CTRL THE FUTURE LLC

HIPAA SECURITY READINESS CHECKLIST

A practical self-review aligned to foundational HIPAA Security Rule safeguard areas

Purpose: This checklist is an educational readiness tool for HIPAA regulated entities evaluating foundational practices used to protect electronic protected health information (ePHI). It is not a substitute for the accurate and thorough risk analysis required by the HIPAA Security Rule and does not determine or certify HIPAA compliance.

Organization: _____

Entity type: ■ Covered Entity ■ Business Associate ■ Other / Unsure

Completed by: _____

Date: _____

How to Use This Checklist

For each statement, select the response that best reflects current practices. For addressable implementation specifications, organizations should evaluate whether the safeguard is reasonable and appropriate and document decisions and alternatives as required. Record evidence, owners, or follow-up actions in Notes.

READY	PARTIAL	NOT READY	N/A
Implemented / supported	Some elements exist	Absent, incomplete, or unknown	Not applicable

1. Security Management Process & Risk Analysis

HIPAA Security readiness statement	Ready	Partial	Not Ready	N/A	Notes
An accurate and thorough risk analysis addresses potential risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI created, received, maintained, or transmitted.	■	■	■	■	
The organization has identified where ePHI is stored, received, maintained, and transmitted, including relevant systems, devices, locations, and services.	■	■	■	■	
Reasonably anticipated threats and vulnerabilities affecting ePHI are identified and documented.	■	■	■	■	
Current security measures are assessed to determine whether they appropriately reduce identified risks.	■	■	■	■	
Risk management actions are documented and tracked to reduce risks and vulnerabilities to a reasonable and appropriate level.	■	■	■	■	

2. Assigned Responsibility, Workforce & Access Management

HIPAA Security readiness statement	Ready	Partial	Not Ready	N/A	Notes
A security official is designated with responsibility for developing and implementing Security Rule policies and procedures.	■	■	■	■	
Workforce access to ePHI is authorized according to role and business need.	■	■	■	■	
Processes exist to authorize, modify, and terminate access when workforce responsibilities change.	■	■	■	■	
Workforce members with access to ePHI receive appropriate supervision and access controls.	■	■	■	■	
Security responsibilities and sanctions for violations of security policies are documented and communicated.	■	■	■	■	

3. Security Awareness & Training

HIPAA Security readiness statement	Ready	Partial	Not Ready	N/A	Notes
All workforce members receive security awareness and training appropriate to their responsibilities.	■	■	■	■	
Training and awareness address relevant threats such as malicious software, suspicious activity, passwords, and social engineering.	■	■	■	■	
Security reminders or awareness activities are provided periodically.	■	■	■	■	
Training completion and related security-awareness activities are documented.	■	■	■	■	
Training content is reviewed and updated when risks, technology, or organizational practices change.	■	■	■	■	

4. Security Incident Procedures

HIPAA Security readiness statement	Ready	Partial	Not Ready	N/A	Notes
Policies and procedures exist to identify and respond to suspected or known security incidents.	■	■	■	■	
Personnel know how and where to report suspected security incidents involving ePHI.	■	■	■	■	
Incident response responsibilities, escalation paths, and key contacts are defined.	■	■	■	■	
Harmful effects of known security incidents are mitigated to the extent practicable.	■	■	■	■	
Security incidents and their outcomes are documented.	■	■	■	■	

5. Contingency Planning & Availability

HIPAA Security readiness statement	Ready	Partial	Not Ready	N/A	Notes
Procedures exist to create and maintain retrievable copies of ePHI needed for recovery.	■	■	■	■	
A disaster recovery process supports restoration of lost or unavailable ePHI.	■	■	■	■	
Emergency-mode procedures support continuation of critical business processes while protecting ePHI.	■	■	■	■	
Contingency plans and recovery procedures are tested or exercised periodically as reasonable and appropriate.	■	■	■	■	
Critical applications, data, dependencies, and recovery priorities are identified.	■	■	■	■	

6. Evaluation & Business Associate Arrangements

HIPAA Security readiness statement	Ready	Partial	Not Ready	N/A	Notes
Periodic technical and nontechnical evaluations assess whether security measures continue to meet Security Rule requirements.	■	■	■	■	
Evaluations are considered after environmental, operational, organizational, or technology changes that may affect ePHI security.	■	■	■	■	
Business associates that create, receive, maintain, or transmit ePHI are identified.	■	■	■	■	
Required written business associate agreements or other arrangements are maintained where applicable.	■	■	■	■	
Relevant business associate security responsibilities, incident expectations, and subcontractor obligations are addressed.	■	■	■	■	

7. Physical Safeguards

HIPAA Security readiness statement	Ready	Partial	Not Ready	N/A	Notes
Facility access controls limit physical access to electronic information systems and facilities containing ePHI while allowing authorized access.	■	■	■	■	
Workstation use expectations address appropriate functions, physical surroundings, and access to ePHI.	■	■	■	■	
Physical safeguards are used for workstations that access ePHI.	■	■	■	■	
Device and media controls address receipt, removal, movement, disposal, and reuse of hardware or electronic media containing ePHI.	■	■	■	■	
Accountability and data backup considerations are addressed before movement or disposal of devices/media when applicable.	■	■	■	■	

8. Technical Safeguards - Access & Authentication

HIPAA Security readiness statement	Ready	Partial	Not Ready	N/A	Notes
Technical access controls allow only authorized persons or software programs to access systems containing ePHI.	■	■	■	■	
Each user is assigned a unique identifier for tracking identity and system activity.	■	■	■	■	
Emergency access procedures provide necessary ePHI access during emergencies.	■	■	■	■	
Automatic logoff and encryption/decryption controls are evaluated and implemented when reasonable and appropriate, with decisions documented as required.	■	■	■	■	
Procedures verify that persons or entities seeking access to ePHI are who they claim to be.	■	■	■	■	

9. Technical Safeguards - Audit, Integrity & Transmission

HIPAA Security readiness statement	Ready	Partial	Not Ready	N/A	Notes
Hardware, software, and/or procedural mechanisms record and examine activity in systems that contain or use ePHI.	■	■	■	■	
Audit records or system activity are reviewed as part of ongoing security monitoring.	■	■	■	■	
Policies and procedures protect ePHI from improper alteration or destruction.	■	■	■	■	
Electronic mechanisms to corroborate that ePHI has not been improperly altered or destroyed are evaluated and implemented as appropriate.	■	■	■	■	
Technical security measures protect ePHI transmitted over electronic networks; integrity and encryption safeguards are evaluated and implemented as reasonable and appropriate.	■	■	■	■	

10. Policies, Documentation & Ongoing Review

HIPAA Security readiness statement	Ready	Partial	Not Ready	N/A	Notes
Reasonable and appropriate Security Rule policies and procedures are documented and implemented.	■	■	■	■	
Required Security Rule documentation, including actions and assessments that must be documented, is retained for the required period.	■	■	■	■	
Documentation is available to persons responsible for implementing the related procedures.	■	■	■	■	
Policies, procedures, and security documentation are periodically reviewed and updated in response to environmental or operational changes.	■	■	■	■	
Risk analysis and security management are treated as ongoing processes rather than one-time activities.	■	■	■	■	

HIPAA Security Readiness Summary

Use this page to document priority areas for follow-up. Do not interpret a percentage of Ready responses as a HIPAA compliance score. HIPAA Security Rule compliance depends on the entity's specific environment, applicable requirements, risk analysis, implementation decisions, documentation, and ongoing evaluation.

Priority Area	Gap / Observation	Owner	Target Date
1.			
2.			
3.			
4.			
5.			

Suggested Next Steps

1. Confirm that the scope of the organization's formal risk analysis includes all ePHI it creates, receives, maintains, or transmits.

2. Review Not Ready, Partial, and Unknown areas with the responsible security, privacy, compliance, operational, and technology stakeholders.

3. Document risks, implementation decisions, responsible owners, remediation actions, and target dates.

4. Validate that required policies, procedures, agreements, training records, incident records, and other supporting evidence are current and retained appropriately.

5. Reevaluate safeguards when material environmental, operational, organizational, threat, or technology changes occur.

Need a deeper HIPAA Security review?
CTRL The Future LLC can support HIPAA Security readiness and risk-assessment activities through evidence review, gap analysis, risk documentation, prioritized recommendations, and practical remediation planning.

Regulatory note: This checklist reflects the HIPAA Security Rule currently in effect as of September 2026. HHS has proposed modifications to strengthen the Security Rule; proposed provisions should not be represented as current requirements unless and until they become effective.

Disclaimer: This checklist is provided for general informational and readiness purposes only. It is not legal advice, a formal HIPAA risk analysis, an audit, regulatory certification, or a determination of HIPAA compliance. Organizations should evaluate the requirements and implementation specifications applicable to their circumstances.