CLEARDATA®

Scaling Securely: Preparing for 2026 Compliance Changes

Healthcare's Roadmap to HIPAA & HITRUST Updates and Governing AI Risk in the Next Era of Data Security

Executive Letter from Chris Bowen, Founder & CISO, ClearDATA

Healthcare is entering an inflection point as regulatory requirements evolve at an accelerating pace. By 2026, multiple proposed changes to HIPAA's Security and Privacy Rules, along with tighter HITRUST expectations (especially as they tie into interoperability and vendor assurance), are slated to become the new baseline.

At the same time, new regulations and assurance frameworks are beginning to address the risks of AI in healthcare, further expanding the compliance landscape. For CIOs, CISOs and Compliance Officers, this forecast should feel urgent, but it should also feel actionable.

From our view here at ClearDATA, we see three realities every healthcare organization must face:

1. **Regulations are catching up to threat reality;** Increasing regulatory demands around AI, data access, incident response, audit logging, vendor accountability, and technical controls (e.g. MFA, encryption, asset inventories) reflect what adversaries are already exploiting.

2. **Scaling magnifies risk exponentially;** As you add more cloud services, APIs, endpoints, partners, and hybrid environments, each adds possible gaps. Without robust visibility, automated, policy enforcement, and risk assessment, those gaps multiply.

3. Proactivity is non-negotiabl; Waiting for finalized rules is risky; organizations that align early will have smoother transitions, lower remediation costs, and less reputational exposure.

Ultimately, compliance is not just about regulation, it is about keeping patient trust. Every security gap that leads to downtime, breach, or regulatory penalty undermines confidence in the healthcare system itself. Protecting patient data is protecting patient care.

In this guide, we share what we know now about upcoming HIPAA & HITRUST changes, how AI-related regulations are beginning to influence security and compliance expectations, and exactly how to begin preparing. ClearDATA has built our tools and services with these evolving requirements in mind; we're ready to help you make compliance a source of strength, not a barrier to innovation.

Now is the moment to act.

Chris Bowen
Founder & Chief Information Security Officer, ClearDATA

Why Proactive Compliance is Healthcare's Only Option

The next 18–24 months are sure to be a quickly closing window for healthcare organizations. New HIPAA and HITRUST requirements aren't incremental, They represent a fundamental shift in how regulators expect covered entities and business associates to prove and demonstrate compliance.

In addition to HIPAA and HITRUST updates, federal regulators are also codifying requirements around AI in healthcare. These transparency rules are fluid and emerging. The ONC HTI rules, which update the Health IT Certification Program and information blocking framework, are designed to strengthen interoperability, algorithm transparency, and reporting requirements for certified health IT. The ONC's HTI-1 final rule, still in early-stage development, introduces new transparency and labeling requirements for AI and algorithmic decision-support features in certified health IT. These provisions underscore that compliance expectations now extend beyond traditional data security into the governance of emerging technologies.

Delaying your healthcare organization's preparedness until final rules are published would mean scrambling to retrofit controls, renegotiate contracts, and remediate risks under the pressure of a rapidly ticking clock. Forced into reactive mode, gaps inevitably emerge, such as missed access terminations, incomplete audit logs, and untested incident response plans that adversaries and regulators alike can unravel, or worse, quickly exploit.

We know from watching the news how steep the consequences of waiting for preparedness can be.

- In the last several years, the average cost of a healthcare data breach in 2025 is $7.42breach **range from $7 to $10 million**, and healthcare accounts for the highest average breach cost among industries for the 14th consecutive year.
- According to the Compliancy Group's HIPAA fines directory, the 2025 total to date of public HIPAA settlements and civil penalties is over $6.5 million — and while this likely underrepresents the full enforcement total (some fines may not yet be publicly disclosed), it underscores the considerable regulatory exposure already manifesting this year.

Healthcare is uniquely exposed. Cloud adoption, telehealth platforms, AI-driven diagnostics and decision-support tools, and remote engagement tools have become core to care delivery. Yet every new endpoint, API, or vendor integration expands the scope of the compliance surface area. What was once manageable through static, annual audits are no longer sustainable.

Bottom line: Scaling healthcare services without modernizing compliance is a recipe for risk. Organizations that act now will reduce regulatory exposure, and strengthen their reputation as trusted care providers.

Common Risks When Preparation Is Delayed

- **AI risk oversight:** Algorithms and AI-enabled services may introduce bias, privacy risk, or opaque decision-making. Under HITRUST v11 and ONC HTI rules, organizations will be expected to demonstrate governance and assurance for AI systems that interact with PHI.
- **Shadow cloud services:** A hospital group expands telehealth and remote diagnostics, leveraging SaaS vendors. Without an asset inventory or network map, PHI may flow through systems outside of oversight, lacking MFA, encryption, or vendor contracts consistent with new standards.
- **Delayed access revocation:** A staff turnover process is slow; old credentials persist, offering unauthorized access. Under proposed HIPAA updates, access must be terminated "as soon as possible, but no later than one hour" after termination of employment.

- **Incident response gaps:** Inadequate documentation and testing of response plans could result in failing an audit, or worse: a breach, regulatory fines, and reputational damage.
- **Contract & vendor oversight issues:** When partners (business associates, subcontractors) don't meet new expectations for notification, backups, or risk management, you inherit their vulnerabilities and liability.

These scenarios are not hypothetical. The Office for Civil Rights (OCR) has repeatedly cited organizations for insufficient or non-existent risk analyses, failure to implement MFA, and weak access controls. Enforcement actions are becoming more frequent, and regulators are signaling even higher expectations moving into 2026.

The message is clear: Compliance is no longer a periodic exercise, It must be built into daily operations. Healthcare organizations that take a proactive stance today will spend less, avoid disruption, and protect both patients and reputation when the new rules take effect.

What's Changing in HIPAA & HITRUST (2026 and Beyond)

At a Glance: Why 2026 Matters

- **20+ years outdated:** The HIPAA Security Rule has not been significantly updated since 2003; the new NPRM modernizes safeguards for today's cloud and cyber threat environment.
- **Addressable no more:** Requirements that were once flexible "addressable" specs (e.g., MFA, encryption, asset inventories) will become mandatory for all covered entities and business associates.
- **Audit expectations rising:** Regulators are emphasizing continuous documentation, tested incident response, and tamper-proof audit logs—moving away from "point-in-time" compliance.
- **HITRUST evolves with AI & interoperability:** CSF v11 introduces tighter alignment with CMS and interoperability frameworks, plus new control domains for AI risk, vendor assurance, and a mapping to ISO/IEC 23894 (the global AI risk management standard).
- **Regulatory workload will rise:** HHS estimates covered entities will spend an additional 14 hours annually per safeguard on documentation under the new rules (HHS NPRM Fact Sheet).

Bottom line: By 2026, healthcare organizations will need to demonstrate not just compliance policies, but verifiable operational maturity across IT, security, and vendor ecosystems.

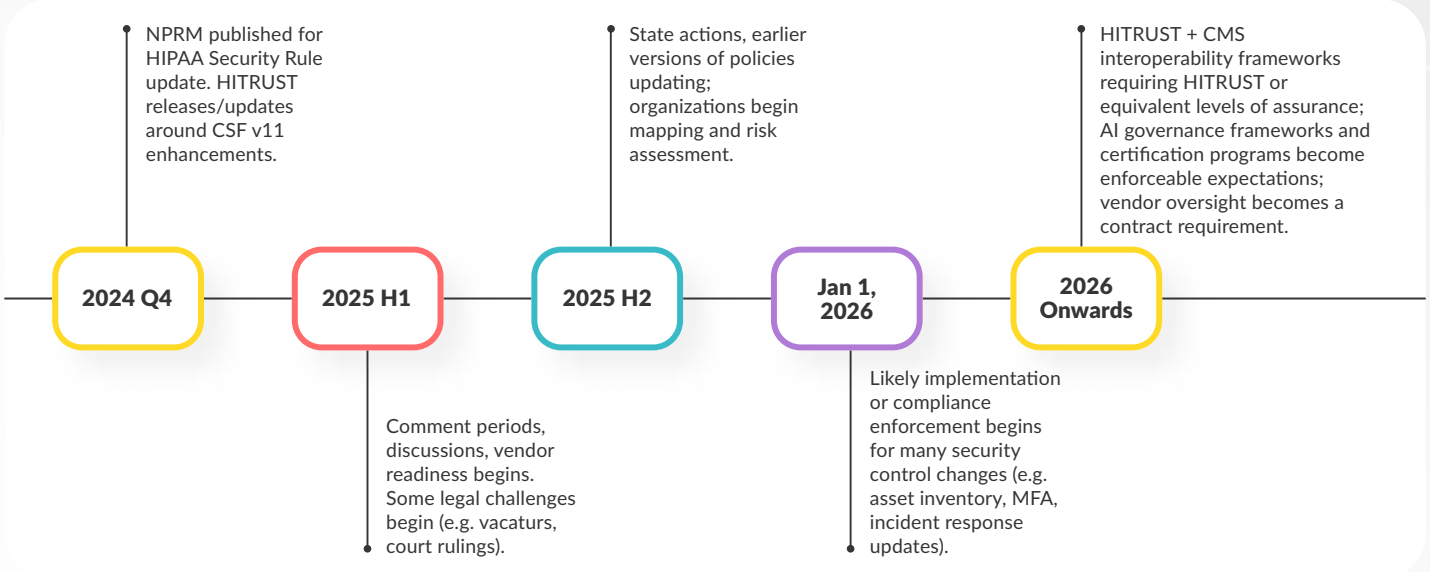
The table below outlines the most significant changes expected between now and 2026, and their implications for healthcare organizations. Some are not yet final, but many have high likelihood based on Notices of Proposed Rulemaking (NPRMs), legal rulings, and related guidance.

Today vs. 2026: Key Requirement Changes

Area	Today's Requirement	2026+ Requirement	Implications
Safeguard Categories	"Required" vs. "Addressable" controls. Addressable = flexible.	Nearly all safeguards become required with limited exceptions.	Organizations will likely need to implement previously addressable controls.
Asset Manageent	No explicit mandate for inventories or mapping.	Mandatory asset inventories and data flow mapping for all ePHI systems, updated annually or after changes.	Requires tooling and ongoing updates.
Access Termination	Termination policies required, no strict timeline.	Access revocation within one hour of workforce termination.	Requires automation and HR/IT integration.
Incident Response	Policies and plans required, but detail varies.	Formal contingency, DR, and criticality analysis documentation and testing required.	Must run annual tests and maintain evidence.
Encryption & MFA	"Addressable" organizations decide if reasonable.	Mandatory MFA for remote/ internet-facing ePHI systems; encryption at rest and transit required.	Tech upgrades likely for many orgs.
Audit Readiness	Documentation required, but audits often point-in-time.	Continuous documentation and audit logs expected, tamper-proof and retrievable.	Elevates audit readiness from event to ongoing state.
HITRUST CSF v11	Certification optional, scope-limited.	New control domains: interoperability, vendor risk, AI governance.	Raises bar for organizations participating in exchanges or using AI.

For a detailed view of these changes, see **Appendix A**, and for a practical roadmap on how your organization can plan compliance readiness initiatives in advance of these changes, see **Appendix B**.

Timeline of Key Regulatory & Standard Changes



Building a Proactive Compliance Program: Your Roadmap to 2026

Preparing for HIPAA and HITRUST changes is not a one-time compliance project—it's an ongoing program of governance, technology, and cultural alignment. Organizations that treat compliance as a continuous operational discipline will be best positioned to avoid disruption, reduce costs, and protect patient trust.

The coming 18–24 months will demand more than just updates to policies and systems. CIOs and Compliance Officers must build programs that anticipate regulatory shifts, integrate AI risk considerations, and ensure vendor ecosystems meet rising assurance requirements.

Key priorities for CIOs and Compliance Officers:

- Translate complex requirements into clear, actionable tasks for internal teams.
- Prioritize high-impact controls that address the most significant risks first.
- Assign ownership across IT, Compliance, Security, and Legal to avoid gaps.
- Create repeatable structures for monitoring, audit readiness, and continuous assurance.

The preparation checklist and policy/control gap matrix below are designed as practical tools to help you operationalize compliance readiness—not just once, but quarter after quarter as regulations evolve.

Preparation Checklist

Area	Action Item	Owner(s)	Ideal completion timeline
Governance & Policy	Inventory current policies vs. proposed HIPAA Security Rule specifications; mark which "addressable" ones are now likely required.	Compliance Officer + Legal + Policy Team	Within next 30 days
	Review business associate agreements (BAAs) and vendor contracts for incident response, notification timeframes, termination clauses, backup/ disaster recovery, data flow visibility.	Legal + Vendor Management	60 days
Technical Controls	Implement or strengthen MFA for all access to ePHI, especially remote or internet-facing systems.	IT / Security	90 days
	Build / update asset inventory: technology assets, systems that create, receive, store, transmit ePHI. Update inventory at least annually / after any infrastructure change.	IT / Security Ops	60-90 days
	Create / maintain network / data flow maps that show where ePHI goes (internal, external, cloud, partner).	Security Architecture	90 days
	Evaluate encryption standards, ensure encryption at rest & in transit for ePHI; review supported protocols.	Security + Infrastructure	120 days
	Review workforce access controls: role-based access, least privilege, timely revocation of access; ensure automated mechanisms for access termination.	HR + IT + Security	60 days
	Perform vulnerability scans at least semiannual + penetration tests at least annually; assess network segmentation; remove or mitigate unsupported software.	Security / Ops	120 days
Incident Response & Continuity	Update incident response plan: include detection, notification, mitigation, documentation, for both covered entities and business associates. Test / review annually.	Security / Compliance	90 days
	Perform criticality analysis: identify which systems/assets are essential for patient care / business continuity; plan disaster recovery and backups accordingly, with specified RTO (recovery time objective).	IT + Security + Business Continuity	120 days
Risk Assessment & Audit Readiness	Conduct a full Security Risk Assessment (SRA) that covers proposed HIPAA changes: definitions, threats and vulnerabilities, external vendors, and risks introduced by AI-enabled systems (decision support, automation,predictive analytics).	Security + Compliance + External Consultant	90-120 days
	Prepare for more frequent / formal audits; establish internal audit schedule; gather documentation: network maps, policies, training records, incident logs	Compliance / Audit	60 days
HITRUST & Vendor / Partner Engagement	Map existing controls to HITRUST CSF v11; identify gaps; plan for control updates	HITRUST / Security Team	120 days
	Implement or upgrade third-party risk management (TPRM) tooling; ensure vendor assurances, continuous monitoring, validated assessment reports. If using or procuring AI-enabled solutions that handle PHI, determine whether a HITRUST AI Security Assessment or Certification is appropriate and plan accordingly.	Vendor Management + Security	90-120 days
	If participating in health information exchanges or under CMS frameworks, verify whether HITRUST or equivalent assurance will be required; plan certification or re-certification path.	CIO + Compliance	120 days

Template: Policy / Control Gap Matrix

Below is a simplified gap matrix template you can use to track where you are today versus where proposed changes require you to be.

Control / Requirement	Current Status (Y/N)	Evidence / Documentation Location	Gap Severity (High / Medium / Low)	Owner	Remediation Planned Completion
Asset inventory & network mapping					
MFA for all remote / internet-facing access to ePHI					
Written incident response plan & annual testing					
Encryption in transit & at rest					
Role-based access, role changes,					
Asset inventory & network mapping					
MFA for all remote / internet-facing access to ePHI					
Written incident response plan & annual testing					
Encryption in transit & at rest					
Role-based access, role changes,					

Choose the Right Compliance Readiness Partner for Healthcare

Successfully navigating the 2026 HIPAA and HITRUST changes will require more than just internal effort. Most organizations will need a partner who can provide the scale, specialization, and foresight that's difficult to maintain in-house. The right partner not only supplies tools and services but also
brings healthcare-specific expertise and a proven ability to adapt to shifting regulatory landscapes.

Use this checklist to evaluate cloud partners against the most important criterion for compliance readiness.

Partner Readiness Evaluation Quick Checklist

Automated Control Enforcement	Enforcement of safeguards such as MFA, encryption, endpoint protection, and vulnerability management across multi-cloud environments.	☐ Yes ☐ No
Continuous Visibility & Mapping	Dashboards that track asset inventories, ePHI flows, and network maps, with alerts for configuration drift or missing controls.	☐ Yes ☐ No
Vendor & Partner Risk Orchestration	Integrated tools to oversee third-party risk, contract obligations, monitoring, and documentation to reduce exposure from business associates.	☐ Yes ☐ No
Audit Readiness & Documentation	Pre-built templates, policy libraries, and incident response playbooks; preservation of logs and audit trails to streamline HIPAA and HITRUST reviews.	☐ Yes ☐ No
Expert Guidance & Threat Intelligence	Ongoing monitoring of regulatory changes, threat landscape, and AI/ML risks to ensure proactive compliance.	☐ Yes ☐ No
Healthcare-Specific Expertise	Exclusive healthcare focus, familiarity with PHI workflows, and understanding of clinical and operational realities.	☐ Yes ☐ No
Proven HITRUST & HIPAA Competency	Demonstrated track record aligning with both frameworks; able to support certification efforts and withstand regulatory scrutiny.	☐ Yes ☐ No

Want to rate several different partners to help make your choice? Use our Cloud Compliance Partner Evaluation Matrix (Appendix C) to score potential partners for HIPAA/HITRUST Readiness.

Preparing for the Future of Healthcare Compliance

2026 will most certainly not be the finish line. Consider this the starting point of a new compliance era. Healthcare organizations will face continuous oversight, stricter enforcement, and emerging requirements for AI, global data governance, and patient access rights.

If you act now, you'll do more than simply check the HIPAA and HITRUST compliance boxes—you'll:

- **Reduce financial and operational risk** by avoiding costly breaches, fines, and last-minute remediation.
- **Build lasting resilience** across a complex vendor and cloud ecosystem, ensuring continuity even as threats evolve.
- **Earn and protect patient trust** by demonstrating that security and compliance are core to care, not an afterthought.

Don't wait until 2026. Start now—close gaps, build resilience, and turn compliance into a competitive advantage.

Here are three steps to start now:

1. **Conduct a Compliance Readiness Review** — Assess your current state against what's likely coming; map risk, define gaps, and prioritize remediation.
2. **Establish a Cross-Functional HIPAA/HITRUST Working Group** — Align IT, Security, Legal, Vendor Management, and Compliance leaders on priorities and timelines.
3. **Pilot Your Most Critical Controls First** — Begin with high-impact safeguards such as MFA, asset mapping, incident response, and vendor contract clauses. Demonstrating early wins builds organizational momentum and reduces risk.

Get ahead of compliance changes now. Schedule your **Compliance Readiness Review** and our experts will assess your current state, identify gaps, and create a roadmap to ensure your organization scales securely, stays compliant, and avoids risk, cost, and reputational damage.

Talk to a healthcare cloud expert

See how ClearDATA can accelerate your cloud, streamline your operations, and extend your staff.

CLEARDATA®

SPEAK WITH AN ADVISOR

sales@cleardata.com

Appendix A: The Details of HIPAA and HITRUST Changes for 2026

Change Area	What's Proposed or Happening	Implications for Organizations
HIPAA Security Rule Update (OCR NPRM, Jan. 2025)	• Remove "addressable" vs "required" distinction: almost all implementation specs become required with limited exceptions (HHS.gov fact sheet). • Stronger documentation: all policies, procedures, plans, and analyses must be in writing (HHS.gov). • Asset inventory & network mapping requirement: organizations must maintain an inventory of technology assets and map flows of ePHI throughout systems, updated at least annually or when environments change (HHS.gov). • Expanded definitions of "information systems," threat, risk, and vulnerability; clarification of what counts as "relevant electronic information systems" (Epstein Becker Green analysis). • Mandatory multi-factor authentication (MFA) in more cases; stronger encryption; more frequent risk assessment; better workforce access and termination policies (Axonius blog). • New contingency and incident response specifications: disaster recovery, backups, and criticality analysis must be documented and tested (HHS.gov fact sheet).	• Organizations will need to inventory all relevant systems, document flows of ePHI, and map dependencies across providers, cloud / partner services. • Policies that were previously "addressable" must be turned into formal, required controls—may require new governance & technical investments. • IAM, MFA, termination, access review practices will need tightening. • Incident response, backup strategy, critical system prioritization will need testing, documentation, and capacity to meet compressed timelines. • Audits (either internal or independent) will become more frequent / rigorous.
Legal & Court Developments	• Some HIPAA Privacy Rule changes (e.g., strengthening reproductive health care privacy) have been finalized but challenged or vacated in parts by federal courts (HHS.gov regulatory initiatives). • Part 2 regulations (governing substance use disorder records) are being aligned more closely with HIPAA (HIPAA Journal). • Regulatory enforcement has spotlighted patients' rights of access to their records, and interoperability/information blocking requirements are increasing (Reuters).	• Policy teams need to monitor states & court rulings; implementation of recently finalized rules may be delayed or altered due to litigation. • Organizations must maintain readiness to adopt or revert policies depending on final legal outcomes. • Patient access requests, data portability, and exception handling will be more scrutinized.

HITRUST & Standards Evolution	• HITRUST CSF version 11 (v11) introduces a threat-adaptive portfolio, new assessment types, more aligned control mappings, and more efficient assessments (A-LIGN overview). • HITRUST's third-party risk management (TPRM) tools, such as Assessment XChange and integrations with vendor platforms, are expanding to support continuous oversight (HITRUST press release). • CMS interoperability frameworks increasingly require HITRUST certification or equivalent to validate health information exchange participation (HITRUST blog). • Growing emphasis on AI risk and governance, with HITRUST assessments beginning to include new control requirements for AI/ML systems handling PHI (HITRUST webinar).	• HITRUST certified/enrolled organizations need to plan for updates in CSF v11, possibly adjusting audit cycles, control mapping, and gaps from older version. • Vendor / partner risk programs will need to integrate more deeply — not just auditing once, but continuous oversight and validation. • Participating in interoperability networks may require obtaining or maintaining HITRUST; future contracts may include this as a baseline. • If using AI or ML systems processing PHI, expect requirements for governance, documented risk assessment, transparency, possibly new control requirements.

Appendix: How to use

1. **Weighting:** The suggested weights reflect healthcare organizations' top priorities, but you may adjust them based on your risk profile.
2. **Scoring:** Rate each partner from 1–5 for every criterion.
3. **Decision-Making:** The partner with the highest weighted score is the strongest candidate, but also consider cultural fit and long-term partnership potential.
4. **Calculate Weighted Score:** Multiply each score by the weight. Add up to get the vendor's total score.

Tip for CIOs & Compliance Officers: Run this evaluation with a cross-functional team (IT, Security, Compliance, Legal, Vendor Mgmt.) to ensure broad alignment and reduce bias in the final selection.

Appendix B: Sample 12–18 Month Compliance Roadmap

This roadmap illustrates how healthcare organizations can structure compliance readiness initiatives leading up to 2026 HIPAA and HITRUST changes. Actual timelines will vary based on organizational size, cloud maturity, and resource availability.

Timeline	Key Activities	Outputs & Milestones
Quarter 1 (Months 1–3)	- Conduct gap analysis against proposed HIPAA Security Rule & HITRUST CSF v11. - Develop/update asset inventory and network/data flow maps. - Review vendor contracts/BAAs for new notification and recovery requirements. - Form cross-functional HIPAA/HITRUST Working Group.	- Gap Analysis Report - Initial Compliance Roadmap Draft - Updated Asset Inventory & Data Flow Diagrams - Draft contract addendum language
Quarter 2 (Months 4–6)	- Roll out MFA across all ePHI systems. - Conduct incident response tabletop exercise aligned with new regulatory expectations. - Begin workforce training updates (access controls, new policies, AI/ML risks). - Draft documentation for contingency and disaster recovery plans.	- MFA deployment report - Incident Response Exercise Report - Updated Workforce Training Curriculum - Draft Business Continuity & DR Plans
Quarter 3 (Months 7–9)	- Conduct full Security Risk Assessment (SRA) with updated definitions and asset coverage. - Begin policy harmonization (eliminating “addressable” ambiguity, enforcing required controls). - Update encryption standards and validate implementation. - Launch vendor risk monitoring program for continuous oversight.	- Completed SRA Report - Updated Security & Privacy Policies - Encryption Validation Report - Vendor Risk Dashboard
Quarter 4 (Months 10–12)	- Prepare for internal audit: gather documentation, logs, and evidence. - Conduct penetration test and remediate findings. - Finalize incident response and continuity plans; test backups. - Provide board-level compliance update.	- Internal Audit Findings Report - Pen Test Results & Remediation Plan - Validated DR/IR Plans - Board Compliance Briefing
Quarter 5 (Months 13–18)	- Engage external auditor or begin HITRUST certification process if applicable. - Monitor regulatory developments and adjust roadmap accordingly. - Embed compliance monitoring into daily operations (dashboards, drift detection). - Establish quarterly review cadence for readiness steering committee.	- External Audit or HITRUST Readiness Report - Updated Roadmap Adjustments - Continuous Compliance Monitoring in Place - Quarterly Steering Committee Reports

Appendix C: Cloud Compliance Partner Evaluation Matrix

Use this scoring matrix to evaluate potential partners for HIPAA/HITRUST readiness. Assign each criterion a score from 1 **(Poor) to 5 (Excellent)**, then multiply by the weight to calculate a weighted score.

Evaluation Criterion	Weight (%)	Vendor A	Vendor B	Vendor C	Notes
Healthcare Focus & Expertise Track record in healthcare, depth of PHI workflows knowledge, HITRUST/HIPAA case studies	20%				
Visibility & Monitoring Real-time dashboards for asset inventory, ePHI flows, compliance status	20%				
Automated Safeguards & Control Enforcement MFA, encryption, endpoint protection, vulnerability management	15%				
Third-Party/Vendor Risk Management Tools for BAAs, contract monitoring, and continuous vendor oversight	10%				
Audit Readiness & Documentation Templates, policy libraries, incident response playbooks, preserved logs	10%				
Security & Threat Intelligence Continuous monitoring of threat landscape, AI/ML risk governance	10%				
Support & Responsiveness SLA quality, escalation processes, 24/7 support	5%				
Regulatory Foresight Demonstrated ability to anticipate and adapt to evolving HIPAA/HITRUST requirements	5%				
Total Score	100%				