Health Information Compliance Alert

HIPAA Quiz Answers: See How You Fared on Breach Notification

Hint: BAs have direct liability, too.

After you've read the questions carefully and decided on your answers, check your knowledge against the experts.

Answer 1: False. Not every issue can be defined as a breach, and there are three exceptions, admits the **HHS Office for Civil Rights** (OCR) in its guidance.

Definition: "According to the Privacy Rule, a breach is any acquisition, access, use, or disclosure in violation of the privacy rule - and that covers a lot," says **Jim Sheldon-Dean,** founder and director of compliance services at **Lewis Creek Systems, LLC** in Charlotte, Vermont.

However, there are exceptions under which CEs aren't required to report the breach, according to Dean. They include:

- **Unintentional internal use, in good faith**: For instance, if you put a folder on the wrong desk and a physician opens it, says, "Oh, these aren't my patient's notes, these belong to someone else" and closes it, you aren't required to report that.
- **Inadvertent internal use, within job scope:** For example, someone looks up the records for Mary Smith but opens the notes for the wrong Mary Smith, realizes her mistake, and then closes out the notes.
- **Information cannot be retained:** For instance, you lose a box of medical records and you find them the next day with the box still sealed the way you left them, and you know the information was not breached.

Answer 2: False. "Breach notification obligations differ based on whether the breach affects 500 or more individuals or fewer than 500 individuals," OCR says. However, if a CE doesn't know how many patients were affected, it must still offer the HHS secretary an estimate of how many individuals had their PHI exposed - and submit updates accordingly.

Answer 3: True. According to OCR guidance, CEs may post "substitute" breach notifications when 10 or more of their patients' contact information is "insufficient or out of date."

Here are the details for releasing substitute breach notifications:

- Post the breach specifics on your website for at least 90 days.
- Announce the breach details in the state or jurisdiction where the incident occurred on print or broadcast media for at least 90 days.
- Institute a toll-free phone number that is active for at least 90 days for patients to call with questions.

Answer 4: True. When CEs expose patients' PHI, whether accidentally or purposely, they violate HIPAA, requiring them to report it - ASAP. Plus, if a CE doesn't report the breach according to the rules, it could get nicked for willful neglect.

Why? If a patient finds out that her PHI was breached and the CE did not properly notify her, she may file a complaint with HHS. If a patient files a complaint before the CE files an individual breach notice, it will be too late for the organization to be in compliance, reports Sheldon-Dean.

Depending on the size and scale of a breach, three different factions must be notified under the Breach Notification Rule. OCR expects CEs to inform these entities of the violation in this order if a breach occurs:

- **Individuals:** You must immediately notify any patient, business associate (BA), employee, etc., that the breach affects.
- **Secretary:** You must notify the HHS Secretary of any breaches by completing a breach report form, which

can be found online at www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

- **Media:** If you experience a breach that affects more than 500 residents of a state or jurisdiction, you must notify the affected individuals and "provide notice to prominent media outlets serving the state or jurisdiction," OCR reports.

Answer 5: False. Notifying patients after a breach is paramount, and the disclosure must include particular elements outlined by the feds in HIPAA. The notification must have the following:

- The date of the breach;
- The date of the discovery of the breach;
- The information that was breached;
- Steps the individual should take to protect PHI;
- What the CE is doing to remedy the breach. (For example: "Practice is investigating the incident", "Practice is evaluating mitigating impacts that might have contributed to the breach", "Practice is forming an action plan to protect against future breaches", etc.); and
- CE contact information if the individual has questions, including practice phone number, email address, postal address, website, etc.

Answer 6: False. BAs, just like CEs, "have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach," cautions OCR guidance.

Check out the direct liability of BAs at www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html.

Answer 7: True. According to the feds, CEs are held to a higher standard and must follow up after a breach with certain administrative requirements, including written breach notification "policies and procedures;" staff training on the protocols; and "sanctions against" employees who don't comply with the rules.

Expert advice: Don't try to avoid a breach - accept it and follow the policies and procedures, advises attorney **Lauren M. Ramos,** with **McGuire Woods LLP** in Richmond, Virginia. "Collect all the facts as quickly as possible, mitigate the damages to [the] greatest extent possible, and loop in legal counsel as early as possible."

OCR looks favorably on those who comply with the HIPAA breach requirements, Ramos indicates. "Providers should remember that OCR does not investigate every breach, especially small ones. In fact, OCR likely investigates only a small percentage of all reported breaches. Following the correct procedures and reporting a breach does not mean that an OCR investigation is inevitable," she counsels.

Resources: Find OCR breach notification guidance at www.hhs.gov/hipaa/for-professionals/breach-notification/index.html and read 45 CFR § 164.400-164.410 for more HIPAA specifics at www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-404.pdf.