PACKET33

HIPAA Risk Assessment Checklist

A two part framework: a structured interview mapped to NIST 800-66, paired with technical verification of the actual cloud environment.

This checklist mirrors the methodology we use in our own HIPAA risk assessments. Part One is an administrative and policy review mapped against NIST Special Publication 800-66. Part Two is a technical verification pass against the actual cloud environment, since policy documents and real system configuration frequently do not match. Each finding should be scored on likelihood and impact from 1 (low) to 5 (high) rather than treated as a simple pass or fail.

Part One. Structured Interview (NIST 800-66 mapped)

Administrative Safeguards

- [ ] Security management process is documented, including a formal risk analysis and risk management plan
- [ ] A sanction policy exists for workforce members who fail to comply with security policies
- [ ] Information system activity is reviewed on a regular, defined cadence
- [ ] A named individual holds assigned security responsibility for the organization
- [ ] Workforce security procedures cover authorization, supervision, and clearance
- [ ] Termination procedures revoke system access promptly when employment ends
- [ ] Access authorization and access establishment procedures are documented and followed
- [ ] Security awareness and training is provided to the workforce, including phishing and password guidance
- [ ] Security incident response and reporting procedures are documented and tested
- [ ] A contingency plan exists, covering data backup, disaster recovery, and emergency mode operation
- [ ] The contingency plan has been tested within the last 12 months
- [ ] Periodic technical and nontechnical evaluation of safeguards is performed
- [ ] Business associate agreements are in place with every vendor that touches PHI

Physical Safeguards

- [ ] Facility access controls limit physical access to systems containing PHI
- [ ] A facility security plan documents how physical access is controlled and monitored
- [ ] Workstation use policies define appropriate use of systems that access PHI
- [ ] Workstation security controls (screen locks, physical placement) are in place
- [ ] Device and media disposal procedures ensure PHI is unrecoverable before disposal
- [ ] Media reuse procedures remove PHI before storage media is repurposed

Technical Safeguards

- [ ] Unique user identification is enforced for every individual accessing PHI
- [ ] An emergency access procedure exists for obtaining PHI during an emergency
- [ ] Automatic logoff is enforced after a defined period of inactivity
- [ ] Audit controls record and examine activity in systems containing PHI
- [ ] Integrity controls confirm PHI has not been improperly altered or destroyed
- [ ] Person or entity authentication verifies users are who they claim to be

- [ ] Transmission security controls protect PHI in transit, including encryption

Part Two. Technical Verification (cloud environment)

This pass verifies that the safeguards described in Part One are actually configured in the live environment. We run this using Prowler against the cloud accounts in scope, but the checks below apply regardless of tooling.

Identity and Access Management

- [ ] Multi factor authentication is enforced for all users with access to systems containing PHI
- [ ] No unused or stale credentials remain active on privileged accounts
- [ ] Access follows least privilege, with no broad admin roles assigned by default
- [ ] Root or account owner credentials are not used for day to day operations

Encryption

- [ ] Data containing PHI is encrypted at rest in every storage location and database
- [ ] Data containing PHI is encrypted in transit, with TLS enforced and weak protocols disabled
- [ ] Encryption key management follows documented rotation and access procedures

Logging, Monitoring, and Network Configuration

- [ ] Audit logging is enabled across all systems and cloud services in scope
- [ ] Logs are retained for a defined period consistent with policy and regulatory expectations
- [ ] No storage buckets or databases containing PHI are publicly exposed
- [ ] Network security groups and firewall rules restrict access to only what is required
- [ ] Backup configurations are verified as functioning, not just documented as existing

---

Scoring Findings

Score every gap on two axes, likelihood (how probable is exploitation or failure) and impact (how severe is the consequence if it occurs), each on a 1 to 5 scale. Multiply the two scores to prioritize remediation. A finding scoring 4 or 5 on either axis should be addressed before the next audit cycle or enterprise deal review, regardless of its combined score.
