VitalEdge IT

Empowering Healthy Technology

# HIPAA for Business Associates Compliance Checklist

**In Partnership with Vanta • Automated Compliance Monitoring**

**IMPORTANT DISCLAIMER**

This interactive checklist is for general informational and self-assessment purposes only. It does not qualify as legal advice and does not certify HIPAA compliance. Business Associates must comply with applicable HIPAA Rules (primarily Security Rule, Breach Notification Rule, and Privacy Rule provisions in BAAs). Always consult qualified legal and compliance professionals. Completing this form does not create any certification or warranty. Vital Edge IT provides IT and compliance support services but is not a law firm and is not affiliated with HHS, OCR, or any government body.

**How to Use This Interactive Form:**

- Click any checkbox to toggle it on/off. Your selections are saved when you save the PDF.
- Review your organization's policies, procedures, and technical controls against each item.
- Use this as a gap analysis tool. Vital Edge IT can help implement and automate many of these controls via Vanta.

**POWERED BY VANTA — AUTOMATED COMPLIANCE**

Vital Edge IT (Vanta Partner) helps healthcare organizations implement these safeguards while automating evidence collection, continuous monitoring, risk assessments, policy management, and audit-ready reporting. Focus on patient care — we handle the compliance heavy lifting.

**New Resource: Visit our HIPAA Compliance Knowledge Base**

https://vitaledgeit.com/hipaa-resources — Official government links, breach reporting guidance, and more learning materials.

**Contact Vital Edge IT: 855-367-8348 | vitaledgeit.com | Free Network Security Risk Assessment Available**

# HIPAA Security Rule • Privacy Rule • Breach Notification — Interactive Self-Assessment

## HIPAA SECURITY RULE — Physical Safeguards

- ☐ Clear and specific procedures for physical access to prevent theft of ePHI from servers or devices
- ☐ Protection for workstations that may access ePHI (workstations not in visitor-visible areas)
- ☐ Policies for mobile device access to ePHI
- ☐ Asset log/inventory of all hardware devices that house or transmit ePHI (past or current)

## HIPAA SECURITY RULE — Administrative Safeguards

- ☐ Conduct a yearly (or more frequent) formal risk assessment/analysis
- ☐ Conduct and document regular, ongoing HIPAA training for all employees and contractors
- ☐ Designated HIPAA Compliance/Security Officer responsible for policies and enforcement
- ☐ Policies to maintain the integrity of ePHI within the organization
- ☐ Executed Business Associate Agreements (BAAs) with all Covered Entities and Sub-BAs/vendors
- ☐ Restrict access to ePHI; apply minimum necessary standard when access occurs
- ☐ Policy to report potential security incidents promptly to the HIPAA Compliance Officer

## HIPAA SECURITY RULE — Technical Safeguards

- ☐ Unique usernames/authentication for each user accessing ePHI
- ☐ Procedures for release/disclosure of ePHI to patients, Sub-BAs, CEs, and in emergencies
- ☐ Data integrity/quality measures to detect changes or alterations to ePHI
- ☐ Encrypt all ePHI in transit (especially outside secure environments) and decrypt on receipt
- ☐ Secure, reviewable access/audit logs for all ePHI access
- ☐ Documented login, logout, session timeout, and workstation locking procedures

## HIPAA PRIVACY RULE REQUIREMENTS

- ☐ Internal training for employees on what information can/cannot be shared (uses & disclosures)
- ☐ Written Covered Entity authorization before using PHI for marketing, fundraising, or research
- ☐ Procedures to honor patient's right of access to ePHI/PHI (generally within 30 days)
- ☐ Documented Privacy Rule responsibilities per the specific language in your BAAs

## HIPAA BREACH NOTIFICATION REQUIREMENTS

- ☐ Policies to submit breach notifications promptly to OCR/HHS (and affected individuals) as required
- ☐ Media/press release capability if breach affects 500+ individuals
- ☐ Policies for submitting notifications for <500 individuals to the HHS/OCR portal (annual or per timeline)
- ☐ Documentation of all breach investigations, risk-of-harm assessments, and notifications retained as required

# Ready to Simplify HIPAA Compliance?

Vital Edge IT + Vanta = Automated, Continuous Compliance for Healthcare Organizations

## WHAT VITAL EDGE IT + VANTA DELIVERS

- Continuous compliance monitoring & automated evidence collection (400+ integrations)
- Real-time dashboards, risk assessments, policy management, and training tracking
- Proactive breach prevention, forensics support, and incident response assistance for client organizations
- Audit-ready reporting and simplified preparation for OCR/HHS reviews
- Tailored support for EHR integrations, M365, cloud infrastructure, and healthcare workflows

**Protecting your practice so you can protect patients — secure, compliant, and human-centered.**

**Next Steps:**

1. Complete this interactive checklist as a starting gap analysis (click boxes above, then save).
2. Visit our new HIPAA Compliance Knowledge Base: https://vitaledgeit.com/hipaa-resources
   (Official government resources, breach reporting portal guidance, in-depth learning materials)
3. Schedule your Free Network Security Risk Assessment or compliance consultation with our team.

**Contact Vital Edge IT Today**

855-367-8348 • vitaledgeit.com • info@vitaledgeit.com