PANDORA CLOUD
UNPACKING COMPLEXITY

HIPAA Cloud Compliance Checklist

36 cloud-specific safeguards for healthcare SMBs handling PHI on AWS, Azure, or Google Cloud. Plus a 30-day implementation path.

A Pandora Cloud Buyer's Resource

May 2026

Pandora Cloud LLC
Women-Owned Small Business (WOSB) | AWS Advanced Partner
GSA MAS: 47QTCA24D00D3 | CAGE: 9JSG7 | UEI: R36GQ3N4XT63
Secret Facility Clearance | pandoracloud.net

About This Checklist

If your healthcare practice, healthtech startup, billing operation, claims handler, or any business handling Protected Health Information (PHI) runs on Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP), this checklist tells you in fifteen minutes whether your cloud-based PHI handling is ready for a Health Insurance Portability and Accountability Act (HIPAA) complaint investigation, an Office for Civil Rights (OCR) audit, or an enterprise security questionnaire from a hospital network or insurance carrier.

It is for SMB owners, practice managers, and compliance leads at organizations of fewer than 100 people running on cloud infrastructure. The 36 items below cover the six areas where cloud-based PHI workloads most commonly fail HIPAA scrutiny, with cloud-provider-specific guidance for AWS, Azure, and GCP.

The most useful insight in this checklist is not the score. It is the recognition that HIPAA in the cloud is a different exercise than HIPAA on-premises. Your cloud provider has a HIPAA Business Associate Agreement (BAA) that covers their infrastructure. You still own configuration, access, encryption-at-the-customer-level, and audit logging at the application level. SMBs that treat the BAA as the compliance ceiling fail audits on the customer-side controls.

Why HIPAA Cloud Compliance Matters Now

The compliance pressure on cloud-based healthcare SMBs has tightened over the past two years.

OCR enforcement targets cloud configuration failures specifically. Recent OCR settlements have called out cloud misconfigurations as the proximate cause: publicly accessible Amazon Simple Storage Service (S3) buckets, unencrypted Azure Blob Storage containers, Google Cloud Storage buckets with permissive Identity and Access Management (IAM) policies. The settlement paperwork increasingly references cloud-specific control failures by name; this is no longer a footnote.

The HIPAA Security Rule Notice of Proposed Rulemaking (NPRM) raises the bar. The Department of Health and Human Services published an NPRM on January 6, 2025 with substantial proposed changes. Encryption of electronic Protected Health Information (ePHI) at rest and in transit moves from "addressable" to required (with limited exceptions). Multi-factor authentication will be required across relevant systems. Mandatory vulnerability scanning, asset inventory, and tightened risk analysis cadence are all in the proposed rule. Organizations operating cloud-based PHI workloads should be aligning to the proposed rule today.

Enterprise procurement teams ask cloud-specific questions. Hospital networks, large insurance carriers, and regional health systems running vendor-risk programs increasingly ask: "Is your cloud provider HIPAA-eligible? Which specific services are in scope of the BAA? Where are PHI workloads located? How are encryption keys managed?" SMBs that cannot answer these in writing fail vendor reviews regardless of how well other controls are implemented.

Cyber insurance underwriting now cares about cloud configuration. Underwriters routinely request evidence of cloud-specific HIPAA controls: encryption-at-rest verification, audit-logging proof, IAM policy review records. Premium deltas between cloud-mature and cloud-immature healthcare SMBs can run 30 to 50 percent.

The 36-item checklist below is the floor. The 30-day implementation path is the way to close gaps quickly. The HIPAA-eligible services reference is the cheat sheet for the cloud-provider conversations that come next.

What HIPAA Cloud Compliance Actually Requires

Before scoring yourself, a quick orientation. Cloud-based PHI handling layers two responsibility models: HIPAA's safeguards model and the cloud provider's shared responsibility model.

HIPAA Security Rule safeguards (45 CFR 164.308 through 164.316). Three categories: administrative (workforce, training, vendor management), physical (facility access, device controls), and technical (access controls, audit controls, integrity, transmission security). Cloud providers cover physical safeguards inherently; they share technical safeguards with the customer; administrative safeguards remain entirely the customer's responsibility.

Cloud provider BAA scope. AWS, Azure, and GCP all offer HIPAA Business Associate Agreements. Each has a list of HIPAA-eligible services covered under the BAA. Services not on the list are not in scope of the BAA; using them for PHI is a HIPAA violation regardless of how secure they are technically. The HIPAA-eligible service list is the first thing to verify before designing any PHI workflow.

Shared responsibility line for PHI workloads. The cloud provider secures the platform (data centers, hypervisors, managed service plumbing). You secure the workload (configuration, IAM, application-level encryption, application-level audit logging, customer data). Most HIPAA cloud failures sit on the customer side of this line: a misconfigured S3 bucket, an over-privileged IAM role, an unencrypted database snapshot, a forgotten audit log retention setting.

The HIPAA-eligible service lists as of May 2026. AWS publishes a HIPAA-eligible services list at aws.amazon.com/compliance/hipaa-eligible-services-reference; the list currently includes 100+ services covering most primary compute, storage, database, networking, and analytics needs. Azure publishes its HIPAA/HITECH offering documentation at the Microsoft Service Trust Portal. GCP publishes its HIPAA-compliant products list at cloud.google.com/security/compliance/hipaa-compliance.

The provider-specific gotcha. Each cloud provider has services that are explicitly NOT HIPAA-eligible or that require customer-side configuration to qualify. Verify on the current published list before building.

How to Use This Checklist

Walk through the 36 items below with your team. For each item, mark one of:

- Implemented: the control is in place, configured for your cloud provider, and you have evidence to show it.
- Partial: the control is partially in place; gaps exist or evidence is incomplete.
- Missing: the control does not exist or has not been documented.

Count the implemented items. Use the scoring tiers to determine your readiness state. Then read the 30-day implementation path for the gap-closing sequence.

Section 1: Access Controls and Identity

Cloud-based PHI access control failures appear in nearly every OCR enforcement action involving cloud workloads. Six controls below close the gaps most-often called out.

- [ ] Unique user identification for every workforce member (no shared accounts) across cloud console, services, and applications.
- [ ] Multi-factor authentication (MFA) enforced for all access to systems handling PHI, including cloud console access (HIPAA 164.312(a)(2)(i)).
- [ ] Role-based access control (RBAC) aligned with the minimum necessary standard; cloud IAM policies grant least privilege.
- [ ] Automatic session timeout configured for PHI-handling applications and cloud console sessions.
- [ ] Emergency access procedures documented (break-glass accounts with mandatory audit logging and post-use review).
- [ ] Workforce access reviews conducted quarterly with documented sign-off (HIPAA 164.308(a)(4)).

Section 2: Audit Logging and Monitoring

Cloud audit logging is more capable than on-premises in most cases but requires specific configuration to satisfy HIPAA. Six controls cover the cloud-native logging requirements.

- [ ] All PHI access logged with user, timestamp, action, and record identifier (HIPAA 164.312(b)).
- [ ] Cloud-native audit logs enabled across all in-scope accounts: AWS CloudTrail, Azure Activity Log, or Google Cloud Audit Logs.
- [ ] Audit logs protected from tampering (write-once or immutable storage; AWS S3 Object Lock, Azure immutable Blob Storage, GCP retention policies).
- [ ] Log retention meets HIPAA minimum (6 years from creation or last in effect, per 45 CFR 164.316(b)(2)(i)).
- [ ] Automated alerts for unusual access patterns (after-hours, bulk export, unauthorized records) via Amazon GuardDuty / Microsoft Sentinel / Google Security Command Center.
- [ ] Log source heartbeat monitoring (alert when any log source goes silent).

Section 3: Encryption of PHI

Cloud encryption is the area where the HIPAA Security Rule NPRM moves most aggressively. Six controls satisfy current requirements and align to the proposed rule.

- [ ] All PHI encrypted at rest using Advanced Encryption Standard (AES) 256-bit or stronger across S3/EBS/RDS (AWS), Storage/Disk/SQL (Azure), or Cloud Storage/Persistent Disk/Cloud SQL (GCP).

- [ ] All PHI encrypted in transit using Transport Layer Security (TLS) 1.2 or higher (no plain HTTP, no Simple Mail Transfer Protocol (SMTP) without STARTTLS); weak cipher suites disabled.
- [ ] Encryption keys managed with documented key rotation policy; AWS Key Management Service (KMS), Azure Key Vault, or Google Cloud Key Management Service in use.
- [ ] Backup data encrypted with separate keys from production; key-tier separation documented.
- [ ] Mobile devices and endpoints accessing PHI use full-disk encryption; cloud-managed Mobile Device Management (MDM) such as Microsoft Intune or AWS Workspaces enforces it.
- [ ] Email containing PHI uses encryption (secure portal, end-to-end encryption, or HIPAA-eligible encrypted email service such as Paubox or AWS WorkMail with encryption).

Section 4: Backup, Disaster Recovery, and Business Continuity

Cloud-native backup capabilities are powerful but require explicit HIPAA-aligned configuration. Six controls cover the requirements.

- [ ] Automated PHI backups occurring at minimum daily frequency via AWS Backup, Azure Backup, or Google Cloud Backup.
- [ ] Backups stored in a separate Region or Availability Zone from primary data; geographic separation verified.
- [ ] Restore procedures tested at least quarterly with documented results; test restore evidence retained.
- [ ] Recovery Time Objective (RTO) and Recovery Point Objective (RPO) defined per workload and met in tests.
- [ ] Business Associate Agreements (BAAs) current with all backup, disaster recovery, and managed-service vendors (cloud provider BAAs cover provider services; third-party tools need separate BAAs).
- [ ] Documented contingency plan per HIPAA 164.308(a)(7) reviewed annually; cloud-specific failover procedures included.

Section 5: Workforce and Vendor Management

Cloud workforce management adds complexity (more service surfaces to govern) but also adds capability (automated lifecycle management). Six controls cover the cloud-specific concerns.

- [ ] HIPAA training completed by all workforce members within 30 days of hire; cloud-specific PHI handling included in training.
- [ ] Annual HIPAA refresher training documented for all workforce; refresh covers cloud-environment changes since last training.
- [ ] Terminated workforce access revoked within 24 hours of separation across cloud console, identity provider, and any third-party PHI-handling SaaS (HIPAA 164.308(a)(3)(ii)(C)).
- [ ] Business Associate Agreements signed with every vendor handling PHI; cloud provider BAAs current and on file.

- [ ] Vendor risk assessments documented for all PHI-handling third parties, including HIPAA-eligible service status verified for cloud services.
- [ ] Sanctions policy documented and applied for HIPAA violations; sanctions extend to cloud-environment misuse.

Section 6: Risk Analysis and Documentation

Cloud-specific risk analysis is the most-cited gap in OCR cloud-related settlements. The risk analysis must explicitly address cloud architecture; "we use AWS so we are HIPAA compliant" is not a risk analysis.

- [ ] Annual risk analysis completed and documented per HIPAA 164.308(a)(1)(ii)(A); covers all PHI systems including cloud-resident workloads.
- [ ] Risk management plan addresses identified risks with assigned owners and target dates.
- [ ] Security incident response plan documented and tested; cloud-specific incident scenarios (account compromise, misconfiguration discovery, data exfiltration via cloud APIs) covered.
- [ ] Breach notification procedure documented (60-day notification window per HIPAA 164.404).
- [ ] Policies and procedures reviewed and updated annually; cloud architecture changes trigger re-review.
- [ ] All HIPAA-related documentation retained for 6 years per 45 CFR 164.316(b)(2)(i).

HIPAA-Eligible Cloud Services: Quick Reference

The HIPAA-eligible services list is the foundation of any cloud PHI architecture. Services not on the list are not covered by the cloud provider's BAA; using them for PHI handling is a violation regardless of technical controls. Verify the current published list before designing any new PHI workflow; the lists are updated regularly as new services come online.

PHI workload	AWS	Azure	GCP
Compute	EC2, ECS, EKS, Lambda, Fargate	Virtual Machines, AKS, App Service, Functions	Compute Engine, GKE, Cloud Run, Cloud Functions
Object storage	S3	Blob Storage	Cloud Storage
Block storage	EBS	Managed Disks	Persistent Disk
Relational database	RDS, Aurora	SQL Database, DB for PostgreSQL	Cloud SQL, AlloyDB
Document database	DynamoDB, DocumentDB	Cosmos DB	Firestore (Datastore mode)
Audit logging	CloudTrail, CloudWatch Logs	Activity Log, Monitor Logs	Cloud Audit Logs, Cloud Logging
Key management	KMS, CloudHSM	Key Vault, Managed HSM	Cloud KMS, Cloud HSM
Identity	IAM, IAM Identity Center, Cognito	Entra ID (Azure AD), B2C	IAM, Identity Platform
Backup	AWS Backup, S3 versioning	Azure Backup, snapshot policies	Backup and DR Service, snapshot schedules
Healthcare analytics	HealthLake, Comprehend Medical	Azure Health Data Services	Healthcare API, Healthcare Data Engine
AI / Machine Learning	SageMaker (HIPAA features), Bedrock	Azure ML (BAA terms)	Vertex AI

The full lists are longer than this excerpt; verify the current published list at aws.amazon.com/compliance/hipaa-eligible-services-reference, the Microsoft Service Trust Portal, and cloud.google.com/security/compliance/hipaa-compliance respectively.

Scoring

Total items implemented (out of 36):

●	**30 to 36 items**	Strong cloud HIPAA posture. Maintain through continuous monitoring. Focus next on aligning to the proposed HIPAA Security Rule NPRM (encryption everywhere, MFA across all relevant systems) so you are

	positioned for the final rule.
20 to 29 items	Foundations in place, gaps could expose you. Address gaps via the 30-day implementation path before any audit, vendor questionnaire, or insurance renewal cycle.
Below 20 items	Significant gaps. PHI in your cloud environment is at material risk. Start with encryption (Section 3) and access controls (Section 1); these have the highest concentration of OCR settlement findings.

What to Do With Your Score

The score is only useful if it points to a specific next move.

If you scored 30-36 (Strong): Your cloud foundation is in place. The next investment is alignment to the proposed HIPAA Security Rule NPRM (encryption-everywhere, MFA-everywhere, vulnerability scanning) and continuous monitoring instrumentation so your annual risk analysis is evidence-driven, not a rebuild. If enterprise buyers are also asking for SOC 2 Type II, your cloud HIPAA controls satisfy most of SOC 2's Security trust services criterion already.

If you scored 20-29 (Foundations Forming): The gaps you have are likely concentrated in audit logging configuration (Section 2) or risk analysis documentation (Section 6). The 30-day path below targets exactly those gaps. Pick the section where you have the lowest score and work through it first.

If you scored below 20 (Significant Gaps): You are carrying material breach and regulatory risk. The cost of a HIPAA settlement for an SMB regularly exceeds breach notification, credit monitoring, legal fees, and reputational damage in totals that can reach several million dollars when the full picture is counted. Start with Days 1-10 of the path; the early items remove the highest-risk exposures.

Your 30-Day Cloud HIPAA Implementation Path

This path targets teams scoring Yellow or Red on the 36-item checklist. Strong-foundation teams can compress it; teams with significant gaps may need 60 days.

The path is sequenced so each phase enables the next. Skipping ahead (for example, starting with audit logging before access controls are in place) produces logs of broken access patterns and creates more remediation work, not less.

Days 1 to 10: Identity, access, and the cloud foundation

Goal: Centralized identity with MFA enforced across all PHI-handling systems. Access reviews scheduled. Departing-workforce deprovisioning under 24 hours. HIPAA-eligible services verified for every existing PHI workload.

- **Day 1-2:** Inventory every cloud account, system, and SaaS tool that holds or processes PHI. Map workforce access to each.
- **Day 3-4:** Verify HIPAA-eligible status for every cloud service in scope. Cross-reference your inventory against the AWS / Azure / GCP HIPAA-eligible services lists. Flag any service not on the list as a remediation priority.
- **Day 5-6:** Stand up centralized identity if not already in place. Move every cloud account, SaaS app, and internal tool behind it (AWS IAM Identity Center, Microsoft Entra ID, or Google Workspace + Cloud Identity). Enforce MFA universally.
- **Day 7-8:** Implement RBAC with least-privilege defaults. Audit existing IAM policies; remove standing administrator access; require just-in-time elevation for privileged operations.
- **Day 9-10:** Run the access review across all in-scope systems. Document sign-off. Remediate over-privileged accounts. Document the deprovisioning procedure with named owner and 24-hour SLA.

Days 11 to 20: Encryption, backups, and audit logging

Goal: Encryption verified at rest and in transit across all PHI stores. Backups encrypted, isolated, and tested. Cloud-native audit logging enabled across all accounts with tamper-resistant retention.

- **Day 11-12:** Audit every storage bucket, database, file share, and managed-service data store for encryption-at-rest status using AES-256 or stronger. Turn on encryption for any unencrypted store.
- **Day 13-14:** Verify TLS 1.2 or higher is enforced on every public endpoint and internal service connection handling PHI. Disable weak cipher suites. Move any plain-HTTP connections behind TLS.
- **Day 15-16:** Enable cloud-native audit logging across every account: CloudTrail (AWS), Activity Log (Azure), Cloud Audit Logs (GCP). Centralize the destination. Configure retention to meet the 6-year HIPAA minimum.
- **Day 17-18:** Make logs tamper-resistant via S3 Object Lock, Azure immutable Blob Storage, or GCP retention policies. Configure alerts for high-risk events (privilege changes, public-access changes, log source going silent).
- **Day 19-20:** Audit backup configuration across all PHI stores. Verify encryption on backup data, separate keys

from production, geographic separation, and successful restore tests. Document the contingency plan if not already in place.

Days 21 to 30: Risk analysis, training, and program governance

Goal: Annual risk analysis completed with cloud-specific scope. Workforce training current. Vendor inventory verified with current BAAs. Incident response plan tested.

Day 21-23: Complete the annual risk analysis. Document identified risks by category (access, encryption, audit, backup, vendor, workforce, physical). Assign owners and target dates for each identified risk.

Day 24-25: Refresh the vendor inventory. Verify every PHI-handling vendor has a current BAA. Verify cloud provider BAAs are current and on file. Triage any gaps and assign remediation owners.

Day 26-27: Verify workforce training records. Assign refresher training to any workforce member overdue. Confirm cloud-specific PHI handling is in the training curriculum.

Day 28-29: Run a tabletop incident response exercise. Use a cloud-specific scenario (account compromise, S3 bucket misconfiguration discovered, audit logs going silent). Document what worked, what did not, and what the plan needs.

Day 30: Re-take the checklist. Compare scores. The improvement tells you whether the program is working; persistent low-score areas are the next quarter's priorities.

Common Patterns We See

Across cloud-based healthcare SMBs running HIPAA programs, the same five gaps show up over and over.

1. The "we have a cloud BAA so we are HIPAA compliant" gap. A signed BAA is necessary but not sufficient. It covers the cloud provider's infrastructure; you still own configuration, IAM, encryption-at-customer-level, and application-level audit logging. SMBs that treat the BAA as the compliance ceiling fail audits on the customer-side controls.

2. The non-HIPAA-eligible service slip. Workflows leak PHI into services that are not on the cloud provider's HIPAA-eligible list: a non-eligible analytics tool, a beta service still in preview, a third-party SaaS plugin that does not have its own BAA. This is the single most common HIPAA cloud finding in our practice. Audit your service inventory annually against the current HIPAA-eligible services list.

3. The configuration drift problem. PHI workloads are configured correctly at launch; over time, someone changes an IAM policy, opens a security group, or adds a forgotten storage bucket. Continuous configuration monitoring (AWS Config, Azure Policy, GCP Security Command Center) is the only way to catch drift in real time.

4. The audit log retention misconfiguration. Cloud-native logging is enabled but retention is set to the provider's default (often 90 days), well below the HIPAA 6-year requirement. Alternatively, logs are retained but stored in mutable storage where anyone with admin access can delete them.

5. The "annual training is enough" trap. HIPAA expects role-relevant security awareness training. Once-a-year click-through training rarely satisfies an OCR investigator; quarterly micro-training plus an annual

deep dive is what passes.

If you scored Yellow or Red, at least three of these patterns are almost certainly the cause.

Cost Expectations

What does cloud HIPAA implementation actually cost an SMB? Honest ranges, with what pushes them up and how to hold them down.

Initial implementation (0 to 60 days). $15,000 to $75,000 for a typical SMB scope: cloud configuration audit ($5-15k), control remediation ($5-30k), policy and risk analysis documentation ($3-15k), workforce training rollout ($1-5k), continuous monitoring tooling setup ($1-10k). Pushed up by complex multi-cloud or hybrid environments, large workforce, and pre-existing technical debt. Held down by clear scope, automation-first remediation, and starting with a focused 30-day path before tackling everything.

Ongoing annual operations. $10,000 to $40,000 per year for a typical SMB: cloud configuration monitoring tooling ($3-12k), annual risk analysis refresh ($2-10k), workforce training and refresher cycles ($1-5k), audit log review and incident response readiness ($2-8k), BAA renewal and vendor risk assessment ($1-5k). Held down by automating evidence collection so the program runs as part of normal operations, not as a separate audit prep cycle.

The cost driver to watch. Cloud configuration drift is the single biggest hidden cost. Without continuous monitoring, drift accumulates between audits and remediation becomes a fire drill. Investing $5k-$10k/year in cloud configuration monitoring tooling typically saves $20k-$50k in audit-prep remediation cycles.

A Worked Example

A 28-person specialty medical practice running on AWS with about 40,000 active patient records scored 14 of 36 on this checklist. The practice manager believed they were "HIPAA compliant in AWS" because they had a signed AWS BAA and used an Electronic Health Record (EHR) system advertised as HIPAA-compliant.

The 22 missing items included: MFA enforced for the EHR but not for AWS console access, workforce access reviews never run, S3 buckets containing scanned patient documents with default encryption disabled, CloudTrail enabled but with 90-day retention (not the 6-year HIPAA minimum), audit logs in mutable S3 storage, no quarterly restore testing, no documented incident response plan, and an analytics SaaS tool processing de-identified data that was actually mishandling PHI in a way the practice had not realized.

They worked the 30-day path. By Day 10 they had: centralized identity with MFA enforced across AWS console and all SaaS tools, completed access review with five over-privileged accounts remediated, identified and replaced the analytics SaaS that was processing PHI without a BAA. By Day 20 they had: encryption verified across all S3 buckets and RDS instances, CloudTrail retention bumped to 7 years and moved to immutable storage, restore testing completed on the EHR backup with a documented test plan. By Day 30 they had: completed the annual risk analysis with cloud-specific scope, refreshed all workforce training, ran a tabletop

incident response exercise covering an S3 misconfiguration discovery scenario.

They scored 32 of 36 on the re-take; the remaining gaps were just-in-time access elevation (deferred to next quarter as a tooling investment) and continuous configuration monitoring instrumentation (deferred pending an AWS Config rules deployment).

The cost: roughly 60 hours of practice manager time, 40 hours of contracted security engineer time, and one weekend for the centralized-identity migration. Total: around $18,000 in external engineering plus internal time. The result: the practice signed a $250,000 multi-year contract with a regional hospital network six weeks later, which had previously been gated on producing current HIPAA documentation including cloud-specific controls. The 36-item checklist was the diagnostic. The 30-day path was the prescription. The contract was the outcome.

Where to Go From Here

The HIPAA Cloud Compliance Checklist sits in a longer compliance journey. Depending on your situation, the natural next moves:

If you scored Yellow or Red: Start with the 30-day path. Re-score at Day 30 to measure progress.

If you also process credit card payments: Pick up the HIPAA & PCI Readiness Checklist. Many cloud HIPAA controls satisfy PCI DSS simultaneously. Free at pandoracloud.net/hipaa-pci-checklist.

If enterprise buyers are asking for SOC 2 Type II: Pick up the SOC 2 Readiness Checklist. The cloud HIPAA controls you have already implemented satisfy most of SOC 2's Security trust services criterion. Free at pandoracloud.net/soc2-readiness-checklist.

If you are pursuing federal contracts (e.g., VA healthcare or DoD healthcare systems): Pick up the ATO Readiness Checklist. Free at pandoracloud.net/ato-readiness-checklist.

If you have not yet established the cloud foundation: Take the Cloud Compliance Foundation Worksheet first. It is the entry-point assessment that this checklist builds on. Free at pandoracloud.net/foundation-worksheet.

If your underlying cloud architecture is informal: Pick up the Cloud Landing Zones Guide. The HIPAA technical safeguards in this checklist presume an underlying multi-account separation and tamper-resistant logging architecture; the Guide is the 28-page playbook for building that foundation. Free at pandoracloud.net/cloud-landing-zones-guide.

If you want the cross-framework view: Pick up the Future of Cloud Compliance Whitepaper. Free at pandoracloud.net/future-of-compliance-whitepaper.

In every case, the cloud-specific controls in this checklist are the highest-leverage investment for healthcare SMBs. Implement once correctly; satisfy HIPAA, SOC 2, and (where applicable) PCI DSS simultaneously.

Framework Updates to Watch

The compliance landscape is in motion. The citations and controls in this checklist are accurate as of May 2026, but several frameworks have updates in progress that will affect how organizations document and demonstrate compliance over the next 12 to 24 months. If your readiness work is anchored to current rule citations, you are correctly positioned for today; this section names what to watch for.

HIPAA Security Rule (NPRM published January 2025). The Department of Health and Human Services published a Notice of Proposed Rulemaking on January 6, 2025 with substantial proposed changes. The final rule has not yet been issued. The federal regulatory agenda now targets July 2027 for final action, pushed back from an earlier 2026 estimate, and that target is not binding. A 180-day compliance period follows publication. Key proposed changes: encryption of ePHI at rest and in transit moves from "addressable" to required (with limited exceptions); multi-factor authentication required across relevant systems; removal of the "required vs. addressable" distinction; mandatory vulnerability scanning, asset inventory updates, and tightened risk analysis cadence. This is the most material upcoming change affecting this checklist.

Cloud provider HIPAA-eligible services lists (continuously updated). AWS, Azure, and GCP add and occasionally remove services from their HIPAA-eligible lists as services mature. Treat the lists as live references, not snapshots; verify before designing new PHI workflows. Subscribe to the cloud provider's compliance update notifications.

SOC 2 / AICPA Trust Services Criteria (stable). The 2017 Trust Services Criteria with revised 2022 Points of Focus remains the current standard. The American Institute of Certified Public Accountants (AICPA) periodically updates Points of Focus without changing the underlying criteria; the framework has been stable for new audits.

PCI DSS v4.0.1 (current and stable). v4.0.1 became fully mandatory March 31, 2025; v3.2.1 is retired. Cloud-based merchants accepting card payments must operate against v4.0.1 numbering.

NIST 800-53 Rev 5 / FedRAMP (stable). FedRAMP officially moved to Rev 5 in May 2023. Cloud-based PHI workloads serving federal healthcare buyers (Veterans Affairs, military health) increasingly intersect with FedRAMP requirements; align cloud HIPAA controls to NIST 800-53 Rev 5 mappings to ease the federal pursuit if it comes.

CMMC 2.0 (Phase 1 in force; Phase 2 suspended). If your healthcare SMB also serves DoD-adjacent contracts (military health, defense health agency partners), CMMC Level 2 self-assessment under Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7021 has applied since November 10, 2025. The Phase 2 shift to third-party assessment by a CMMC Third-Party Assessment Organization (C3PAO), originally November 10, 2026, was suspended by DoD on July 13, 2026 pending a program review; plan for it on a date not yet announced. Most cloud HIPAA controls satisfy CMMC Level 2 control families simultaneously.

What this means for you: HIPAA Security Rule final-rule publication is the most material upcoming change. Cloud provider HIPAA-eligible service lists are continuously updated and need annual verification at minimum. Everything else is stable for the immediate future.

Printable Scoring Sheet

Print this page. Take it to a conference room. Walk through the 36 items with the team and mark each one. The page is designed to live on a wall or in a binder for the duration of your readiness work.

1. Access Controls and Identity

- ☐ Unique user identification across all systems _____
- ☐ MFA enforced for all PHI-handling access _____
- ☐ RBAC with minimum necessary; least privilege _____
- ☐ Automatic session timeout configured _____
- ☐ Emergency access procedures with audit _____
- ☐ Quarterly access reviews documented _____

2. Audit Logging and Monitoring

- ☐ PHI access logged with user/timestamp/action _____
- ☐ CloudTrail / Activity Log / Audit Logs enabled _____
- ☐ Logs in tamper-resistant immutable storage _____
- ☐ 6-year retention configured _____
- ☐ Alerts on unusual access patterns _____
- ☐ Log source heartbeat monitoring active _____

3. Encryption of PHI

- ☐ PHI encrypted at rest (AES-256+) _____
- ☐ PHI encrypted in transit (TLS 1.2+) _____
- ☐ KMS / Key Vault / Cloud KMS with rotation _____
- ☐ Backup encrypted with separate keys _____
- ☐ Endpoint full-disk encryption via MDM _____
- ☐ Email containing PHI uses encryption _____

4. Backup, DR, and Business Continuity

- ☐ Automated daily backups via cloud-native tools _____
- ☐ Backups in separate Region/AZ _____
- ☐ Quarterly restore tests documented _____
- ☐ RTO and RPO defined and met _____
- ☐ BAAs current with all backup vendors _____
- ☐ Documented contingency plan reviewed annually _____

5. Workforce and Vendor Management

- ☐ HIPAA training within 30 days of hire _____
- ☐ Annual refresher training documented _____
- ☐ Termination access revoked within 24 hours _____
- ☐ BAAs with all PHI-handling vendors _____
- ☐ Vendor risk assessments documented _____
- ☐ Sanctions policy documented and applied _____

6. Risk Analysis and Documentation

- [ ] Annual risk analysis with cloud scope _____
- [ ] Risk management plan with owners _____
- [ ] IR plan tested with cloud scenarios _____
- [ ] Breach notification procedure (60 days) _____
- [ ] Annual policy and procedure review _____
- [ ] Documentation retained 6 years _____

Total implemented (out of 36): _____

30-36: Strong cloud HIPAA posture; align to NPRM and continuous monitoring.
20-29: Foundations in place; close gaps via the 30-day path.
Below 20: Significant gaps; start with encryption and access controls.

A Note on Pandora Cloud

Pandora Cloud is a Women-Owned Small Business and an Amazon Web Services (AWS) Advanced Tier Partner with a Defense Counterintelligence and Security Agency (DCSA) Secret-level Facility Clearance and Cybersecurity Maturity Model Certification (CMMC) Level 2 self-assessment status. We help regulated SMBs across healthcare, finance, legal, insurance, and defense build compliant cloud environments and operate them as part of normal business, not as periodic audit projects.

If you scored Yellow or Red and want a second set of eyes on which gaps to prioritize, we offer free 30-minute consultations.

See what HIPAA compliance actually costs for a healthcare SMB your size: pandoracloud.net/cost-calculator/. The Healthcare scenario models the full proactive-versus-reactive picture.

Want a second set of eyes on your gaps?

Schedule a free 30-minute consultation. We will walk through your scored checklist and help you prioritize the next 30 days.

pandoracloud.net/#schedule-consultation

Glossary

For readers new to HIPAA cloud vocabulary, this glossary names the most common terms used in this checklist.

AES (Advanced Encryption Standard)
Symmetric block cipher used for encrypting data at rest. AES-256 is the standard for HIPAA-aligned cloud encryption.

BAA (Business Associate Agreement)
Contract under HIPAA between a covered entity and a third party handling Protected Health Information (PHI). Required for any vendor or cloud provider that touches patient data.

CloudTrail
AWS service that records account activity for security analysis and compliance. The HIPAA-aligned audit logging mechanism on AWS.

Cloud Audit Logs
GCP service that records account and resource activity. The HIPAA-aligned audit logging mechanism on Google Cloud.

Cloud KMS / Key Vault / KMS
Cloud-native key management services on GCP, Azure, and AWS respectively. Used to manage encryption keys for HIPAA-aligned at-rest encryption.

ePHI (Electronic Protected Health Information)
PHI created, received, maintained, or transmitted in electronic form. The HIPAA Security Rule applies specifically to ePHI.

EHR (Electronic Health Record)
Digital version of a patient chart. EHR vendors maintain HIPAA-eligible products but configuration responsibility sits with the customer.

HIPAA-Eligible Service
A cloud provider service explicitly covered under that provider's BAA. Services not on the published list are not in scope of the BAA; using them for PHI is a HIPAA violation regardless of technical controls.

IAM (Identity and Access Management)
Cloud-native service for managing identities and access permissions. AWS IAM, Microsoft Entra ID (Azure AD), Google Cloud IAM.

MFA (Multi-Factor Authentication)
Login that requires more than just a password. Required for all privileged access under HIPAA-aligned cloud configurations.

NPRM (Notice of Proposed Rulemaking)
Federal rulemaking document proposing changes to existing regulations. The HIPAA Security Rule NPRM was published January 6, 2025; final rule now targeted for July 2027.

OCR (Office for Civil Rights)
US Department of Health and Human Services agency that enforces HIPAA. Investigates complaints, breach notifications, and tips; imposes civil monetary penalties.

PHI (Protected Health Information)
Individually identifiable health data covered under HIPAA. Includes 18 specific identifiers ranging from names tied to appointment dates to IP addresses linked to patient portals.

Risk Analysis
Documented assessment of risks to ePHI per HIPAA 164.308(a)(1)(ii)(A). Required annually and after significant system changes.

RTO / RPO (Recovery Time Objective / Recovery Point Objective)
Defined targets for how quickly systems must be restored after an outage (RTO) and how much data loss is acceptable (RPO). Required components of a HIPAA-aligned contingency plan.

S3 Object Lock
AWS S3 feature that enables write-once-read-many (WORM) protection on objects. Used to satisfy HIPAA tamper-resistant log retention requirements.

TLS (Transport Layer Security)
Cryptographic protocol that secures data in transit. HIPAA-aligned cloud configurations require TLS 1.2 or higher; weak cipher suites must be disabled.