Prevalent™

A Checklist for Compliance

HIPAA and Third-Party Risk Management

Table of Contents

HIPAA and Third-Party Risk Management

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was established to ensure that sensitive protected health information (PHI) would not be disclosed without the patient's consent. HIPAA includes a Security Rule that establishes safeguards for organizations holding electronically stored protected health information PHI (ePHI), as well as a Privacy Rule that sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.

HIPAA regulations are most closely aligned with "covered entities" such as health plans, health care clearinghouses, and some health care providers. However, it also applies to "business associates" — third-party vendors that have access to PHI. Business associates include vendors such as claims processors, consultants, medical transcriptionists, pharmacy benefits managers. They also include clinical trial organizations, cloud service providers, and managed services providers. Given that the average hospital has over 1,300 vendors, this dramatically expands the number of organizations that must comply with HIPAA requirements – and the number of third parties that providers must assess.

Almost all businesses are also subject to HIPAA. While employers don't typically provide healthcare, they do handle documentation related to group health insurance and medical records employees authorize their doctors to provide to the company for specific purposes (e.g., excused abscesses, Family Medical Leave (FML) documentation, or disability accommodation requests).

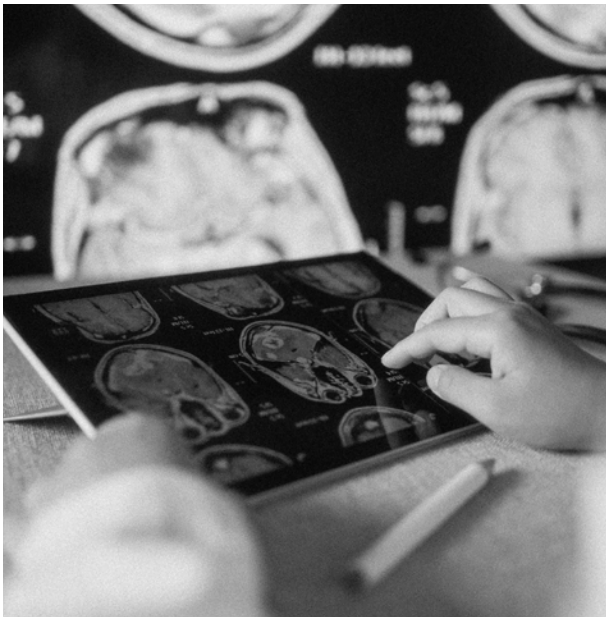
Risk Analysis is a Requirement

Organizations must be aware of risks to critical information both within their own entity and with third parties that have access to ePHI. HIPAA makes this a requirement, and extends the term "organization" to covered entities and business associates. Section 164.308(a)(1)(ii)(A) states:

> ***RISK ANALYSIS (Required)****. Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization].*

Evaluating a vendor's readiness to comply with the covered entity's security expectations is achieved through a vendor risk assessment. The costs of not complying with a thorough risk assessment are well documented:

- Excellus Health Plan agreed to a $5.1 million settlement for violation of HIPAA rules including, "failure to conduct an enterprise-wide risk analysis, and failures to implement risk management, information system activity review, and access controls."
- In 2020 Premera Blue Cross was fined $6.85 million for HIPAA violations, including failure to conduct an enterprise-wide risk analysis. In addition, Premera settled a class-action lawsuit for $74 million and a suit with 30 states totaling $10 million.
- California-based Cottage Health had a $4 million cyber insurance claim denied and later paid a $3 million HIPAA settlement when their IT vendor exposed information on over 32,000 patients.
- Touchstone Medical Imaging, a diagnostic medical imaging services company, also agreed to a $3 million settlement after it was found to maintain an unprotected FTP server – accessible over the Internet – and allowed anonymous connections to a shared directory.
- CardioNet, a provider of remote mobile monitoring and rapid response services, was fined $2.5 million after Office of Civil Rights (OCR) investigators determined that they, "failed to conduct an accurate and thorough risk analysis to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI and failed to plan for and implement security measures sufficient to reduce those risks and vulnerabilities.



Checklist for Meeting HIPAA Security Rule Third-Party Risk Management Requirements

Healthcare and related organizations must ensure that business associates and other third parties have the security and privacy controls in place to prevent unwanted access that impacts the confidentiality, integrity or available of ePHI. To achieve this, companies should conduct thorough vendor risks assessments. The table below summarizes specific Security Rule requirements and provides guidance* on suggested capabilities.

***Note:** This guidance should not be used in place of official audit or legal recommendations.*

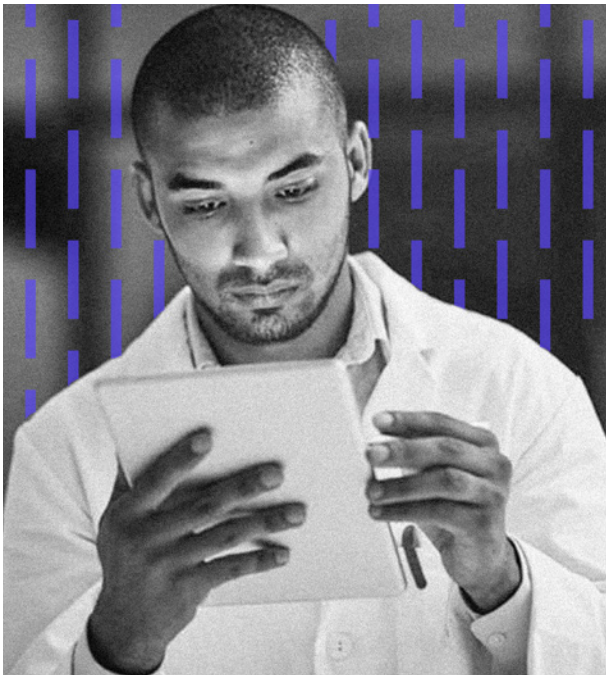
HIPAA Security Rule 45 CFR Parts 160, 162, and 164 – Health Insurance Reform: Security Standards; Final Rule	What it Means to Organizations
Security Management Process Administrative Safeguards (§ 164.308(a)(1)) (A) Risk analysis (REQUIRED) "A covered entity or business associate must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate."	The first step in complying with HIPAA regulations is a comprehensive risk assessment – both internally and of third parties that may have access to PHI. While some organizations attempt this with spreadsheet-based questionnaires, that approach does not scale. Prevalent offers security, privacy, and risk management professionals a platform to automate the third-party risk assessment, scoring, and remediation process and determine compliance with IT security, regulatory, and data privacy requirements. Prevalent provides a library of over 75 standardized assessment templates – including for HIPAA and the Health Information Sharing and Analysis Center (H-ISAC) – customization capabilities, and built-in workflow and remediation guidance. In addition, the Prevalent Healthcare Vendor Network simplifies and accelerates the due diligence process, providing an on-demand library of thousands of completed healthcare vendor risk reports based on the H-ISAC questionnaire, which are continuously updated and backed by supporting evidence.
Security Management Process Administrative Safeguards (§ 164.308(a)(1)) (B) Risk management (REQUIRED) "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [HIPAA Security Standards]."	Once risks are identified, organizations must implement controls to minimize risk. Once assessments are collected and analyzed, the Prevalent TPRM Platform offers built-in remediation recommendations and guidance. With clear reporting and remediation guidance, the platform ensures that risks are identified, analyzed, and escalated to the proper channels so that your organization achieves a risk level appropriate to its risk appetite.

HIPAA Security Rule 45 CFR Parts 160, 162, and 164 – Health Insurance Reform: Security Standards; Final Rule	What it Means to Organizations
Security Management Process Administrative Safeguards 164.308(a)(1)) (D) Information system activity review (REQUIRED) "Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."	Since a lot can change between annual assessments, organizations should perform continuous monitoring of risks, contract performance and service level agreements (SLAs). Prevalent delivers a continuous view of risks through Internet and Dark Web threat monitoring feeds, as well as business and financial risk analysis, to reveal developments that could impact risks. The Prevalent Platform also enables comprehensive reviews with a dedicated and custom contract assessment questionnaire, plus continuously tracked performance metrics via centralized vendor dashboards. Prevalent maintains a complete repository of all documentation collected and reviewed during the diligence process, with specific regulatory compliance and security framework reporting.
Business associate contracts and other arrangements. § 164.308(b)(1) "A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor."	Business associate contracts are required, but smart compliance and security teams will require evidence of compliance and controls. Prevalent's assessment capabilities simplify compliance and reduce risk with automated collection, analysis, and remediation of vendor responses using industry-standard or custom surveys – including those measuring information safeguards. Although not required, Prevalent provides visibility into 4th and Nth parties (e.g., subcontractors) with detailed relationship mapping, providing audit trails of flows of information throughout a supplier ecosystem.

HIPAA Security Rule 45 CFR Parts 160, 162, and 164 – Health Insurance Reform: Security Standards; Final Rule	What it Means to Organizations
Security Management Process, Administrative Safeguards § 164.308(a)(6) Implementation specification: Response and reporting (REQUIRED) "Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes."	Some vendors may not know when they have been breached, or may not promptly report incidents which can delay Mean Time to Discovery (MTTD) and Mean Time to Resolution (MTTR), opening an organization up to potential exploits. Prevalent Vendor Threat Monitor (VTM) monitors the Internet and Dark Web for cyber threats and vulnerabilities – as well as public and private sources of reputational, sanctions, and financial information – providing real-time visibility into risks and enabling risk management and security teams to act immediately. The Prevalent Third-Party Incident Response Service enables organizations to rapidly identify and mitigate the impact of third-party breaches by centrally managing vendors, conducting event assessments, scoring identified risks, and accessing remediation guidance.
Security Management Process, Administrative Safeguards § 164.308(a)(8) "Standard: Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart."	All organizations experience personnel changes and periodically implement new policies and procedures. Covered entities must continuously monitor cyber, business, and financial intelligence for visibility into material changes to a vendor's risk profile between annual internal control assessments. Prevalent Vendor Threat Monitor alerts organizations to adverse changes in third parties' businesses and triggers targeted assessments to address interim immediate risks. Early alerts enable more time to respond to incidents and built-in remediation guidance helps organizations protect PHI and avoid OCR actions and reputational damage. Some changes, like the COVID-19 pandemic, forced fundamental changes in how businesses operate. Prevalent's assessment questionnaires include questions designed to reveal internal business continuity gaps and external supply chain weaknesses that could negatively impact an organization's ability to maintain control over sensitive PHI or prompt one to consider alternate vendors.

HIPAA Security Rule 45 CFR Parts 160, 162, and 164 – Health Insurance Reform: Security Standards; Final Rule	What it Means to Organizations
Policies and procedures and documentation requirements § 164.316(b)(1) "Standard: Documentation • (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and • (ii) If an action, activity, or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment."	In the event of an incident or audit, or in the course of a business relationship, organizations are required to produce evidence supporting policies, identified risks, and controls. The Prevalent TPRM Platform includes contract, document, evidence and certifications management with built-in version controls, task assignment, and auto-review cadences in centralized vendor profiles. In addition, Prevalent captures and audits conversations and matches documentation or evidence against risks. Intuitive and straightforward dashboards provide a clear overview of tasks, schedules, risk activities, survey completion status, agreements, and associated documents.

How Prevalent Helps Address HIPAA TPRM Requirements



Complying with HIPAA requires a complete internal and external view of the controls in place for all business associates. Managing this process efficiently across hundreds of third parties with manual spreadsheets is impossible**.**

At a basic level, organizations should:

- Automate business associate vendor onboarding and offboarding to ensure consistent processes
- Profile, tier and score inherent risk to guide full risk assessment decisions
- Assess business associates against standardized content that simplifies regulatory and standards mapping
- Centralize all business associate documentation, including contract, reporting and evidence
- Perform continuous monitoring of cybersecurity, business/reputational and financial information to correlate risks against assessment results
- Report regularly against SLAs, performance and compliance using standardized, pre-built templates
- Leverage best practices guidance to guide remediation decisions according to organizational risk appetite

The Prevalent Third-Party Risk Management Platform can help ensure the security of PHI in compliance with the HIPAA regulations. This cloud-based platform combines automated, standardized vendor risk assessment with continuous vendor risk monitoring, assessment workflow, and remediation management across the entire vendor lifecycle. The platform is complemented by vendor intelligence networks offering on-demand access to completed, standardized risk reports on thousands of companies. All Prevalent solutions are backed by expert professional services and managed vendor risk assessment services to help you optimize and mature your TPRM program.

Contact Prevalent today for a free maturity assessment to determine how your TPRM policies stack up to the HIPAA requirements.

About Prevalent

Prevalent takes the pain out of third-party risk management (TPRM). Companies use our software and services to eliminate the security and compliance exposures that come from working with vendors, suppliers and other third parties across the entire vendor lifecycle. Our customers benefit from a flexible, hybrid approach to TPRM, where they not only gain solutions tailored to their needs, but also realize a rapid return on investment. Regardless of where they start, we help our customers stop the pain, make informed decisions, and adapt and mature their TPRM programs over time.

To learn more, please visit www.prevalent.net.