



HIPAA PENETRATION TEST

Scope definition checklist

A working checklist for scoping systems, applications, and network components that create, receive, maintain, or transmit ePHI.

HIPAA penetration testing scope must cover all systems, applications, and network components that create, receive, maintain, or transmit ePHI. This includes often-overlooked areas such as medical device connectivity and IoMT (Internet of Medical Things) infrastructure.



1. Core application testing scope

Web application security assessment:

- ☐ Authentication and session management testing across all user roles
- ☐ Input validation and injection attack simulation (SQL, NoSQL, LDAP, XML)
- ☐ Business logic flaw identification affecting patient data access controls
- ☐ File upload security and data export functionality validation

API security testing requirements:

- ☐ REST and GraphQL endpoint authentication bypass attempts
- ☐ Parameter manipulation and data exposure testing
- ☐ Rate limiting and DDoS protection validation
- ☐ API versioning security and deprecated endpoint assessment

2. Infrastructure and network testing scope

Internal network penetration testing:

- ☐ Network segmentation validation between ePHI and non-ePHI systems
- ☐ Privilege escalation testing from compromised workstations
- ☐ Database access control validation and data exfiltration testing
- ☐ Wireless network security assessment, including guest access isolation

Cloud infrastructure security testing:

- ☐ Container and serverless function security validation
- ☐ Cloud storage permission and encryption testing (S3, Azure Blob, GCP buckets)
- ☐ Identity and access management (IAM) role permission validation
- ☐ Logging and monitoring system security assessment

3. Medical device and IoMT security testing

Device connectivity security:

- ☐ Medical device network isolation and communication encryption
- ☐ Device authentication and certificate management validation
- ☐ Firmware update security and default credential testing
- ☐ Patient monitoring system data transmission security

Integration point testing:

- ☐ HL7 FHIR API security validation
- ☐ Electronic health record (EHR) integration security testing
- ☐ Telehealth platform security assessment
- ☐ Medical imaging system (DICOM) security validation

4. Third-party integration testing scope

Business associate security validation:

- ☐ Vendor API access control testing
- ☐ Data sharing agreement technical implementation validation
- ☐ Third-party authentication integration security assessment
- ☐ Backup and disaster recovery system security testing

Scope	Recommended frequency
Full scope testing	Annually or after major system changes
Application focused testing	Quarterly for customer-facing applications
Infrastructure testing	Semi-annually or after network modifications
Continuous monitoring	Daily automated scans, or monthly automated penetration tests with monthly comprehensive analysis

Where Beagle Security fits in

A scope checklist only tells you what to check. Beagle Security is how you actually keep testing it, release after release, instead of year after year. It covers the web applications and API layers in this checklist, including REST and GraphQL endpoints your ePHI moves through, and runs on a set schedule instead of a single scan. That's the difference auditors care about: HIPAA's Security Rule expects ongoing risk analysis and not a one time, check the box test.

Ready to see where your own application stands? Start a free trial at <https://app.beaglesecurity.com/signup> and get your first HIPAA mapped report without waiting on a consultant's calendar.