HIPAA Health Insurance Portability and Accountability Act

Breach Reporting Decision Tree

Potential Breach Incident

Did the incident involve one or more of the 18 identifiers considered PHI?

NO → **No federal or state notification Required**

YES

Did the incident involve unsecured/ unencrypted PHI?

NO → **No federal or state notification Required**

YES

Does the event qualify as one of the following exceptions?

1. Good faith, unintentional acquisition, access or use of PHI by staff?
2. Inadvertent disclosure to another authorized person within the Covered Entity ?
3. Recipient could not reasonably have retained the event data.

YES → **No federal or state notification Required**

NO

Is there a low probability that the PHI has been compromised based on a risk assessment of at least the following factors :

1. Nature and extent of PHI included, identifiers and likelihood of re-identification
2. Identity of the unauthorized person or to whom impermissible disclosure was made
3. Whether PHI was actually viewed or only the opportunity to do so existed
4. The extent to which the risk has been mitigated.

YES → **No federal or state notification Required**

NO

Reportable Event Has Occurred!

Notify Individuals and Necessary Government Agencies using Breach Reporting Protocol. If 500 or more individuals are affected HHS and prominent media outlets must be notified.

The following 18 identifiers are considered Protected Health Information (PHI)

1. Names;
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes;
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images;
18. Any other unique identifying number, characteristic, or code.

Examples of Unsecured and Unencrypted PHI

1. A nurse mistakenly faxes medical records to a wrong number.
2. A pharmacist gave the wrong prescription to a patient.
3. A staff member sends an unencrypted email containing patient information to the wrong email account.
4. A doctor reports a stolen laptop that was password-protected, but not encrypted. Records including personal information about patients: names, medical record numbers, and health treatment were on the laptop. The laptop was stored overnight in an employee's car, which was parked in front of her house.
5. A manager lost an unencrypted USB thumb drive containing patient information including patient names, medical record number, birthday, blood type, blood test results, brief medical history, and physician's name.