ProCern™
TECHNOLOGY SOLUTIONS

1-833-PROCERN (776-2376) | PROCERN.COM

Preparing for the 2025 HIPAA Security Rule Changes:

A Practical Checklist

As the healthcare industry braces for significant changes to the HIPAA Security Rule in 2025, organizations must act now to safeguard electronic protected health information (ePHI). This checklist is designed to help organizations navigate the evolving compliance landscape with practical steps divided into four categories: Quick Wins, Medium Effort Initiatives High Effort Initiatives, and Do As Required. By starting with the immediate priorities and addressing more complex projects over time, you can prepare for the 2025 update to HIPAA's Security Rule ahead of time and minimize the burden to your organization when the full implementation happens.

1

Immediate Priorities

Tasks that can be quickly addressed

These initiatives require minimal resources and should be tackled immediately.

- [ ] **Set Specific Compliance Timelines**
  Establish deadlines for meeting the upcoming requirements to stay organized and focused.
- [ ] **Update Asset Management Practices**
  Create and maintain an up-to-date technology asset inventory and a network map showing ePHI movement. Update this inventory annually or after operational changes.
- [ ] **Conduct a Detailed Risk Analysis**
  Write a comprehensive risk assessment that identifies threats, vulnerabilities, and risk levels using your asset inventory and network map.
- [ ] **Test Security Measure Effectiveness**
  Conduct annual penetration tests, ongoing vulnerability scans, and reviews of your security measures to verify their efficacy.
- [ ] **Modernize Standards**
  Update policies and procedures to align with new technological advancements and definitions under the revised Security Rule.
- [ ] **Mandate Encryption**
  Implement encryption for ePHI at rest and in transit, with exceptions only where justified.

STEPS CONTINUED ON NEXT PAGE

2

Strategic Next Steps

Medium-effort initiatives that build on foundational compliance efforts

These projects may require a moderate investment of time and resources but can be completed relatively quickly.

- [ ] **Enhance Documentation Requirements**

  Ensure all Security Rule policies, procedures, plans, and analyses are documented in writing.

- [ ] **Strengthen Technical Controls**

  Implement multi-factor authentication, anti-malware protection, vulnerability scans (every six months), annual penetration testing, and restrict unused network ports and extraneous software.

- [ ] **Improve Contingency and Incident Planning**

  Develop detailed contingency and incident response plans. Ensure systems can be restored within 72 hours and test/revise plans annually.

- [ ] **Establish Backup and Recovery Standards**

  Implement robust technical controls for backing up and recovering ePHI and related systems.

- [ ] **Adopt Uniform Implementation Standards**

  Transition from optional “addressable” specifications to mandatory compliance with most implementation requirements, addressing all controls outlined by NIST. Currently, NIST lists 805 “required” and “addressable” actions for the HIPAA Security Rule.

3

Conditional Requirements

Take action when applicable

These steps may only apply if the requirements are finalized or relevant to your organization’s operations.

- [ ] **Implement Contingency Notifications**

  Notify business associates and subcontractors of contingency plan activation within 24 hours.

- [ ] **Fulfill Group Health Plan Responsibilities**

  Ensure group health plans comply with safeguards, hold agents accountable, and provide contingency plan activation notifications within 24 hours.

- [ ] **Conduct Annual Compliance Audits**

  Perform annual audits to assess and confirm compliance with the HIPAA Security Rule.