To that end, the following checklist may help entities evaluate whether a breach is reportable.

Checklist for Breach Notification Analysis

- Was there an unauthorized access, acquisition, use or disclosure of protected health information ("PHI"), i.e., individually identifiable information concerning a person's health, healthcare or payment for their healthcare?
- Was the PHI encrypted? PHI that is encrypted or otherwise secured as defined HHS is not subject to breach notification. (*Id.* at § 164.402 and .404).
- Did the access, acquisition, use or disclosure violate the HIPAA privacy rules? The following uses or disclosures generally do not violate HIPAA privacy rules or require breach notification:
    - Incidental disclosures, i.e., disclosures incidental to a permitted use or disclosure despite the use of reasonable safeguards. (45 C.F.R. § 164.502(a)(1)(iii)).
    - Use or disclosures for purposes of treatment, payment or healthcare operations. (*Id.* at § 164.506).
    - Use or disclosures consistent with a valid authorization. (*Id.* at § 164.508).
    - Disclosures to family members or others involved in the patient's care or payment for care. (*Id.* at § 164.510(b)).
    - Disclosures to avoid a serious and imminent threat of harm. (*Id.* at § 164.512(j)).
    - Use or disclosures required by law; for public health activities; for abuse reporting; for health oversight functions; for judicial or administrative proceedings; for certain law enforcement purposes; or for workers compensation. (*Id.* at § 164.512(a)-(f), (l)).
- Is there a low probability that the PHI has been compromised based on a risk assessment of the following factors? If so, there is no duty to report the breach. You should carefully document your risk assessment and conclusion. (*Id.* at § 164.402).
    - What kind of and how much PHI was involved? For example, did the breach involve financial, sensitive, or detailed information?
    - Who used or received the PHI? For example, is the recipient covered by HIPAA or otherwise required to protect

the confidentiality of PHI?

- What is the probability that the PHI has been or will be acquired or viewed?
- Has the risk to the PHI been mitigated? For example, have you obtained reliable assurances that the use or disclosure was very limited, the PHI has been returned or destroyed, and that the PHI will not be further used or disclosed?
- Are there other relevant circumstances that should be considered?

- Does an exception to the breach notification rule apply? If so, there is no duty to report the breach. (*Id.* at § 164.402).
  - Did the breach involve the unintentional acquisition, access or use of PHI by a workforce member (or other person acting under the authority of the covered entity or business associate) who was acting in good faith and within the scope of their authority, and there was no further improper use or disclosure?
  - Did the breach involve an inadvertent disclosure by an authorized person to another authorized person at the same entity, and there was no further improper use or disclosure of PHI?
  - Do you have a good faith belief that the person to whom the PHI was disclosed would not reasonably be able to retain the PHI?

For questions regarding this update, please contact
Kim C. Stanger
Holland & Hart, U.S. Bank Plaza, 101 S. Capitol Boulevard, Suite 1400, Boise, ID 83702-7714
email: kcstanger@hollandhart.com, phone: 208-383-3913
