HIPAA: Securing Electronic Protected Health Information

The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. federal law established to protect sensitive patient health information. If a company provides medical services in the U.S. or works in partnership with U.S. medical providers, compliance with HIPAA recommendations is mandatory. The framework aims to secure electronic protected health information (e-PHI).

Pentesting as a Security and Risk Analysis Tool

The HIPAA Security Rule requires organizations to implement security measures that are "reasonable and appropriate" for their specific entity. While this language historically allowed for considerable discretion, penetration testing fulfills essential components of the rule.

- **Risk analysis and assessment:** HIPAA requires a risk analysis that includes evaluating the likelihood and impact of potential risks and reviewing and considering threats and vulnerabilities experienced in the last 12 months. Pentesting provides an in-depth review of discovered vulnerabilities and helps organizations document their approach to assessing and addressing the risk posed by exploitable vulnerabilities.
- **Periodic assessment:** Pentesting can fulfill the requirement for a periodic assessment of whether security policies meet the rule's requirements, providing a thorough analysis from an impartial third party.
- **Scope:** Security controls should focus specifically on defending electronic protected health information.

Stricter Requirements Going Into Effect in 2026

Recent proposed updates to HIPAA security regulations are tightening security guidelines and clarifying that all security guidelines are mandatory. Although the proposed changes are not final as of Q4 2025, it is likely they will not change significantly before final implementation sometime in 2026. These changes integrate the concept of Cybersecurity Performance Goals (CPGs) into the regulatory framework.

The enhanced goals include establishing pentesting and attack simulation processes. Most notably, the proposed security rule would explicitly require organizations to implement semi-annual vulnerability scanning and annual pentesting.

These new requirements underscore the transformation of pentesting from a highly recommended practice to a mandatory, auditable control for organizations handling e-PHI. By proactively protecting against breaches involving e-PHI, through a rigorous security testing program, organizations minimize HIPAA compliance risk and ensure patient trust.

See how Cobalt helps a healthtech provider comply with HIPAA

READ CASE STUDY

About Cobalt

Cobalt is the pioneer in pentesting as a service (PTaaS) and a leader in offensive security services.

We are focused on combining talent and technology with speed, scalability, and expertise. Thousands of customers and hundreds of partners rely on the Cobalt Offensive Security Platform, along with the industry's largest exclusive community of 450+ trusted pentesters and security experts, to find and fix vulnerabilities across their environments. By enabling faster pentest launches, real-time collaboration with testers, continuous scanning, and seamless integration with remediation workflows, we help organizations identify critical issues and accelerate risk mitigation so they can operate fearlessly and innovate securely.

Book a demo to see how Cobalt can help you achieve compliance and build your offensive security program.

BOOK A DEMO