Meeting HIPAA Third-Party Risk Requirements

By: Christine Kitamura on June 25 2024

5 min read

Certain industries, like finance and healthcare, are at a higher risk of data breaches because they deal with vast amounts of sensitive information. While the finance industry has its own standards for protecting consumer data, healthcare organizations must follow expectations outlined in the **Health Insurance Portability and Accountability Act (HIPAA)**.

This comprehensive regulation is composed of the Privacy Rule and Security Rule, which are designed to safeguard protected health information (PHI) in both physical and electronic forms. HIPAA guidelines are applicable to many types of healthcare organizations and their business associates, or third-party vendors, that have access to a patient's PHI.

This blog will provide a high-level overview of HIPAA's standards for PHI and business associates, as well as the regulation's breach notification requirements. We'll explain how you can use your third-party risk management (TPRM) program to meet these compliance requirements with your business associates.

Note: Regulatory text is noted in *italics*.

HIPAA Requirements for Business Associates and Third-Party Relationships

Covered entities under HIPAA and their business associates must be able to protect sensitive patient health information. Covered entities include healthcare providers, health plans, and healthcare clearinghouses.

The Privacy Rule sets limits on how entities are allowed to use and disclose PHI without the individual's authorization. It also protects an individual's right to gain access to their PHI and authorize how it's used.

The Security Rule outlines administrative, physical, and technical safeguards that should be applied to electronic PHI. The rule further lists requirements related to business associate contracts and policies and procedures.

Healthcare organizations must meet many HIPAA requirements related to third parties, which includes:

- **Have a policy and procedure** to *identify and respond to suspected or known security incidents* and mitigate the *effects of security incidents that are known to the covered entity or business associate*.
- **Identify any *vulnerabilities*** *to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate*.
- **Receive assurances** *that the business associate will appropriately safeguard electronic PHI*.
- **Develop contracts** with their business associates to ensure they *appropriately safeguard the information* and report *to the covered entity any security incident of which it becomes aware*.
- **Remain aware** of *environmental or operational changes affecting the security of the electronic protected health information*.

Meeting HIPAA Requirements With Third-Party Risk Management

As a rule, organizations and their business associates must ensure the *confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits*.

The following third-party risk management elements can be used to ensure HIPAA compliance:

- **Policies and procedures** – It's important to have documentation on how your organization will identify and respond to a third-party security incident. Governance documents, such as a **third-party risk management policy**, program, and procedures will help communicate your organization's objectives, roles, and responsibilities when an incident occurs.

  These governance documents should also describe how your organization will **mitigate third-party security risk** and keep records of any incidents and their outcomes. Policies should be reviewed and approved at least annually by the board of directors or senior management.

- **Vendor risk assessments** – Healthcare organizations should **perform a comprehensive risk assessment** on any business associate that has access to PHI. These assessments should first be completed during the onboarding stage of the **third-party risk management lifecycle** before the contract is signed and address risk domains such as compliance, cybersecurity, privacy, financial, and

reputation. Some organizations may choose to develop vendor questionnaires using frameworks, such as NIST 800-53 rev 5 or HITRUST CSF, which will provide further insight into the business associate's data protection controls.

Pro Tip: Business associates that have HITRUST r2 Certification can provide a copy of their full HITRUST report rather than completing an assessment questionnaire.

- Due diligence – Pre-contract due diligence is another activity that can help meet HIPAA compliance. This process involves collecting and reviewing relevant documentation from the business associate, such as business continuity and disaster recovery (BC/DR) plans, data retention and destruction policies, and vulnerability and penetration testing results.

  Incident response plans should also be evaluated to ensure the business associate can effectively detect, respond to, and resolve a cybersecurity event. Due diligence reviews should always be performed by a qualified subject matter expert (SME) who can provide an opinion on whether the business associate has sufficient controls in place.

- **Contracting** – Business associate contracts and agreements are another focal point of HIPAA, which outlines a few specific requirements related to safeguarding information, subcontractors, and reporting security incidents. Healthcare organizations should collaborate with their legal teams to thoroughly review and negotiate their contracts to ensure compliance with HIPAA requirements. Contracts should also ensure any subcontractors, or fourth parties, who have access to PHI are required to comply with the same security standards.

- **Periodic assessments and due diligence** – Periodic risk re-assessments help meet compliance expectations by keeping your organization aware of the current risk environment that may have changed since you signed the contract. For instance, a business associate may have implemented a new software system or experienced a security incident which requires a new round of vulnerability testing. Periodic due diligence reviews are also needed to ensure you have the most current documentation on file, such as SOC reports or insurance certificates, both of which can become outdated.

HIPAA Breach Notification Rule Requirements for Third Parties

HIPAA requires organizations to notify individuals or any data breaches that have impacted their PHI. These requirements apply even if the breach was caused by a third-party vendor.

Here are 4 details to consider in HIPAA's third-party data breach notification requirements:

1. **Timing** – Your vendor should notify your organization of a security incident no later than 60 days after discovery and include the date of the incident.
2. **Impact** – The notification should identify each individual who was impacted in the breach and the types of PHI that were involved.
3. **Response** – After an incident is discovered, your vendor should explain how they're investigating the breach and how they're protecting against further incidents.
4. **Next steps** – Data breaches can be stressful and filled with uncertainty, so it helps to understand any next steps that the impacted individuals can take to mitigate harm. This can also include contact information for the individuals to learn more about the situation.

Safeguarding PHI is an ongoing challenge, but implementing these third-party risk management practices is an effective strategy that will help your organization and third parties maintain HIPAA compliance.