HIPAA Breach Notification Rule

HIPAA's Breach Notification Rule requires covered entities to notify patients when their unsecured protected heath information (PHI) is impermissibly used or disclosed—or "breached,"—in a way that compromises the privacy and security of the PHI.

An impermissible use or disclosure of PHI is *presumed* to be a breach unless the covered entity demonstrates that there is a "low probability" that the PHI has been compromised.

A physician must take an active role in evaluating the severity of improper use or disclosure of PHI by assessing whether the use or disclosure meets HIPAA's "low probability of compromise" threshold. To do so, physicians must use a 4-factor test:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of reidentification
2. The unauthorized person (or people) who used the PHI or to whom the disclosure was made
3. Whether the PHI was actually acquired or viewed
4. The extent to which the risk to the PHI has been mitigated

In the absence of an exception or a demonstration of a low probability of compromise, physicians must notify patients and the U.S. Department of Health & Human Services (HHS) in the event of an impermissible use or disclosure of PHI. If, after evaluating whether the PHI has been compromised, a covered entity or business associate reasonably determines that the probability of such compromise is low, breach notification is not required.

Covered entities are under no obligation to perform the entire 4-factor risk assessment if the PHI is obviously compromised. Covered entities may always begin the breach notification process without conducting a formal risk assessment.

Timing

Once a covered entity knows or by reasonable diligence should have known (referred to as the "date of discovery") that a breach of PHI has occurred, the entity has an obligation to notify the relevant parties (individuals, HHS and/or the media) "without unreasonable delay" or up to 60 calendar days

following the date of discovery, even if upon discovery the entity was unsure as to whether PHI had been compromised.

Parties to notify

If the breach involves the unsecured PHI of more than 500 individuals, a covered entity must notify a prominent media outlet serving the state or jurisdiction in which the breach occurred, in addition to notifying HHS. For breaches involving fewer than 500 individuals, covered entities are permitted to maintain a log of the relevant information and notify HHS within 60 days after the end of the calendar year via the HHS website.

Encryption safe harbor

HIPAA only requires breach notification for unsecured PHI (e.g., unencrypted PHI). As such, physicians are encouraged to use appropriate encryption and destruction techniques for PHI, which render PHI unusable, unreadable or indecipherable to unauthorized individuals.

- PHI techniques
- AMA EdHub™: The nuts and bolts of achieving HIPAA security rule compliance through effective risk assessment
- HHS guidance on the Breach Notification Rule
- HHS breach notification portal
- HHS privacy and security toolkit
- HHS Office of the National Coordinator for Health IT (ONC) guide to privacy and security of health information (PDF)
- Submitting notice of a breach to the secretary
- HIPAA privacy and security toolkit: Helping your practice meet compliance requirements (PDF)

This resource is provided for informational and reference purposes only and should not be construed as the legal advice of the American Medical Association. Specific legal questions regarding this information should be addressed by one's own counsel.