ITVORTEX
SIMPLIFY. PROTECT. EVOLVE.

FREE RESOURCE · COMPLIANCE GUIDE

HIPAA Cloud Compliance Guide.

What "HIPAA-ready" actually requires of your cloud, your backups, and your access controls, mapped to the Security Rule's three safeguard categories. Not a checklist of buzzwords, but the specific controls an auditor asks about first.

SAFEGUARD SETS
3
administrative, physical, technical

CLOUD ESSENTIALS
4
encryption, access, BAA, backup/DR

REQUIRED SIGNER
BAA
with every vendor touching ePHI

RECORDS KEPT
6 yr
HIPAA documentation retention

ITV-HIPAA-CL-2026 · v1.0

What the rule actually requires.

HIPAA doesn't certify your cloud, it holds you accountable for it. There is no "HIPAA-certified" provider that absolves you of responsibility. The Security Rule makes you accountable for protecting electronic PHI wherever it lives, including someone else's datacenter. Here is what it requires, and what to demand from any cloud that touches your data.

EDUCATIONAL, NOT LEGAL ADVICE

The HIPAA Security Rule (45 CFR Part 164, Subpart C) sets the standards summarized here. This guide is for understanding, not compliance certification. Confirm how each requirement applies to your organization with your compliance officer or counsel.

A Administrative safeguards — the policies and the people

RULE REQUIRES A documented risk analysis and risk management process, an assigned security official, workforce access management, security training, and a contingency plan covering backup, disaster recovery, and emergency-mode operation.

IN THE CLOUD A risk analysis that explicitly includes the cloud, role-based access you control and review, and a signed Business Associate Agreement with the provider.

P Physical safeguards — the facilities and devices

RULE REQUIRES Facility access controls, workstation use and security policies, and device and media controls covering disposal, re-use, and movement of hardware holding ePHI.

IN THE CLOUD The provider's datacenter controls, evidenced by attestations such as SOC 2, plus your own controls on every laptop and device that reaches the data.

T Technical safeguards — the systems and data

RULE REQUIRES Access control with unique user IDs and automatic logoff, audit controls, integrity controls, person or entity authentication, and transmission security.

IN THE CLOUD Encryption at rest and in transit, audit logs you can actually review, multi-factor authentication, and integrity protection on ePHI.

Where compliance gets specific.

1 Encryption, at rest and in transit

ePHI encrypted on disk and over the wire with TLS. Encryption is an **addressable** specification, not optional: if you don't encrypt, you must document why and what you do instead. Encrypted data that is lost or stolen may also qualify for breach-notification safe harbor.

2 Access control and audit logging

Unique user IDs, least-privilege roles, MFA, and automatic logoff, paired with audit logs that record who accessed what and when. Logs only count if they are retained and someone actually reviews them.

3 Business Associate Agreements (BAAs)

Any vendor that creates, receives, maintains, or transmits ePHI on your behalf needs a signed BAA. No BAA means no compliant use, full stop. That includes your cloud, backup, and email providers, not just your EHR.

4 Backup and disaster recovery

The contingency-plan standard requires a data backup plan, a disaster recovery plan, and emergency-mode operation. Backups of ePHI must be protected to the same standard as production, and you must be able to restore them when it counts.

THE QUESTIONS AN AUDITOR ASKS FIRST

- [ ] Do you have a current risk analysis that explicitly includes the cloud?
- [ ] Is there a signed BAA with every vendor that touches ePHI?
- [ ] Is ePHI encrypted both at rest and in transit?
- [ ] Are audit logs enabled, retained, and actually reviewed?
- [ ] Is there a tested backup and disaster recovery plan for ePHI?
- [ ] Is required documentation retained for six years?

Ready before the audit.

Most HIPAA findings aren't exotic. They're a missing BAA, an unencrypted backup, or audit logs nobody reviews. We build the cloud, backup, and security layers so those answers are already yes when the auditor asks. Here's where each safeguard gets handled.

Security as a Service (SECaaS)
theitvortex.com/secaas/

Access control, MFA, audit logging, and monitoring mapped to the technical safeguards.

Backup as a Service (BaaS)
theitvortex.com/veeam-baas-offerings/

Encrypted, immutable backups of ePHI protected to the same standard as production.

Disaster Recovery (DRaaS)
theitvortex.com/disaster-recovery-as-a-service/

A tested DR and emergency-mode plan that satisfies the contingency standard.

Cloud Hosting (IaaS)
theitvortex.com/cloud-hosting-iaas/

Private cloud with encryption, attested datacenter controls, and a signed BAA.

Talk through your obligations: (201) 225-8670 · www.theitvortex.com

WALK IN READY

Have an IT Vortex engineer map your cloud against the three safeguard categories and the four essentials. We'll show you where you're covered and where a finding is waiting.

BOOK A COMPLIANCE REVIEW