Managing the Regulatory Environment

ADA's Guidelines for Practice Success™ (GPS™)

ADA Tip Sheet on the HIPAA Breach Notification Rule

The U. S. Health and Human Services' Breach Notification Rule covers the right of individuals to be notified when their unsecured protected health information (PHI) has been improperly used or disclosed. Notification is not required when electronic PHI is properly secured, which, means it has been properly encrypted.

OCR defines a breach as:

> "the acquisition, access, use or disclosure of protected health information in a manner not permitted under [the Privacy Rule] which compromises the security or privacy of the protected health information." An impermissible acquisition, access, use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
>
> 1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
> 2. The unauthorized person who used the protected health information or to whom the disclosure was made;
> 3. Whether the protected health information was actually acquired or viewed; and
> 4. The extent to which the risk to the protected health information has been mitigated."[1]

OCR outlines three exceptions to the definition of a "breach:"

1. The unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority.
2. The inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
3. In situations where the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information.

Many breaches are the result of theft or loss of laptops and portable storage devices. Proper encryption of electronic protected health information by covered entities and business associates provides a safe harbor from the breach notification rule. According to the agency, from September 2009-February 2015:

- 60% of all large breaches were due to theft or loss
- 32% of all large breaches involved laptops and other portable storage devices
- 22% of all large breaches resulted from the loss of paper records

[1] https://www.hhs.gov/hipaa/for-professionals/breach-notification/

Covered entities must notify affected individuals of a breach of unsecured PHI without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. If applicable state law requires faster notice, the state law time period would apply.

Any breach of unsecured PHI must be reported to OCR; the procedures for reporting a breach are available through the OCR webpage on Submitting Notice of a Breach to the Secretary. Requirements for reporting a breach to OCR vary depending upon the number of individuals affected:

For breaches affecting fewer than 500 individuals, the covered entity:

- must notify the HHS Secretary of the breach within 60 days of the end of the calendar year in which the breach was discovered;
  - is not required to wait until the end of the calendar year to report breaches affecting fewer than 500 individuals
  - may report breaches at the time they are discovered
  - may report all breaches affecting fewer than 500 individuals on one date but must complete a separate notice for each breach incident

For breaches affecting 500 or more individuals, the covered entity:

- must notify the HHS Secretary of the breach without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach
- must also issue a media notice regarding the breach if more than 500 residents of a state or jurisdiction are affected by the breach

☐ How OCR handles breach notifications and complaints:

✓ any notification, regardless of whether it was reported by a covered entity or through an individual complaint, is:

- investigated by an equal opportunity specialist (EOS) who:
  - collects evidentiary information regarding the alleged disclosures
  - applies relevant federal health regulations and laws to the evidence
  - negotiates and oversees corrective action on the part of covered entities
- reviewed by subject matter experts, if warranted
- resolved by recommendations for closure
- closed

✓ enforcement activities may result in:

- voluntary compliance
- a resolution agreement (RA) and Corrective Action plan (CAP)
- civil monetary penalty (CMP) or settlement

☐ Examples of red flags that might be identified by an investigator include:

✓ The inability to prove:

- the existence of written policies and procedures regarding the:
  - Privacy Rule
  - Security Rule
  - Breach Notification Rule
- that risk analysis and risk management plans are in effect and that both plans include appropriate safeguards
- that staff has been trained on policies and procedures
- the existence of compliant and up-to-date business associate agreements
- that removable media, mobile devices and hard drives are properly safeguarded

☐ Here are a few examples of things covered entities must do for HIPAA compliance:
- ✓ Develop policies and procedures to be compliant with the Privacy Rule, the Security Rule and the Breach Notification Rule
  - review and update policies or procedures as necessary
- ✓ Develop a Notice of Privacy Practices (NPP) to be shared with all patients
  - review and update the NPP as needed
- ✓ Train employees on policies and procedures
  - document all training

RESOURCES: HHS Breach Notification Rule
OCR Submitting Notice of a Breach to the Secretary