What is a breach according to HIPAA?

- “Unauthorized acquisition, access, use or disclosure of protected health information (PHI) which compromises the security and privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information” (Section 13400 (1) (A) of the HITECH Act)

- An impermissible use or disclosure of PHI is presumed to be a breach, and breach notification is necessary unless the covered entity (CE) or business associate (BA) demonstrates that there is a low probability the PHI has been compromised or if the PHI was unreadable or undecipherable

- If a breach is suspected, a breach notification risk assessment must be conducted. A risk assessment considers at least the following factors:
  - The nature and extent of the PHI involved, including types of identifiers and likelihood of re-identification
  - The unauthorized person who used the PHI or to whom the disclosure was made
  - Whether the PHI was actually acquired or viewed
  - The extent to which the risk to the PHI has been mitigated; if there is significant risk of harm to the affected individual(s) as a result of the breach, then breach notification(s) are required (164.402)

A breach excludes the following, according to HIPAA:

- Any unintentional acquisition, access or use of the PHI by a workforce member or an individual acting upon the authority of the CE or a BA if this was within the normal scope of his/her authority, and if the PHI is not further used or disclosed

- Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CA or BA, and if the PHI is not further used or disclosed

- A disclosure of PHI where the CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not have reasonably been able to retain such information

- Encryption and destruction are technologies and methods for securing PHI and if PHI is secured through the appropriate encryption or destruction methods are relieved of the notification obligation (164.402)

What are the rules for breach notification?

- Individuals must be notified in writing, via first class mail, without unreasonable delay after the breach is discovered but not later than 60 days after discovery. Contents of written notification must include (Section 13402 (e) (1) of the HITECH Act):
  - A brief description of what happened, including the date of the breach and the date of the discovery of the breach
- A description of the unsecured PHI disclosed in the breach
- Steps the patient should take to protect themselves from harm resulting from the breach
- A brief description of the actions taken by the CE to investigate the breach, mitigate harm to individuals and protect against future breaches
- Provide contact procedures for individuals to ask questions, including a toll-free number, an email address, website or postal address (Section 13042.f.1-5)

- BAs who have access to PHI must notify the CE of a breach, including the name(s) of the individual(s) whose PHI has been compromised
- If the breach affects less than 500 individuals, a log or other documentation of such breaches must be maintained and submitted not later than 60 days after the end of each calendar year and HHS must be notified in the manner specified on the HHS website
- If the breach affects 500 or more individuals, notice must also be provided to major media outlets serving the relevant state or jurisdiction and contain the same information as the written notice not later than 60 days after discovery and the Department of Health and Human Services (HHS) must be notified in the manner specified on the HHS website (Sec. 13402)

### How is a breach violation enforced?

- The Office of Civil Rights (OCR) will investigate each complaint it receives in order to determine whether it can investigate the complaint. OCR must determine whether it has legal authority to investigate, meaning whether the complaint alleges a violation of one or more of the laws OCR enforces; must also determine whether the complaint was filed in a timely manner; and if there is enough information about the alleged violation to proceed with an investigation.
  
  [http://www2.ed.gov/about/offices/list/ocr/complaints-how.html](http://www2.ed.gov/about/offices/list/ocr/complaints-how.html)

- Civil penalties:
  
  A CE or BA may be subject to multiple violations.

- Criminal penalties can result in imprisonment from one year to up to 10 years, depending on the severity of the offense

### VIOLATION | PENALTY | MAX CALENDAR YEAR
--- | --- | ---
Did Not Know | $100–$50,000 | $1,500,000
Reasonable Cause | $1,000–$50,000 | $1,500,000
Willful Neglect (Corrected) | $10,000–$50,000 | $1,500,000
Willful Neglect (Not Corrected) | $50,000 | $1,500,000

For more information about this issue of AFMC HealthIT HIPAAwatch, please visit afmc.org/healthit, email healthit@afmc.org or call 501-212-8616.