About the HIPAA Privacy Breach Notification Rule…

If there is a breach of unsecured protected health information (PHI), the HIPAA Breach Notification Rule requires HIPAA covered entities and business associates to provide notification. Similar breach notification provisions enforced by the Federal Trade Commission (FTC) apply to vendors of personal health records and their third-party service providers, pursuant to the HITECH Act.

How Is a Breach Defined?

Generally, a breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that PHI has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the protected health information or to whom the disclosure was made.
- Whether the protected health information was actually acquired or viewed.
- The extent to which the risk to the protected health information has been mitigated.

PRACTICAL POINTER:

There are a few instances that are exceptions to the breach definition, including access by workforce members done unintentionally and in good faith. Additionally, notification is required only if the breach involved unsecured PHI.

Breach Notification Checklist:

Following a breach of unsecured PHI, covered entities must provide notification to the affected individuals, the Secretary of Health and Human Services, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

Individual Notice. Covered entities must provide affected individuals:

- ☐ Written notice by first-class mail or by e-mail if the affected individual has agreed to receive such notices electronically.
- ☐ Individual notifications without unreasonable delay and in no case later than 60 days following the discovery of a breach.
- ☐ A notification that includes:
  - ☐ a brief description of the breach,
  - ☐ a description of the types of information that were involved in the breach,
  - ☐ the steps affected individuals should take to protect themselves from potential harm,
  - ☐ a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as
  - ☐ contact information for the covered entity (or business associate, as applicable).

Media Notice. In addition to notifying the affected individuals, covered entities that experience a breach affecting more than 500 residents of a state or jurisdiction are required to:

- ☐ Provide notice to prominent area media outlets, usually in the form of a press release.
- ☐ Provide notice without unreasonable delay and in no case later than 60 days following the discovery of a breach.
- ☐ Include the same information required for the individual notice.

Notice to Secretary.

If a breach affects **500 or more individuals**, covered entities must:

- ☐ Notify the Secretary without unreasonable delay and in no case later than 60 days following a breach.

If a breach affects **fewer than 500 individuals**, the covered entity may:

- ☐ Notify the Secretary of such breaches on an annual basis.

NOTE: Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.

Notification by a Business Associate.

If a breach of unsecured PHI occurs at or by a business associate, the business associate must:

- ☐ Notify the covered entity following the discovery of the breach.
- ☐ Provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach.

To the extent possible, the business associate should:

- ☐ Provide the covered entity with the identification of each individual affected by the breach.
- ☐ Provide any other available information that will be required for the covered entity in its notification to the affected individuals.

Administrative Requirements and Burden of Proof

Covered entities and business associates have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured PHI did not constitute a breach. Additionally, covered entities must address breach notification via:

- policies and procedures;
- training; and
- sanctions against workforce members who do not comply with the organization's policies and procedures.

The Breach Notification process may be documented in a manner such as the following:

Complaints/ Reports

- Establish a process for individuals and workforce members to report
- Receive reports/complaints and should be immediately reviewed by the Privacy Officer

Detection

- Document the first known date of the incident and identify all records that potentially were affected
- Document the scope of the incident, and what measures were taken to stop the unallowable disclosure

Assessment

- Privacy Office will lead the investigation/assessment of the incident
- Determine if the disclosure constituted a breach; if so, was there any harm or losses to the individual

Mitigation

- What steps were taken to reduce and stop the unlawful disclsure of PHI as a result of this incident
- What steps are being taken to ensure that this will not re-occur; have any staff been sanctioned

Notification

- Determine if a breach notification is required according to the Rule—either to individuals, the media, or HHS—must be submitted electronically
- Document all breach notifications and the dates sent; determine if any further action is needed

About BlueOrange Compliance:

BlueOrange Compliance specializes in assisting healthcare organizations navigate HIPAA and HITECH privacy and security requirements. Complex, ever-changing healthcare regulations and increasing risks make it difficult for organizations to stay in front of emerging cyber threats. As a single source, we equip every client with affordable, practical, comprehensive privacy and security solutions, including multiple sources of information to help manage risk. Our clients have peace of mind knowing they are compliant and prepared for potential breaches and adverse audits.