HIPAA Security Rule

Pentesting Requirements

A practical guide for healthcare IT leaders, security teams, covered entities, and business associates navigating HIPAA Security Rule compliance - with specific 45 CFR control references and 2024 NPRM updates.

Contents

01 Quick Summary

WHAT HEALTHCARE SECURITY TEAMS NEED TO KNOW

HIPAA's Security Rule does not use the words 'penetration testing' - but it absolutely requires it in practice. The rule mandates risk analysis, safeguard evaluation, and ongoing technical assessments that the healthcare industry, OCR auditors, and the HHS NPRM (2024) all treat penetration testing as the primary method to satisfy. Here is the simplified version:

AT A GLANCE

- Penetration testing satisfies §164.308(a)(8) Evaluation - the most direct compliance hook.
- The 2024 NPRM proposes making annual penetration testing and semi-annual vulnerability scanning explicitly mandatory.
- Both covered entities and business associates (BAs) must have security controls tested.
- ePHI systems - applications, databases, APIs, networks, cloud - are all in scope.
- Password hygiene, access management, encryption, network segmentation, and audit controls all map to specific HIPAA CFR references.
- Vulnerability scanning alone does not satisfy the evaluation requirement.
- Pentesters must sign a Business Associate Agreement (BAA) before testing can begin.
- Healthcare is the most expensive industry for data breaches - $7.42M average per incident in 2025 (IBM).

02 What Is HIPAA and Who Does It Cover?

BACKGROUND AND CONTEXT

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes national standards for protecting individually identifiable health information. The Security Rule (45 CFR Part 164, Subpart C) specifically governs electronic protected health information (ePHI) and applies to:

Entity Type	Examples
Covered Entities (CEs)	Hospitals, clinics, physician practices, health insurers, health plans, healthcare clearinghouses
Business Associates (BAs)	SaaS vendors processing ePHI, billing services, EHR providers, cloud hosting services, IT managed service providers
Subcontractors of BAs	Any downstream vendor receiving ePHI from a BA - subject to same Security Rule obligations
Hybrid Entities	Organizations with both healthcare and non-healthcare functions - must designate healthcare components

Key Terms

Term	Plain English Meaning
ePHI	Electronic Protected Health Information - any individually identifiable health information in electronic form.
Covered Entity (CE)	A healthcare provider, health plan, or clearinghouse subject to HIPAA.
Business Associate (BA)	A vendor or contractor who creates, receives, maintains, or transmits ePHI on behalf of a CE.
BAA	Business Associate Agreement - required contract before any vendor can access ePHI, including pentesters.
OCR	Office for Civil Rights - the HHS division that enforces HIPAA. Conducts investigations, audits, and levies fines.
NPRM	Notice of Proposed Rulemaking - the Dec. 2024 HHS proposal to significantly update the Security Rule.
Required	Implementation specifications that must be implemented. No substitution permitted.
Addressable	Implementation specifications requiring a risk-based decision to implement or document an equivalent alternative. Under NPRM, this distinction may be eliminated.
Risk Analysis	§164.308(a)(1)(ii)(A) - mandatory assessment identifying threats, vulnerabilities, and risks to ePHI.

03 The Three Safeguard Categories

HOW HIPAA ORGANISES SECURITY REQUIREMENTS

The HIPAA Security Rule organizes all controls into three safeguard categories, supported by organizational and documentation requirements. Penetration testing touches all three, with the strongest hooks in Administrative and Technical safeguards.

Category	CFR Reference	What It Covers
Administrative Safeguards	45 CFR §164.308	Risk analysis, workforce security, access management, security training, incident procedures, contingency planning, and evaluation (§164.308(a)(8) - the primary pentest hook).
Physical Safeguards	45 CFR §164.310	Facility access controls, workstation use and security, device and media controls. Physical testing sometimes included in comprehensive HIPAA assessments.
Technical Safeguards	45 CFR §164.312	Access control, audit controls, integrity controls, authentication, and transmission security. The technical layer directly validated by penetration testing.

Organizational Requirements	45 CFR §164.314	Business Associate Agreements, group health plan requirements. BAs must also comply - pentesters must sign BAAs.
Policies and Documentation	45 CFR §164.316	Documentation of all security decisions, policies, and procedures. Pentest reports are key documentation artifacts.

THE SHIFT: REQUIRED vs. ADDRESSABLE

Under the current Security Rule, some specifications are 'Addressable' - meaning covered entities can implement an equivalent alternative with documented rationale. The 2024 NPRM proposes eliminating this distinction, making all specifications mandatory with only limited exceptions. In practice: encryption, MFA, network segmentation, vulnerability scanning, and annual penetration testing would shift from risk-based decisions to universal requirements.

04 Required Controls and Pentest Mapping

45 CFR REFERENCES WITH SECURITY TESTING RELEVANCE

The controls below are drawn directly from 45 CFR Part 164. Each maps to specific security testing activities. The CFR does not use the word 'penetration testing' explicitly, but §164.308(a)(8) Evaluation is the primary regulatory hook - and OCR enforcement actions consistently cite inadequate technical evaluation as a basis for findings.

Administrative Safeguards - 45 CFR §164.308

CFR Reference	Standard / Specification	Pentest Relevance
§164.308(a)(1)(ii)(A)	Risk Analysis (Required)	Penetration testing directly informs risk analysis - it identifies exploitable vulnerabilities, validates threat vectors, and quantifies actual risk to ePHI. Risk analysis without pentest evidence is considered theoretical by OCR.
§164.308(a)(1)(ii)(B)	Risk Management (Required)	Pentest findings drive the risk management remediation plan. The test-remediate-retest cycle is the operational core of HIPAA risk management.
§164.308(a)(1)(ii)(D)	Information System Activity Review (Required)	Pentest validates that audit log monitoring is working. If a pentest generates no alerts in your SIEM, that is a direct finding under this specification.
§164.308(a)(4)	Information Access Management	Access control testing - privilege escalation, orphaned accounts, least privilege violations - validates that access management controls actually restrict unauthorized access to ePHI.
§164.308(a)(5)(ii)(B)	Protection from Malicious Software (Addressable)	Payload delivery simulation during pentesting validates AV, EDR, and endpoint defenses against malicious software targeting ePHI systems.

§164.308(a)(6)(ii)	Response and Reporting (Required)	Pentest exercises validate that incident response procedures activate correctly when ePHI systems are attacked. Tabletop exercises paired with pentesting address this.
§164.308(a)(8)	Evaluation (Required)	THE PRIMARY PENTEST CONTROL. Requires periodic technical and non-technical evaluation of security policies to ensure ongoing protection of ePHI. OCR and HHS treat penetration testing as the gold standard for satisfying this requirement.

§164.308(a)(8) - EVALUATION: THE CORE PENTEST HOOK

The HIPAA Security Rule states: 'Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of ePHI, that establishes the extent to which an entity's security policies and procedures meet the requirements.' OCR has confirmed in guidance that technical evaluations should include penetration testing. This is the regulation that security auditors point to when asking for pentest evidence during HIPAA compliance reviews.

Technical Safeguards - 45 CFR §164.312

Technical safeguards are the most directly tested category. Every specification below maps to specific penetration testing techniques.

CFR Reference	Standard / Specification	Pentest Relevance
§164.312(a)(1)	Access Control (Required)	The core technical access control standard. Penetration testing validates: authentication bypass, session hijacking, unauthorized access paths, API access control, and ePHI system boundary enforcement.
§164.312(a)(2)(i)	Unique User Identification (Required)	Tests validate that shared accounts, generic credentials, and service accounts are identified and restricted. Credential reuse and shared account testing directly address this.
§164.312(a)(2)(iii)	Automatic Logoff (Addressable)	Session management testing validates that inactive sessions terminate correctly and cannot be hijacked after timeout.
§164.312(a)(2)(iv)	Encryption and Decryption (Addressable, proposed Required)	Encryption testing validates TLS configuration, cipher suite strength, certificate validity, and absence of cleartext ePHI transmission. Under NPRM, this becomes mandatory.
§164.312(b)	Audit Controls (Required)	Pentest validates that audit logging captures all access to ePHI, cannot be bypassed, and that logs are protected from tampering. Log injection and log bypass testing is in scope.
§164.312(c)(1)	Integrity (Required)	Testing validates that ePHI cannot be altered or destroyed without authorization - tests include unauthorized modification attempts, database manipulation, and file integrity bypass.

§164.312(d)	Authentication (Required)	Authentication testing covers: MFA bypass, password policy validation, brute force protections, SSO weaknesses, and API authentication mechanisms.
§164.312(e)(1)	Transmission Security (Required)	Tests validate that ePHI in transit is protected - TLS validation, man-in-the-middle testing, API transport security, and VPN security are in scope.
§164.312(e)(2)(ii)	Encryption of ePHI in Transit (Addressable, proposed Required)	Specific testing for encryption of ePHI during transmission - validates no cleartext PHI passes over unencrypted channels, including internal network traffic.

Physical Safeguards - 45 CFR §164.310

Physical safeguards are less commonly included in standard HIPAA pentests but are relevant for on-premises healthcare environments.

CFR Reference	Standard / Specification	Pentest Relevance
§164.310(a)(1)	Facility Access Controls (Required)	Physical penetration testing validates that unauthorized individuals cannot access server rooms, workstations, or medical devices containing ePHI. Badge cloning, tailgating, and physical bypass testing.
§164.310(b)	Workstation Use (Required)	Workstation security testing validates endpoint controls - screen lock enforcement, USB restrictions, and authorized software controls.
§164.310(d)(1)	Device and Media Controls (Required)	Testing validates that removable media controls prevent unauthorized data exfiltration from devices containing ePHI.

05 Highlighted Control Areas

SECURITY TOPICS WITH SPECIFIC CFR MAPPINGS

The following areas represent the most scrutinized controls in HIPAA OCR audits and enforcement actions. Each maps to specific CFR references and includes testing guidance.

Password Hygiene and Credential Security

RELEVANT CONTROLS: §164.308(a)(5)(ii)(D), §164.312(a)(2)(i), §164.312(d)

§164.308(a)(5)(ii)(D) requires procedures for creating, changing, and safeguarding passwords (Addressable). §164.312(a)(2)(i) requires unique user identification (Required). §164.312(d) requires authentication controls. Password hygiene failures appear in nearly every major HIPAA breach. Penetration testing validates that policies are enforced in practice - not just documented.

Testing Area	CFR Reference

Password complexity enforcement and lockout policies	§164.308(a)(5)(ii)(D), §164.312(d)
Default credentials on medical devices and systems	§164.312(a)(2)(i) - unique identification required
Credential stuffing and brute force resistance	§164.312(d) - authentication controls
MFA bypass and authentication weakness testing	§164.312(d) - (MFA mandatory under proposed NPRM)
Service account and shared account validation	§164.312(a)(2)(i) - unique user identification required
Password reset and credential recovery workflows	§164.308(a)(5)(ii)(D) - safeguarding passwords

Access Management

RELEVANT CONTROLS: §164.308(a)(4), §164.312(a)(1), §164.312(a)(2)

Information access management (§164.308(a)(4)) and technical access control (§164.312(a)(1)) together govern who can access ePHI and under what conditions. These are among the most frequently cited controls in OCR enforcement actions and breach investigations. Access control testing validates that the principle of least privilege is enforced in practice - not just stated in policy. Privilege escalation and horizontal access bypass are priority test techniques.

Testing Area	CFR Reference
Role-based access control and least privilege enforcement	§164.308(a)(4), §164.312(a)(1)
Privilege escalation (vertical and horizontal)	§164.312(a)(1) - access only to authorized persons
Broken object-level authorization (BOLA/IDOR) in EHR/APIs	§164.312(a)(1) - technical access control
Orphaned accounts and terminated employee access	§164.308(a)(3)(ii)(C) - workforce clearance procedures
Admin interface exposure and hardening	§164.312(a)(1), §164.308(a)(4)
Third-party vendor access validation	§164.308(a)(4), §164.314 - BA access controls

Encryption

RELEVANT CONTROLS: §164.312(a)(2)(iv), §164.312(e)(2)(ii), §164.312(e)(1)

Currently Addressable, encryption is proposed as mandatory under the 2024 NPRM. ePHI must be encrypted both at rest and in transit. OCR's Guidance on Encryption confirms that NIST-approved algorithms (AES-256, TLS 1.2+) are the standard. Weak encryption is treated the same as no encryption. Penetration testing validates that encryption is correctly implemented - not just that a policy says it is.

Testing Area	CFR Reference

TLS configuration and cipher suite validation	§164.312(e)(1), §164.312(e)(2)(ii)
Cleartext ePHI detection in transit (internal + external)	§164.312(e)(2)(ii) - transmission encryption
Database encryption validation at rest	§164.312(a)(2)(iv) - encryption and decryption
API response data - ePHI not over-exposed	§164.312(e)(1), §164.312(a)(1)
Encryption key management and exposure testing	§164.312(a)(2)(iv) - key security
Backup and archive encryption	§164.312(a)(2)(iv) + proposed NPRM backup controls

Network Segmentation

RELEVANT CONTROLS: §164.312(a)(1), §164.308(a)(1) - proposed explicit requirement under NPRM

Network segmentation is not explicitly named in the current Security Rule but is implied by the access control and risk management standards. The 2024 NPRM proposes making network segmentation an explicit requirement. OCR breach investigations consistently cite flat networks as an aggravating factor. The Change Healthcare breach (2024) - the largest healthcare breach in US history - exploited inadequate network segmentation that allowed lateral movement from a compromised entry point to critical ePHI systems.

Testing Area	CFR Reference
ePHI network isolation from corporate and guest networks	§164.312(a)(1) + proposed NPRM network segmentation
Lateral movement from compromised non-ePHI host	§164.308(a)(1)(ii)(A) - risk analysis validation
Medical device network segmentation (IoMT)	§164.312(a)(1) - ePHI system access control
Cloud VPC and subnet segmentation testing	§164.312(a)(1) - applies to cloud-hosted ePHI
VLAN hopping and inter-segment traversal	Validates physical and logical segmentation effectiveness
Firewall rule review and bypass testing	§164.312(a)(1), §164.308(a)(1)

Vulnerability Management

RELEVANT CONTROLS: §164.308(a)(1)(ii)(A), §164.308(a)(8)

Vulnerability management sits at the intersection of Risk Analysis (§164.308(a)(1)(ii)(A)) and Evaluation (§164.308(a)(8)). The 2024 NPRM proposes explicit cadence: vulnerability scans every 6 months, penetration testing at least annually, with critical patches required within 15 calendar days. Under current rule: frequency is risk-based. Under proposed NPRM: specific cadences are mandated.

Activity	CFR Reference / NPRM Cadence

Vulnerability scanning (automated)	§164.308(a)(8) - every 6 months under NPRM; risk-based under current rule
Annual penetration test	§164.308(a)(8) - annually under NPRM; periodic under current rule
Critical patch deployment	Proposed NPRM: within 15 calendar days of availability
High severity patch deployment	Proposed NPRM: within 30 calendar days
Remediation retesting	Expected by OCR auditors to confirm findings are resolved
Post-change security testing	§164.308(a)(8) - testing required after significant environmental changes

Audit Controls and Logging

RELEVANT CONTROLS: §164.308(a)(1)(ii)(D), §164.312(b)

§164.312(b) requires implementation of hardware, software, and procedural mechanisms to record and examine activity in systems containing ePHI. §164.308(a)(1)(ii)(D) requires regular review of audit logs. Penetration testing validates that audit controls actually capture malicious activity - if a pentest runs simulated attacks and no SIEM alerts fire, that is a direct §164.312(b) finding that must be reported.

Testing Area	CFR Reference
SIEM/log detection validation (did pentest generate alerts?)	§164.312(b), §164.308(a)(1)(ii)(D)
Audit log integrity testing (can logs be tampered with?)	§164.312(b) - log protection
Audit log completeness (are all ePHI access events captured?)	§164.312(b) - activity recording
Log retention and access control testing	§164.316(b) - documentation retention
Audit bypass testing (can logging be disabled?)	§164.312(b) - control effectiveness

Third-Party and Business Associate Risk

RELEVANT CONTROLS: §164.308(a)(1), §164.314, §164.308(b)

Business Associates handling ePHI are directly subject to the HIPAA Security Rule - not just through BAA contract terms, but as regulated entities in their own right. Under the 2024 NPRM, BAs must verify their technical safeguards are active within 24 hours of a CE request. Pentesters are Business Associates. Any firm accessing ePHI during testing must have a signed BAA in place before the engagement begins. This is non-negotiable - it is a legal requirement.

Scenario	HIPAA Implication

Pentesting firm accesses or could access ePHI during testing	BAA required - must be signed before engagement begins
Third-party EHR or SaaS vendor in scope for testing	§164.314 - BA safeguards must be validated, not just contractually assumed
Cloud hosting provider (AWS, Azure, GCP)	BA relationship - their ePHI configuration must be in pentest scope
Medical device vendor APIs in scope	§164.308(a)(1) - risks from third-party integrations must be assessed
Subcontractor receives ePHI from BA	§164.308(b) - subcontractors have same Security Rule obligations

Medical Device and IoMT Security

RELEVANT CONTROLS: §164.312(a)(1), §164.308(a)(1)(ii)(A)

Internet of Medical Things (IoMT) - connected medical devices, patient monitoring systems, infusion pumps, imaging equipment - are frequently overlooked ePHI attack surfaces. OCR has noted that medical device security is a growing enforcement focus. Medical devices often run legacy operating systems, have hard-coded credentials, and lack patch management. They are connected to the same network segments as ePHI systems - a significant lateral movement risk.

Testing Area	CFR Reference
Medical device default credential testing	§164.312(a)(2)(i) - unique user identification
IoMT network segmentation validation	§164.312(a)(1) - access control boundary testing
Legacy OS and unpatched vulnerability testing	§164.308(a)(1)(ii)(A) - risk analysis
Device API and management interface security	§164.312(a)(1), §164.312(d)
Medical device data exfiltration paths	§164.312(e)(1) - transmission security

06

The 2024 NPRM: What Is Changing?

HHS PROPOSED SECURITY RULE UPDATES - DECEMBER 2024

On December 27, 2024, HHS OCR issued a Notice of Proposed Rulemaking (NPRM) - the most significant proposed update to the HIPAA Security Rule since 2013. The NPRM was published in the Federal Register on January 6, 2025. As of June 2026, the current Security Rule remains in effect while rulemaking continues.

What Is Changing	Current Rule	Proposed NPRM
Penetration testing cadence	Periodic - risk-based, no fixed schedule	Annually (at minimum), or more frequently per risk analysis

Vulnerability scanning	Implied by risk analysis - no explicit cadence	Every 6 months minimum
Required vs. Addressable	Distinction preserved - addressable specs allow alternatives	Distinction eliminated - all specs mandatory (with limited exceptions)
Encryption	Addressable - risk-based decision	Mandatory for ePHI at rest and in transit
Multi-factor authentication	Not explicitly required	Mandatory with limited exceptions
Network segmentation	Implied by access control standards	Explicitly required
Asset inventory	Implied by risk analysis	Written inventory of all ePHI-touching assets, reviewed annually
Critical patch timelines	Risk-based	Critical: 15 days; High: 30 days
BA verification	Contractual attestation	BAs must verify safeguards within 24 hours on CE request

WHAT DOES NOT CHANGE UNDER NPRM

- §164.308(a)(8) Evaluation remains the primary pentest hook - the NPRM strengthens it with explicit cadence.
- Risk Analysis (§164.308(a)(1)(ii)(A)) remains required and foundational.
- Business Associate Agreements remain required - pentesters must still sign BAAs.
- Covered entities and BAs remain jointly responsible for ePHI security.
- Documentation requirements remain in place - pentest reports are still key compliance artifacts.

PLANNING GUIDANCE: ACT NOW, DON'T WAIT FOR FINAL RULE

The 2024 NPRM proposed a compliance window of 180 days after a final rule's effective date. If finalized in 2026, organizations could have as little as 6-8 months to achieve full compliance. Organizations that implement annual pentesting, semi-annual vulnerability scanning, MFA, encryption, and network segmentation now will be ahead of the requirement - and better protected against the ransomware attacks that drove the NPRM in the first place.

07

Pentest Scope for HIPAA

WHAT SHOULD BE IN SCOPE?

HIPAA pentest scope is defined by where ePHI exists or flows. Any system that creates, receives, maintains, or transmits ePHI - directly or indirectly - should be considered for inclusion. The 2024 NPRM proposes requiring a written asset inventory as the basis for scope definition.

Component	Typical Testing Focus	Relevant CFR
EHR / EMR systems	Authentication, access control, ePHI access paths, privilege escalation	§164.312(a)(1), §164.312(d)

Patient portals and web apps	Auth bypass, IDOR, ePHI exposure in API responses, session management	§164.312(a)(1), §164.312(e)(1)
Healthcare APIs and integrations	HL7/FHIR API security, OAuth abuse, data exposure, rate limiting	§164.312(a)(1), §164.312(e)(1)
Clinical networks	Segmentation, lateral movement, medical device access paths	§164.312(a)(1), proposed NPRM
Cloud infrastructure (AWS/Azure/GCP)	IAM misconfigurations, storage exposure, encryption validation	§164.312(a)(2)(iv), §164.312(e)
Medical devices (IoMT)	Default credentials, firmware, network access, management interfaces	§164.308(a)(1)(ii)(A)
On-premises data centers	Physical access, server room controls, endpoint security	§164.310
Backup and DR systems	Backup encryption, access controls, recovery system security	§164.310(d), proposed NPRM
Business Associate connections	Third-party access paths, VPN links, API keys, data sharing interfaces	§164.314

HIPAA-Specific Testing Considerations

- ePHI discovery testing: validate that automated scans can identify where ePHI is actually stored - not just where it should be stored per documentation.
- HL7/FHIR API security: healthcare-specific protocols have unique vulnerabilities. FHIR API authorization (SMART on FHIR) is a common weakness.
- Legacy system testing: many healthcare environments run Windows Server 2008, Windows 7, or older versions on clinical workstations - these must be in scope.
- Medical device network access: connected medical devices are frequently reachable from clinical workstations and should be tested for lateral movement risk.
- Telehealth platforms: video, messaging, and remote monitoring tools that process ePHI should be included in web application testing.

08 What OCR Auditors Expect in Practice

EVIDENCE REQUIREMENTS FOR HIPAA COMPLIANCE REVIEWS

TYPICALLY EXPECTED	COMMONLY RECOMMENDED
- Annual penetration test - internal and external networks. - Web application pentest covering all patient-facing and ePHI apps. - Vulnerability scanning program with documented cadence. - Written risk analysis updated after each pentest cycle. - Remediation tracking and retest evidence. - BAA signed with pentesting firm before engagement. - Pentest report mapped to HIPAA CFR controls. - Documentation retained for 6 years (§164.316(b)(2)).	- Medical device (IoMT) security testing. - Physical security assessment of ePHI facilities. - Social engineering / phishing simulation for workforce testing. - HL7/FHIR API-specific security testing. - Post-breach or post-incident penetration test. - Cloud configuration review (AWS/Azure/GCP). - Annual security awareness training with phishing simulation.

What a Compliant HIPAA Pentest Report Should Include

- Scope definition confirming all ePHI-bearing systems were assessed.
- Testing methodology (NIST SP 800-115, OWASP, or equivalent - must be documented).
- Findings with severity ratings mapped to specific HIPAA CFR controls.
- Proof of exploitation - screenshots, request/response captures, attack chains.
- Business impact articulated in ePHI terms (records at risk, regulatory exposure, breach cost).
- Remediation guidance tied to HIPAA implementation specifications.
- Retest confirmation - evidence that critical and high findings were remediated.
- BAA reference - documentation that the testing firm signed a BAA.
- Tester qualifications - relevant credentials demonstrating offensive security expertise.

DOCUMENTATION RETENTION: §164.316(b)(2)

HIPAA requires that documentation of security policies, procedures, and activities be retained for 6 years from the date of creation or last effective date. Pentest reports are compliance documents - they must be retained for 6 years and available for OCR audit on request.

09 Business Associate Requirements

WHAT BAS AND VENDORS MUST KNOW

Business Associates are directly subject to HIPAA Security Rule requirements - not just through contractual BAA terms, but as regulated entities in their own right under the 2013 Omnibus Rule. This has significant implications for SaaS vendors, MSPs, EHR providers, and any other vendor handling ePHI.

Requirement	What It Means for BAs

Security Rule compliance	BAs must implement all applicable HIPAA Security Rule safeguards - not just whatever the BAA says.
Risk Analysis	BAs must conduct their own risk analysis of ePHI systems - not rely on the covered entity's analysis.
Annual penetration testing	BAs should conduct their own pentest program covering systems that store/process/transmit ePHI for CEs.
BAA with pentesters	When a BA engages a pentesting firm that could access ePHI, a BAA is required.
24-hour verification (NPRM)	Proposed NPRM requires BAs to verify their safeguards are active within 24 hours of a CE request.
Subcontractor obligations	BAs must flow down Security Rule obligations to subcontractors via BAA - and verify compliance.
Breach notification	BAs must notify covered entities of breaches without unreasonable delay and within 60 days.

Pentest Firm = Business Associate

PENTEST FIRM = BUSINESS ASSOCIATE

Any penetration testing firm that could access, receive, maintain, or transmit ePHI during testing is legally a Business Associate under HIPAA. A BAA must be in place before testing begins. What the BAA should cover: permitted uses of ePHI data accessed during testing, data destruction requirements post-engagement, breach notification obligations, and subcontractor restrictions. A pentesting firm that refuses to sign a BAA cannot lawfully conduct testing on systems containing ePHI.

10

Resources

HIPAA SECURITY RULE AND PENTESTING REFERENCES

HHS: HIPAA Security Rule Summary hhs.gov/hipaa/for-professionals/security

Official HHS summary of the Security Rule. Starting point for understanding 45 CFR Part 164 obligations. Free.

HHS OCR: HIPAA Security Rule NPRM (2024) Fact Sheet hhs.gov - NPRM Fact Sheet

Official HHS summary of the December 2024 proposed rule changes including penetration testing and vulnerability scanning requirements.

Federal Register: HIPAA NPRM Full Text (January 6, 2025) federalregister.gov - HIPAA NPRM 2024

The complete proposed rule text including proposed CFR language for penetration testing, vulnerability scanning, MFA, encryption, and network segmentation.

eCFR: 45 CFR §164.312 - Technical Safeguards (Current Rule) ecfr.gov - §164.312

Live current text of the Technical Safeguards standard including access control, audit controls, integrity, authentication, and transmission security.

HHS: HIPAA Security Series - Technical Safeguards (Guidance Paper) hhs.gov - Technical Safeguards Guide

Official HHS implementation guidance for §164.312. Explains each specification and how to implement them. Essential reading for scoping HIPAA pentests.

NIST SP 800-66 Rev. 2: Implementing the HIPAA Security Rule csrc.nist.gov - NIST SP 800-66

NIST's guidance for implementing HIPAA Security Rule controls, including risk analysis and evaluation. The standard methodology reference for HIPAA technical assessments.

NIST SP 800-115: Technical Guide to Information Security Testing csrc.nist.gov - NIST SP 800-115

The how-to-test standard referenced by HIPAA assessors. Defines penetration testing methodology acceptable for §164.308(a)(8) Evaluation. Use for scoping and methodology documentation.

Software Secured: NIST SP 800-115 and Pentesting softwaresecured.com

Explains how NIST SP 800-115 (technical testing standard) maps to compliance frameworks including HIPAA. Useful for client conversations about test methodology and scope.

HHS: OCR Cybersecurity Performance Goals (CPGs) hhs.gov - HHS CPGs

HHS-published cybersecurity performance goals aligned to HIPAA Security Rule obligations. Includes guidance on penetration testing, vulnerability management, and incident response.

OWASP Testing Guide v4.2 owasp.org - OWASP Testing Guide

The widely referenced methodology for web application and API security testing. Directly applicable to EHR/EMR systems, patient portals, and healthcare APIs under §164.312(a)(1).