GRYPHON SECURITY

# HIPAA Security Rule Risk-Based Security Audit

**Clear Risk Insight. Defensible Decisions.**

A focused security assessment designed for organizations that create, receive, maintain, or transmit electronic protected health information (ePHI), where regulatory compliance, operational continuity, and organizational trust are non-negotiable.

HIPAA-regulated environments face a distinct risk profile. They concentrate sensitive health information, rely on interconnected clinical and business systems, and are frequent targets for ransomware, credential compromise, and data extortion. This service provides leadership with a clear, defensible understanding of their current security posture using a risk-based approach grounded in the HIPAA Security Rule.

## What We Do

We conduct a structured security audit evaluating the **administrative, technical, and physical safeguards** implemented to protect ePHI, as required by the HIPAA Security Rule.

Rather than applying generic checklists or prescriptive frameworks, we assess how safeguards operate in actual workflows – how users authenticate, how systems containing ePHI are accessed, how data is stored and transmitted, how security events are detected, and how third-party relationships affect overall risk.

The result is a practical, evidence-based evaluation of current safeguards – not a certification, scorecard, or compliance checkbox exercise.

## Why This Matters

Security Rule compliance is inherently risk-based. Organizations must be able to demonstrate that safeguards are reasonable and appropriate given their size, complexity, and risk environment.

Safeguard gaps can expose ePHI, disrupt operations, and lead to regulatory scrutiny, contractual impact, and loss of trust. This audit identifies where material risk exists, distinguishes high-impact exposures from lower-value issues, and equips leadership with a defensible basis for security decisions before an incident or inquiry occurs.

## Our Assessment Approach

This service applies a risk-based assessment methodology aligned with the HIPAA Security Rule.

The assessment is not a certification, attestation, or government audit. It is a structured risk evaluation designed to answer one core question:

**If an incident, breach, or regulatory review occurs, can leadership demonstrate that security decisions were informed, reasonable, and defensible under the HIPAA Security Rule?**

Findings are contextualized to the organization's operational model, workforce, systems, and threat exposure so recommendations are achievable, prioritized, and aligned with actual risk.

## What's Evaluated

The audit focuses on safeguard areas most relevant to protecting ePHI, including:

- **Access & Authentication**
  Workforce access controls, authentication mechanisms, and access lifecycle management
- **Monitoring & Logging**
  Audit controls, activity monitoring, and visibility into unauthorized or suspicious activity
- **Backup & Recovery**
  Backup coverage, data integrity, recovery capability, and resilience against destructive events
- **Incident Readiness**
  Detection capability, response procedures, internal roles, and coordination readiness
- **Data Protection**
  Encryption, transmission security, data handling practices, and protection of ePHI
- **Governance & Training**
  Policies, risk management processes, workforce training, and leadership oversight

Each area is evaluated in terms of whether safeguards are reasonable, appropriate, implemented, and operating as intended.

## What You Receive

- Executive-level findings written in clear, non-technical language
- Risk-rated gaps (High / Medium / Low) tied to realistic threat scenarios
- Evidence-based recommendations grounded in observed conditions
- A prioritized remediation roadmap to support planning, budgeting, and accountability

## Who This Service Is For

This service is designed for:

- HIPAA covered entities
- Business associates and subcontractors
- Healthcare providers, payers, and healthcare support organizations
- Any organization that creates, receives, maintains, or transmits ePHI

It is particularly valuable for organizations preparing for OCR inquiries, insurance renewal, third-party risk assessments, or internal governance reviews.

## This Service Is *Not* Designed For

- Organizations seeking a checkbox compliance audit
- Organizations looking for managed security services or tool resale
- Environments without leadership commitment to remediation and risk ownership

Gryphon Security focuses on clarity, independence, and defensible outcomes.

## Why Gryphon Security

- **HIPAA Security Rule Focused:** Built around the "reasonable and appropriate" safeguard standard
- **Clear & Defensible:** Findings leadership can understand and justify
- **Independent & Vendor-Neutral:** No resale pressure, no product bias

## Next Steps

An initial conversation is structured, confidential, and obligation-free.

We will:

- Confirm scope and environment
- Discuss key risk concerns
- Explain exactly what the assessment will and will not cover

We will not pressure you into tools, managed services, or long-term contracts.

**Gryphon Security, LLC**
Risk-Based HIPAA Security Assessments
info@gryphonsec.com | www.gryphonsec.com