Scrut Automation

Checklist

Scrut Automation HIPAA Security Rule Checklist

Scrut Automation

Scrut Automation HIPAA Security Rule Checklist

Key steps to comply with critical healthcare legislation

Healthcare is one of the most heavily regulated sectors in the United States. The Health Insurance Portability and Accountability Act (HIPAA), a federal law, is the foundation of that regulatory framework. It imposes strict controls for Protected Health Information (PHI), which it defines as all "individually identifiable health information" (with some narrow exclusions).

Covering everything from medical records to information security standards, the regulations implementing HIPAA contain complex requirements for certain organizations. One of the most important ones is the "Security Rule," laid out in Title 45 of the U.S. Code of Federal Regulations (CFR), specifically part 160 and subparts A and C of part 164.

This checklist provides a comprehensive, step-by-step guide to meeting HIPAA's requirements. We'll include references to the relevant section (§) along the way.

STEP 1: Determine if HIPAA applies (§160.102)

Two types of organizations need to worry about HIPAA, so determine if you are a:

- [ ] **Covered Entity,** which includes health:
  - Plans
  - Clearinghouses
  - Care providers
- [ ] **Business Associate,** which
  - Does anything with PHI on behalf of a Covered Entity (or other Business Associate), such as:
    - [ ] Claims processing or administration
    - [ ] Data analysis, processing, or administration
    - [ ] Utilization review
    - [ ] Quality assurance
    - [ ] Patient safety activities
    - [ ] Billing
    - [ ] Benefit management
    - [ ] Practice management
    - [ ] Repricing
  - **An entity that provides services requiring disclosure of PHI**, such as those related to:
    - [ ] Law
    - [ ] Actuarial services
    - [ ] Accounting
    - [ ] Consulting
    - [ ] Data aggregation
    - [ ] Management
    - [ ] Administration

- [ ] Accreditation
- [ ] Finance

If you check any of these boxes, proceed to the next step.

General requirements (§164.306)

- Everyone subject to HIPAA must, at a high level:
  - Ensure the confidentiality, integrity, and availability of all PHI created, received, maintained, or transmitted.
  - Protect against reasonably anticipated threats or hazards to the security or integrity of such information.
  - Protect against any reasonably anticipated impermissible uses or disclosures of such information.
  - Ensure workforce compliance.

STEP 2: Analyze how best to implement HIPAA requirements (§164.306)

Those subject to HIPAA have some flexibility in meeting its requirements and:

- May use any security measures to reasonably and appropriately implement the Security Rule.
- Should consider:
  - Their size, complexity, and capabilities.
  - Their technical infrastructure, hardware, and software security capabilities.
  - The costs of security measures.
  - The probability and criticality of potential risks to PHI.

The Security Rule also establishes two categories of requirements:

- **Required:** These measures must be implemented—there is no choice.
- **Addressable:** This means the organization has two options:
  - Implement the measure; OR
  - Document why it would not be reasonable and appropriate to implement the measure; AND
  - Implement an equivalent alternative measure if reasonable and appropriate.

Addressable measures are **not** optional. Organizations must assess whether the measure is reasonable and appropriate. If not, they must document their decision and implement an equivalent alternative measure, if reasonable and appropriate.

In this checklist, assume a control is required unless labeled addressable.

STEP 3: Implement administrative safeguards (§164.308)

These include:

- [ ] **Policies and procedures to prevent,** detect, contain, and correct security violations, including:
- [ ] Thoroughly assessing risks and vulnerabilities to the confidentiality, integrity, and availability of PHI.
- [ ] Applying security measures sufficient to reduce risks and vulnerabilities to a reasonable level.

- [ ] Applying sanctions against employees who do not comply with security policies and procedures.
- [ ] Conducting procedures to regularly review records of information system activity, such as audit logs, access reviews, and security incident reports.

- **Identifying a security official** responsible for developing and implementing policies and procedures.
- **Policies and procedures to ensure workforce members have appropriate access to PHI** and prevent those who should not have access from obtaining it, such as:
  - [ ] For the authorization and supervision of employees who work with PHI or in locations where it might be accessed **(addressable).**
  - [ ] To determine whether a workforce member's access to PHI is appropriate **(addressable).**
  - [ ] For terminating access to PHI when employment ends **(addressable).**
- **Policies and procedures for authorizing access to PHI,** like:
  - [ ] Protecting the PHI of a clearinghouse from unauthorized access by the larger organization.
  - [ ] Granting access to PHI through access to a workstation, transaction, program, process, or similar mechanism **(addressable).**
  - [ ] Establishing, documenting, reviewing, and modifying a user's right of access to a workstation, transaction, program, or process **(addressable).**
- **A security awareness and training program,** including these addressable measures:
  - [ ] Periodic security updates.
  - [ ] Procedures for guarding against, detecting, and reporting malicious software.
  - [ ] Procedures for monitoring login attempts and reporting discrepancies.
  - [ ] Password management.
- **Policies and procedures to identify and respond to suspected or known security incidents** and mitigate their harmful effects.
- **Policies and procedures for responding to emergencies** like fire, vandalism, system failure, and natural disasters that threaten PHI, including:
  - [ ] Data backup plans to create and maintain exact copies of PHI.
  - [ ] Disaster recovery plans to restore any loss of data.
  - [ ] Emergency plans to enable the continuation of business processes and protect PHI.
  - [ ] Periodic testing and revision of contingency plans **(addressable).**
  - [ ] Assessment of the relative criticality of specific applications and data in support of contingency plans **(addressable)**
- **Periodic technical and non-technical evaluation** that establishes the extent to which security policies and procedures meet the Security Rule's requirements.

STEP 4: Apply physical protective measures (§164.310)

All organizations subject to HIPAA must:

- [ ] **Implement policies and procedures to limit physical access** to systems and their facilities while ensuring that properly authorized access is allowed, including:
  - **Procedures that allow facility access** to restore lost data (addressable).
  - **Policies and procedures to safeguard facilities and equipment** from unauthorized physical access, tampering, and theft **(addressable).**

- **Procedures to control and validate a person's access to facilities** based on role or function **(addressable).**
- **Policies and procedures to document repairs and modifications** to the physical security components of a facility **(addressable).**

☐ **Implement policies and procedures specifying the proper functions** to be performed, how they are to be performed, and the physical attributes of the surroundings of a specific workstation accessing PHI.

☐ **Restrict access to authorized users** for workstations that can access PHI.

☐ **Implement policies and procedures** for the receipt, removal, and movement of hardware containing PHI, such as:

- Those addressing the final disposition of PHI and the hardware or media storing it.
- Those controlling the removal of PHI from media before re-using it.
- Recording movements of hardware and media and people responsible for them **(addressable).**
- Backing up PHI before moving equipment **(addressable).**

STEP 5: Confirm technical controls (§164.312)

Here, the Security Rule further requires:

☐ **Policies and procedures to restrict access** to information systems containing PHI to authorized users through:

- Unique user identities.
- Emergency access procedures.
- Automatic log-off **(addressable).**
- Encryption **(addressable).**

☐ **Hardware, software, or procedural auditing mechanisms** to record activity in systems processing PHI.

☐ **Protect PHI from alteration or destruction** through:

- Policies and procedures.
- Electronic mechanisms to confirm PHI integrity **(addressable).**

☐ **Verifying the identity of individuals requesting access to PHI to ensure they are who they claim to be.**

☐ **Guarding against unauthorized access to PHI transmitted electronically** by way of:

- Measures to confirm PHI is not incorrectly modified **(addressable).**
- Mechanisms to encrypt PHI **(addressable).**

STEP 6: Enforce contractual and organizational requirements (§164.314)

HIPAA requirements extend throughout the information supply chain, and anyone subject to them must:

☐ **Ensure contracts** with Business Associates **meet Security Rule requirements.**

☐ Require these Business Associates (and any subcontractors) **to report security incidents** to the Covered Entity.

☐ If a group health plan, **ensure PHI transmitted back and forth to the plan sponsor is reasonably and appropriately safeguarded** through requirements that the plan sponsor:

- Have administrative, physical, and technical safeguards protecting the confidentiality, integrity, and availability of PHI.
- Establish reasonable separation between the group health plan and plan sponsor through appropriate security measures.

- Require agents to whom it provides information to apply reasonable security measures.
- Report any security incidents to the group health plan.

STEP 7: Document and retain information about your security program (§164.316)

Finally, under the Security Rule, all organizations subject to HIPAA must:

- **Maintain policies and procedures** meant to comply with the rule.
- **Document all actions, activities, and assessments** required by the rule.
- **Retain all such documentation** for 6 years from creation or last effective date.
- **Make the documentation available** to those implementing Security Rule requirements.
- **Review and update the documentation** as needed based on environmental or operational changes impacting PHI security.

Need help with HIPAA Security Rule compliance?

The Scrut Platform is purpose-built to help growing businesses navigate complex requirements like the HIPAA Security Rule and other standards.

Here's how our platform helps with HIPAA compliance:

- **Automates compliance:** Reduces manual tasks, simplifying HIPAA management.
- **Enhances risk management:** Provides real-time visibility into risks and controls.
- **Centralized platform:** Manage HIPAA and other compliance frameworks in one place.
- **Continuous monitoring:** Keeps you up-to-date on evolving HIPAA requirements.
- **Simplified reporting:** Generates clear, audit-ready compliance reports.

With more than 50+ different compliance frameworks, we can help you stay current with your requirements, meet customer demands, and strengthen your cybersecurity posture.