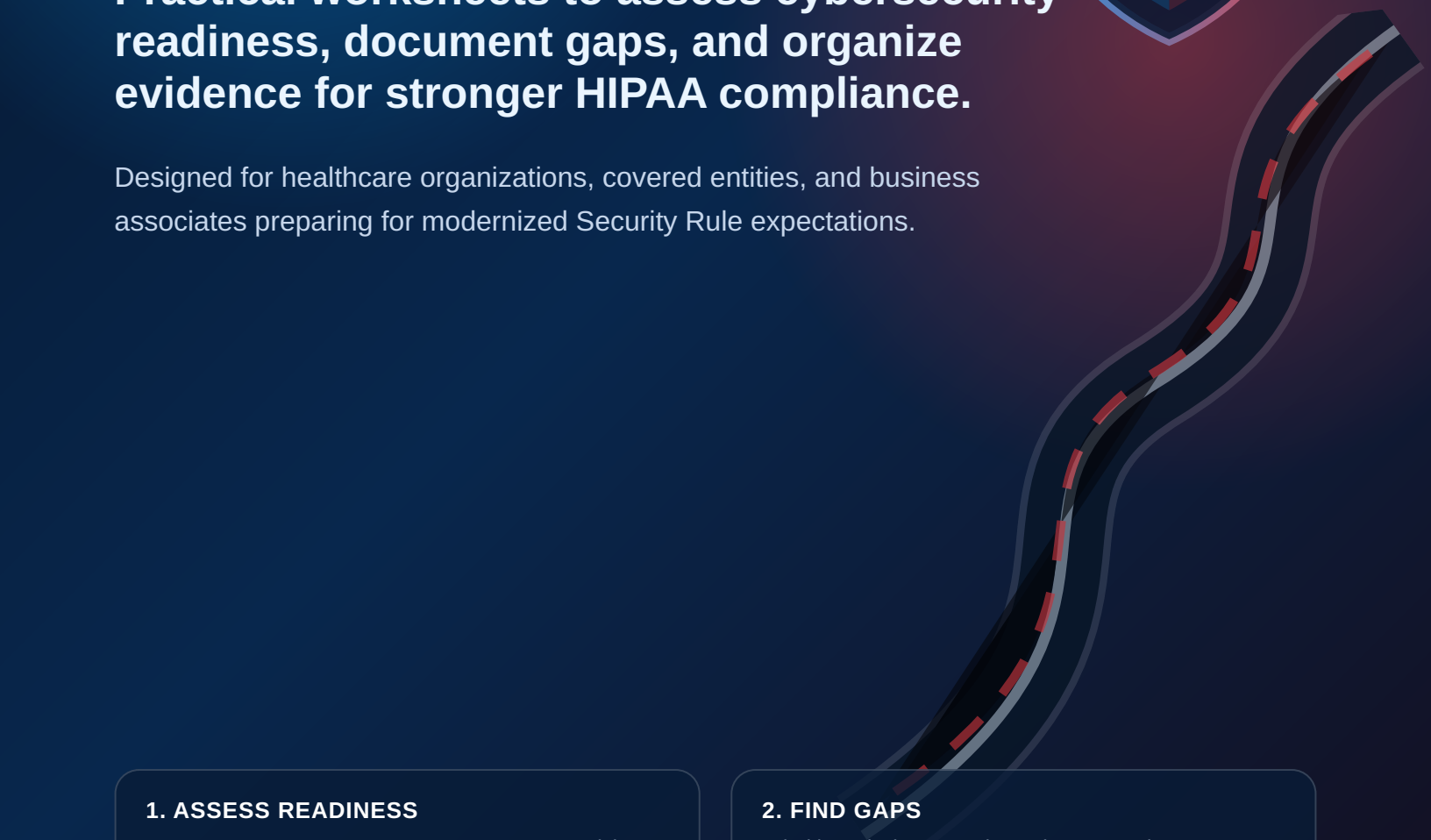
FREE HEALTHCARE COMPLIANCE ASSET

HIPAA 2.0 Readiness Toolkit

Practical worksheets to assess cybersecurity readiness, document gaps, and organize evidence for stronger HIPAA compliance.

Designed for healthcare organizations, covered entities, and business associates preparing for modernized Security Rule expectations.



1. ASSESS READINESS

Score your current posture across governance, risk, assets, vendors, documentation, and response.

2. FIND GAPS

Prioritize missing controls, undocumented processes, and evidence gaps that could slow an audit or investigation.

3. BUILD EVIDENCE

Collect risk analysis, policies, asset inventories, BAAs, logs, training, and incident response records.

4. PLAN NEXT STEPS

Turn checklist results into a 30/60/90-day action plan for stronger compliance and resilience.

Prepared June 2026 | HIPAA 2.0 is an informal shorthand for Security Rule modernization readiness, not an official rule title.

START HERE

How to Use This HIPAA 2.0 Readiness Toolkit

Use this asset as a practical working document. It is not legal advice and it is not a substitute for a formal HIPAA Security Rule risk analysis, but it can help you organize readiness work before an audit, vendor review, or security incident.

Important positioning note

"HIPAA 2.0" is used here as market shorthand for preparing for proposed modernization of the HIPAA Security Rule and stronger cybersecurity expectations for electronic protected health information (ePHI). At the time this toolkit was prepared, HHS/OCR had issued a Notice of Proposed Rulemaking, and the current HIPAA Security Rule remains in effect.

ORGANIZATION _____ PREPARED BY _____

REVIEW DATE _____ REVIEW PERIOD _____

Fast pass: 60-minute review

1. Complete the readiness scoring worksheet.
2. List your highest-risk ePHI systems and vendors.
3. Identify the top five gaps needing executive attention.
4. Assign an owner and due date to each gap.

Deep pass: 1-week working session

1. Validate the asset inventory and data flow map.
2. Update risk analysis and risk treatment notes.
3. Collect evidence for policies, training, BAAs, access reviews, and response plans.
4. Run a tabletop exercise and document lessons learned.

Readiness score key

0	Not documented, not assigned, or unknown.
1	Partially documented, but inconsistent or incomplete.
2	Implemented with some gaps or outdated evidence.
3	Implemented, tested, current, and evidence-ready.

Toolkit contents

HIPAA 2.0 Readiness Assessment Worksheet | Risk Analysis & Gap Assessment Template | PHI Asset Inventory Checklist | Vendor & Business Associate Review Guide | Incident Response Preparedness Checklist | Documentation & Audit Readiness Tracker

WORKSHEET 1

HIPAA 2.0 Readiness Assessment Worksheet

Score each domain from 0 to 3. Use the total score to prioritize follow-up work, not to claim compliance. Focus on whether controls are current, tested, and supported by evidence.

Readiness domain	What good looks like	Score	Owner	Next action
Governance & accountability	Security responsibility is assigned; HIPAA policies are written, reviewed, and approved; leadership receives security risk visibility.			
Risk analysis & risk management	Risk analysis covers all ePHI; risks have ratings, owners, treatment decisions, due dates, and documented remediation.			
PHI/ePHI asset inventory	Systems, devices, applications, cloud services, data stores, and data flows that create, receive, maintain, or transmit PHI are documented.			
Access management	Access is based on role and minimum necessary principles; privileged access is controlled; periodic access reviews and termination procedures are documented.			
Technical safeguards	Unique user IDs, authentication, encryption where appropriate, audit logging, vulnerability management, endpoint protection, and backup protections are implemented.			
Physical safeguards	Facilities, workstations, devices, media, and printed PHI are protected through defined access, storage, disposal, and visitor controls.			
Workforce training	Security awareness, phishing, privacy practices, incident reporting, sanctions, and role-specific training are assigned and tracked.			
Vendor & BA oversight	Business Associate Agreements are current; vendor security posture is reviewed; incident reporting and subcontractor expectations are documented.			
Incident response & resilience	Incident response, breach assessment, backup restoration, contingency operations, and communications plans are documented and tested.			
Documentation & audit readiness	Policies, procedures, risk analysis, training records, BAAs, access reviews, and incident documentation are stored in an organized evidence library.			

0-10: High exposure

Begin with risk analysis, asset inventory, and evidence collection. Assign executive accountability immediately.

11-22: Building maturity

Prioritize high-risk gaps, outdated documentation, vendor reviews, and incident response testing.

23-30: Evidence-ready

Validate controls, test assumptions, refresh evidence, and prepare for independent review.

WORKSHEET 1 CONTINUED

Detailed Control Readiness Checklist

Use this page to confirm whether each readiness item has a clear owner and evidence. Items below are practical readiness prompts and should be evaluated against your organization's HIPAA obligations and risk profile.

Readiness item	Evidence to gather	Status	Notes / owner / due date
Security officer or responsible security function is assigned.	Role description, committee charter, leadership reporting record.	☐ Ready ☐ Gap	
HIPAA security policies and procedures are current.	Approved policies, review dates, change history, workforce acknowledgment.	☐ Ready ☐ Gap	
Risk analysis includes all systems containing ePHI.	Risk analysis report, asset list, threats, vulnerabilities, risk ratings.	☐ Ready ☐ Gap	
Risk management plan tracks remediation.	Risk register, treatment decisions, owners, due dates, closure evidence.	☐ Ready ☐ Gap	
Asset inventory and data flows are documented.	Inventory, diagrams, PHI data locations, cloud/ SaaS list, network maps.	☐ Ready ☐ Gap	
Unique user IDs and access reviews are enforced.	IAM reports, access review signoffs, joiner/mover/ leaver procedures.	☐ Ready ☐ Gap	
Administrative and privileged access is controlled.	Admin inventory, MFA settings, break-glass process, approval records.	☐ Ready ☐ Gap	
Encryption, logging, and monitoring are defined for ePHI systems.	Encryption configuration, log retention settings, SIEM/alert records.	☐ Ready ☐ Gap	
Backups are protected and restoration is tested.	Backup policy, restore test results, immutable/ offline backup evidence.	☐ Ready ☐ Gap	
Security awareness and incident reporting training is tracked.	Training roster, completion reports, phishing test results, sanctions policy.	☐ Ready ☐ Gap	
Business Associate Agreements and vendor reviews are current.	Executed BAAs, vendor risk assessments, security reports, review schedule.	☐ Ready ☐ Gap	
Incident response and breach processes are tested.	IR plan, breach assessment workflow, tabletop records, lessons learned.	☐ Ready ☐ Gap	

TEMPLATE 2

Risk Analysis & Gap Assessment Template

Use this template to connect risk analysis findings to remediation work. A strong risk analysis should identify where ePHI exists, what could threaten it, which safeguards are already in place, and what residual risk remains.

Risk analysis prompts

- [ ] What systems create, receive, maintain, or transmit ePHI?
- [ ] What threats could affect confidentiality, integrity, or availability?
- [ ] Which vulnerabilities increase likelihood or impact?
- [ ] What safeguards are currently operating?
- [ ] What residual risk remains after safeguards?

Scoring approach

Likelihood x Impact = Risk Score. Use a 1-5 scale for both likelihood and impact. Risks with high impact on patient care, ePHI exposure, ransomware resilience, or regulatory response should receive priority treatment.

Tip: Record accepted risk decisions formally. Do not leave high risks unassigned.

Asset / process	Threat	Vulnerability	Current safeguards	L	I	Score	Treatment plan	Owner	Due

Top 5 priority gaps			
Gap	**Why it matters**	**Immediate next step**	**Target date**
1.			
2.			
3.			
4.			
5.			

CHECKLIST 3

PHI Asset Inventory Checklist

Document every system, application, device, database, storage location, service provider, and workflow that creates, receives, maintains, or transmits PHI or ePHI.

Include these asset types

- [ ] EHR/EMR platforms
- [ ] Billing systems
- [ ] Cloud storage
- [ ] Email/messaging
- [ ] Endpoint devices
- [ ] Medical devices
- [ ] Backups
- [ ] Paper records
- [ ] File shares
- [ ] APIs/integrations

Capture these attributes

- [ ] System owner
- [ ] PHI data type
- [ ] Hosting location
- [ ] Vendor/BA involved
- [ ] Access groups
- [ ] Encryption status
- [ ] Logging coverage
- [ ] Backup status
- [ ] Retention period
- [ ] Criticality

Asset / system	Owner	PHI/ePHI type	Location / hosting	Vendor / BA	Access groups	Encryption	Logging / backup	Risk notes

Tip: Inventory should include assets managed by third parties if the asset stores, processes, transmits, or provides access to PHI/ePHI.

CHECKLIST 3 CONTINUED

PHI Data Flow & Access Review

A useful inventory shows more than system names. It explains how PHI moves, who can access it, and where controls should prevent unauthorized use or disclosure.

PHI source	Transmission method	Destination	PHI data elements	Security controls	Retention	Owner	Notes

MINIMUM ACCESS REVIEW PROMPTS

- [ ] Do workforce members have access only to systems needed for their role?
- [ ] Are privileged accounts named, approved, and protected?
- [ ] Are inactive accounts disabled promptly?
- [ ] Are terminated users removed from all PHI systems?
- [ ] Are shared accounts prohibited or tightly controlled?
- [ ] Are access reviews documented at least periodically?

ACCESS REVIEW WORKING TABLE

Role / group	Systems	Last reviewed	Changes needed

GUIDE 4

Vendor & Business Associate Review Guide

Business associates and vendors can create meaningful risk if they store, process, transmit, support, or can access PHI. Use this guide to verify contracts, security controls, incident obligations, and evidence.

Review triggers

- [ ] New vendor with PHI access
- [ ] New integration or data exchange
- [ ] Renewal or contract change
- [ ] Security incident or breach notification
- [ ] Material change in hosting, subcontractors, or geography

Evidence to request

- [ ] Executed BAA and security addendum
- [ ] Security questionnaire or assessment
- [ ] Independent audit report or attestation, where available
- [ ] Incident response and notification commitments
- [ ] Data return, deletion, and offboarding terms

Vendor / BA	Service provided	PHI access?	BAA on file?	Criticality	Last review	Controls verified	Next step

GUIDE 4 CONTINUED

Business Associate Due Diligence Questions

Use these prompts during vendor intake, renewal, or annual review. The goal is to understand whether the vendor's controls align with the sensitivity and criticality of the PHI involved.

- Is there a signed Business Associate Agreement before PHI is shared?
- What PHI/ePHI will the vendor create, receive, maintain, or transmit?
- Where is data hosted, backed up, replicated, and archived?
- Does the vendor use subcontractors who may access PHI?
- How is PHI encrypted in transit and at rest?
- How is administrative access approved, monitored, and removed?
- Does the vendor enforce MFA for administrative and remote access?
- What logs are retained and for how long?
- What vulnerability management and patching practices are in place?
- What independent reports, attestations, or certifications can be provided?
- How quickly must the vendor notify your organization of a security incident?
- What support will the vendor provide for breach assessment and investigation?
- How does the vendor test backups and disaster recovery capabilities?
- What data return, deletion, or destruction process is available at termination?
- Are contractual obligations aligned with your incident response timeline?
- Who owns vendor risk acceptance decisions?

Question / concern	Vendor response	Evidence received	Risk decision / owner

CHECKLIST 5

Incident Response Preparedness Checklist

A written plan is only useful if people know their roles, alerts are triaged quickly, decisions are documented, and recovery has been tested.

PREPAREDNESS CHECKLIST

- [ ] Incident response plan is current and approved.
- [ ] Privacy, security, legal, IT, and executive contacts are listed.
- [ ] Incident intake process is clear to workforce members.
- [ ] Severity levels and escalation paths are documented.
- [ ] Containment, eradication, and recovery steps are defined.
- [ ] Evidence preservation and forensic support are considered.
- [ ] Breach assessment workflow is documented.
- [ ] Vendor incident notification obligations are known.
- [ ] Backup restoration has been tested.
- [ ] Tabletop exercises are performed and tracked.

COMMON INCIDENT CATEGORIES

Category	Examples	Review owner
Security incident	Malware, phishing, unauthorized access attempt, lost device.	
Privacy incident	Misdirected email, improper disclosure, snooping concern.	
Potential breach	Unauthorized access, use, acquisition, or disclosure of PHI requiring assessment.	
Vendor incident	Business associate outage, data exposure, ransomware, subpoena issue.	

Role	Primary contact	Backup contact	Responsibilities	Notes
Incident commander			Coordinate response, decisions, timeline.	
Security lead			Containment, logging, forensic preservation.	
Privacy / compliance			PHI assessment, documentation, breach review.	
Legal counsel			Privilege, notification, regulatory questions.	
IT operations			System recovery, backups, endpoint support.	
Communications			Internal/external messaging approvals.	
Vendor liaison			Coordinate with business associates and partners.	

CHECKLIST 5 CONTINUED

Breach Preparedness & Tabletop Tracker

Use this page to test decision-making before a real incident occurs. Capture what happened, what evidence was reviewed, and what actions were assigned.

Simple decision workflow

Suspected incident -> determine whether PHI/ePHI may be involved -> preserve evidence -> contain and investigate -> assess unauthorized access, use, acquisition, or disclosure -> involve privacy/legal review -> document risk assessment and notification decisions -> complete corrective actions.

Exercise date	Scenario tested	Participants	Gaps identified	Action owner	Due date

Evidence to preserve

- [ ] Alert records and security logs
- [ ] Timeline of discovery, containment, and recovery
- [ ] Screenshots, email headers, file hashes, or forensic artifacts
- [ ] Systems, users, patients, or records potentially affected
- [ ] Vendor notifications and support records
- [ ] Risk assessment and decision documentation

Recovery validation

- [ ] Known-good backups identified
- [ ] Restore process tested
- [ ] Credentials reset where needed
- [ ] Vulnerabilities patched or mitigated
- [ ] Monitoring rules updated
- [ ] Lessons learned assigned and tracked

TRACKER 6

Documentation & Audit Readiness Tracker

Collect evidence as you go. Audit readiness depends on being able to show policies, procedures, implementation records, and review history without rebuilding the story under pressure.

Evidence item	Owner	Storage location	Last reviewed	Status	Notes / next action
HIPAA Security Rule policies and procedures				☐	
Risk analysis report				☐	
Risk management plan / risk register				☐	
PHI/ePHI asset inventory				☐	
Data flow diagrams and network diagrams				☐	
Access control procedures and access review records				☐	
Workforce training records and security awareness evidence				☐	
Business Associate Agreements				☐	
Vendor risk reviews and security evidence				☐	
Incident response plan and breach assessment workflow				☐	
Tabletop exercise and lessons learned records				☐	
Contingency plan, backup plan, and restore test results				☐	
Audit logs, monitoring rules, and alert response records				☐	
Device, media, workstation, and facility control procedures				☐	

Status key: blank = not reviewed | check box = evidence exists and is current | use notes to record outdated, missing, or owner-required items.

ACTION PLANNING

30/60/90-Day Readiness Roadmap

Translate the worksheet results into a practical plan. Start with visibility, then close control gaps, then validate evidence and response readiness.

First 30 days

30

- Assign readiness owner and executive sponsor.
- Complete scoring worksheet.
- Identify top 5 risk gaps.
- Inventory critical ePHI systems and vendors.
- Collect current BAAs and core policies.

Next 60 days

60

- Update risk analysis and treatment plan.
- Validate access reviews and privileged accounts.
- Review vendor evidence for critical BAs.
- Close quick-win control gaps.
- Test backup restore for critical systems.

By 90 days

90

- Run incident response tabletop.
- Refresh evidence library.
- Review readiness with leadership.
- Validate high-risk remediation.
- Schedule an independent readiness review.

Priority action	Risk level	Owner	Due date	Success evidence
1.				
2.				
3.				
4.				
5.				

Next step

Use the completed toolkit to brief leadership, prioritize remediation, and prepare for a deeper HIPAA readiness review. The strongest programs can show not only that controls exist, but that they are current, tested, and supported by evidence.

REFERENCES & DISCLAIMER

Sources, Scope & Disclaimer

This asset is intended to support readiness conversations. It does not determine compliance, replace counsel, or guarantee audit outcomes.

Scope of this toolkit

This toolkit focuses on security readiness for PHI/ePHI protection, risk analysis, asset visibility, vendor oversight, incident preparedness, and documentation. It should be tailored to your organization, legal obligations, risk profile, technology environment, and operational responsibilities.

Use this checklist to

- [ ] Prepare for a structured readiness review.
- [ ] Identify missing documentation and evidence.
- [ ] Prioritize security remediation work.
- [ ] Improve incident response and vendor oversight.

Do not use it to

- [ ] Claim formal HIPAA compliance by itself.
- [ ] Replace legal advice or regulatory interpretation.
- [ ] Ignore organization-specific risk analysis.
- [ ] Delay required breach or regulatory obligations.

PUBLIC SOURCES CONSULTED

1. U.S. Department of Health and Human Services, Office for Civil Rights: HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information. https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/index.html
2. HHS/OCR Fact Sheet: HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information. https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html
3. Federal Register: HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information, 90 FR 898, January 6, 2025. https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information
4. HHS/OCR: The Security Rule. https://www.hhs.gov/hipaa/for-professionals/security/index.html
5. HHS/OCR: Guidance on Risk Analysis. https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html