HIPAA Penetration Testing Checklist

Scope, safeguards, evidence, and cadence for covered entities and business associates

Use this checklist to prepare a HIPAA penetration test that produces evidence an auditor or HHS OCR reviewer will accept. Every item maps to the HIPAA Security Rule or to the report artifacts that back it up.

1. Scope definition (ePHI systems)

- [ ] Inventory every system that creates, receives, maintains, or transmits ePHI
- [ ] List EHR / EMR platforms and any vendor-hosted clinical modules
- [ ] List patient portals, provider portals, and mobile apps
- [ ] List HL7 v2 and FHIR integration endpoints and interface engines
- [ ] List connected medical devices and device management consoles
- [ ] List cloud accounts, storage buckets, and databases holding ePHI
- [ ] List internal network segments with ePHI access
- [ ] Identify business associates with ePHI access and confirm BAAs are current

2. Administrative safeguards (Sec. 164.308)

- [ ] Confirm the current Security Risk Analysis 164.308(a)(1)(ii)(A) is on file
- [ ] Confirm the last technical evaluation 164.308(a)(8) and its date
- [ ] Map prior findings to remediation owners and closure evidence
- [ ] Confirm workforce access authorization and termination procedures
- [ ] Confirm incident response procedures and breach notification workflow
- [ ] Confirm contingency plan and backup restoration testing

3. Technical safeguards (Sec. 164.312)

- [ ] Access control 164.312(a): unique user IDs, least privilege, emergency access
- [ ] Test for cross-patient and cross-tenant access to ePHI
- [ ] Test authentication: MFA coverage, session handling, password reset flows
- [ ] Audit controls 164.312(b): logging of ePHI access, tamper resistance
- [ ] Integrity 164.312(c): protection against improper alteration or destruction
- [ ] Person or entity authentication 164.312(d): API and machine identity checks
- [ ] Transmission security 164.312(e): TLS configuration and encryption in transit
- [ ] Encryption at rest for databases, backups, and object storage

4. Testing execution

- [ ] Signed rules of engagement and authorization letter
- [ ] Staging or production decision documented with patient-safety review
- [ ] Synthetic data used wherever live ePHI is not required
- [ ] External network and public attack surface tested
- [ ] Web application and API testing against portals and integrations
- [ ] Internal network and lateral movement paths to ePHI tested
- [ ] Social engineering or vishing included if in scope

5. Evidence and reporting

- [ ] Every finding mapped to a Security Rule safeguard citation
- [ ] Executive summary suitable for leadership and HHS OCR review
- [ ] Technical detail with reproduction steps and exploited paths to ePHI
- [ ] Risk ratings tied back into the Security Risk Analysis register
- [ ] Remediation guidance with owners and target dates
- [ ] Retest performed and closure evidence attached
- [ ] Letter of attestation available for customers and payers

6. Cadence and 2026 readiness

- [ ] Penetration test at least every 12 months and after material changes
- [ ] Automated vulnerability scanning at least every 6 months
- [ ] Business associate testing expectations written into vendor reviews
- [ ] Calendar set for next test, next scan, and next risk analysis update
- [ ] HITRUST CSF overlap reviewed if certification is on the roadmap