eSureITy

HIPAA RISK ASSESSMENT

Protect PHI. Prove Control. Stay Insurable.

Compliance without evidence is operational risk

Regulators don't accept "we're compliant" as an answer. They expect a current, documented risk analysis, working safeguards, trained people, and auditable processes tied to how PHI actually moves through your environment.

Annual checklists, stale diagrams, and policy binders that don't match reality leave executives exposed when something breaks in care operations, privacy, or data handling.

eSureITy's HIPAA Risk Assessment pressure-tests your assumptions, exposes the failure paths that matter most, and gives you defensible proof that your safeguards work in practice—not just on paper.

Where Healthcare Organizations Actually Fail

- **Outdated or incomplete risk analysis** - Static, once-a-year exercises instead of a living risk picture mapped to real PHI workflows and system changes.
- **Weak identity & access** - Inconsistent MFA, excessive privileges, shared or service accounts that no one reviews, and missing ownership for elevated access.
- **Unmanaged vendor exposure -** BAAs that don't reflect reality, third parties with broad or persistent access, and no structured oversight of how they handle PHI.
- **Flat networks & remote access sprawl -** Clinical systems reachable from user subnets, generic VPN access without strong controls, and limited segmentation between care delivery and everything
- **Paper policies, no practice -** Incident response plans never exercised, workforce training not measured, and no audit trail to show who did what, when.

Consequence: higher breach likelihood, greater disruption to clinical and business operations, and gaps that are difficult to explain when regulators start asking detailed questions.

What "good" must deliver for HIPAA

A strong HIPAA risk program isn't vague. It produces concrete, repeatable outcomes:

- Current, documented risk analysis tied to actual PHI data flows
- Enforced MFA and least-privilege access for all administrative and remote access
- Network segmentation that protects clinical and other critical systems from broad lateral movement
- Vendor risk management with current BAAs, defined responsibilities, and ongoing oversight
- Incident response that is tested, timed, and capable of producing evidence of actions taken
- A centralized proof pack that auditors, boards, and external reviewers can understand quickly

One outcome of this assessment is a defensible risk analysis and control set that aligns with modern cyber insurance coverage requirements for documented safeguards and tested response.

Anything less is noise.

Contact Us

info@eSureITy.com

www.eSureITy.com

How eSureITy Raises Your Readiness

Threat-led. Regulator-aligned. Built for real environments.

Assessment Framework

1) Discover & Map PHI Reality

- Inventory systems, users, vendors, and data flows
- Identify where PHI is stored, processed, transmitted, and exposed—on-prem, in the cloud, and across third parties

2) Test Safeguards Where They Break

- Validate access controls, encryption, logging, segmentation, remote access, backups, and response
- Examine administrative, physical, and technical safeguards against likely threat paths

3) Quantify Risk & Prioritize Remediation

- Score findings by likelihood and impact to care operations, privacy, and business continuity
- Produce a sequenced, budget-aware plan that focuses on the riskiest gaps first

4) Prove It to Auditors & Insurers

- Package findings, owners, and timelines into concise views for executives, compliance, and IT
- Make it clear what to fix now, what to schedule, and what to monitor

How We Work

- **Reframe:** Connect today's common HIPAA failures directly to fines, downtime, and operational disruption.
- **Diagnose:** Test your safeguards against real PHI workflows and threat scenarios, not just policy text.
- **Prescribe:** Sequence remediation steps that reduce risk fastest with clear owners and target dates.
- **Enable:** Give control owners concrete tasks, examples, and acceptance criteria so fixes can be implemented and verified.

Deliverables Detail

- **Risk Register & Heat Map**: Likelihood × impact scoring with linkage to specific PHI systems and workflows.
- **PHI Data Flow Diagrams:** Systems, vendors, and trust boundaries visualized so gaps are obvious at a glance.
- **Control Effectiveness Scores:** Before/after metrics by safeguard family to show improvement over time.
- **Evidence Library:** Logs, configurations, training artifacts, IR drill outputs, and other audit-ready proof.
- **Board-Ready Summary:** A one-page narrative for executives and trustees that explains risk, progress, and next steps in plain language.

Scope, Methodology, and Outcomes

Scope We Cover (Included in Every Assessment)

- **Administrative safeguards:** Risk analysis/management plan, workforce training, sanctions, contingency planning, incident response program and tabletop validation
- **Physical safeguards**: fFacility access, device and media controls, disposal and sanitization procedures
- **Technical safeguards:** Access control, MFA posture, audit logging, encryption at rest and in transit, integrity controls, ePHI backup and restore validation
- **Network & segmentation:** Isolation of clinical systems, remote access governance, secure configurations, vulnerability-scanning evidence
- **Vendor/BAA oversight:** Inventory, BAA status, data-sharing patterns, access reviews, monitoring expectations
- **Policy & procedure:** Security, privacy, and IT policies mapped to observed practice—not just written intent

What You Get

- ✓ **Executive briefing (PDF + dashboard)** with ranked risks, PHI flow visuals, control gaps, and business impact
- ✓ **Compliance Mapping** aligned to HIPAA Security and Privacy Rules (§164.308, §164.310, §164.312) and related policies
- ✓ **Remediation Roadmap** for MFA, segmentation, vendor control, incident response, and workforce practices—with owners and timelines
- ✓ **Consolidated Evidence** set that reduces friction with auditors, quality committees, and leadership reviews

Why eSureITy

- Healthcare-focused assessors who understand clinical workflows, EHR integrations, and medical-device realities
- Threat-led methodology that ties findings to real attack paths and operational consequences
- End-to-end support from assessment through remediation validation
- Proof over promises: audit-ready artifacts instead of slideware

HIPAA compliance without proof is a liability. eSureITy gives you the analysis, the fixes, and the evidence to protect PHI and strengthen your overall risk posture.

Book your eSureITy HIPAA Risk Assessment.