BLACK BOX

TRUST CENTER | COMPLIANCE & SECURITY

HIPAA Compliance: Our Commitment, Your Confidence

Understanding the Framework — and the Business Value Behind It

Why There Is No Such Thing as HIPAA Certification

The Health Insurance Portability and Accountability Act (HIPAA) is enforced by the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR). Unlike frameworks such as SOC 2 or ISO 27001, HIPAA does not operate through an accredited third-party certification body — and intentionally so.

The regulation was designed as a **self-attestation and audit-readiness model**. Covered Entities and Business Associates are required to implement the Administrative, Physical, and Technical Safeguards defined by the HIPAA Security Rule, maintain documentation, conduct ongoing risk assessments, and be prepared for OCR investigation at any time. Compliance is demonstrated through **practice, not paper certification.**

A critical and often misunderstood aspect of HIPAA is that no federal body — not HHS, not the OCR, not any accredited organization — issues a "HIPAA certification." Any vendor claiming to hold one is either misstating the nature of their posture or referencing an unofficial, non-regulatory credential. This is intentional policy design, not a gap in the framework.

What We Do Instead — A Rigorous, Verifiable Posture

The absence of a formal certificate does not mean the absence of accountability. Our compliance program is designed to meet and exceed the standard of due diligence expected of healthcare-adjacent technology partners. Specifically:

- Annual Risk Assessments: We conduct formal, documented risk analyses annually and following material system changes, consistent with 45 CFR § 164.308(a)(1).
- Business Associate Agreements (BAAs): We execute BAAs with all applicable partners and sub processors, and are prepared to sign a BAA with your organization before any PHI is exchanged.
- Technical Safeguards: PHI is encrypted at rest (AES-256) and in transit (TLS 1.2+). Access controls, audit logging, and automatic session timeouts are enforced across all systems.
- Employee Training: All personnel with access to PHI complete HIPAA training at onboarding and annually. Training records are maintained and available upon request.
- Incident Response Plan: We maintain a documented breach notification procedure in compliance with the HIPAA Breach Notification Rule (45 CFR § 164.400–414), including 60-day notification obligations to affected Business Associates, US Department of Health & Human Services and the affected individuals.

Why Our Compliance Posture Is a Competitive Advantage for Partners

Compliance without a certificate is still a powerful, verifiable trust signal. Here is what our HIPAA posture delivers for organizations that partner with us:

✔**Accelerated Vendor Onboarding**

Our documentation package — risk assessments, policies, BAA templates, and training records — is maintained in audit-ready format. Your legal and security teams have what they need from day one, compressing procurement timelines significantly.

✔Reduced Downstream Liability

Partnering with a HIPAA-aligned vendor directly reduces your organization's exposure under joint liability frameworks. Our controls are designed so that your security team can close findings, not open them.

✔BAA-Ready From Day One

We have executed Business Associate Agreements across a wide range of enterprise requirements and maintain a standard BAA template ready for immediate execution. Custom terms are reviewed promptly by our legal team.

✔Audit Support & Transparency

We actively support your compliance audits. Our team responds to security questionnaires, provides policy documentation, and participates in third-party assessments — reducing your compliance burden, not adding to it.

Our Role: Incidental Exposure, Not PHI Processing

An important context for understanding Black Box's relationship to HIPAA is the nature of our contact with Protected Health Information (PHI) and Electronic Protected Health Information (ePHI). The **vast majority of PHI and ePHI that Black Box encounters is incidental to the performance of network monitoring and technical support services** — it is not deliberately collected, stored, analyzed, or processed as part of our service delivery.

When Black Box performs network monitoring, infrastructure support, or managed services for healthcare clients, our personnel and systems may traverse network segments or diagnostic data that incidentally contain PHI or ePHI. This exposure is a byproduct of the technical environment, not the purpose of our engagement. Under the HIPAA Privacy Rule, such incidental contact — where reasonable safeguards are in place and the minimum necessary standard is observed — does not constitute a violation and is expressly recognized as an unavoidable aspect of legitimate healthcare operations support.

This distinction carries practical compliance significance for our partners:

- Black Box does not build, maintain, or operate systems whose primary function is to store or process PHI on behalf of a Covered Entity. Our role is infrastructure and connectivity, not data custodianship.
- Where incidental PHI or ePHI exposure is foreseeable, Black Box applies the necessary standard — limiting access to only those personnel and systems required to perform the specific support function.
- Technical controls — including network segmentation, role-based access, and encrypted communication channels — are in place to reduce the likelihood and scope of any incidental PHI contact during routine support activities.
- Our Business Associate Agreements accurately reflect this operational reality, defining the scope and limitations of Black Box's contact with PHI and establishing the appropriate obligations on both sides of the relationship.

Documentation Available to Partners

Upon execution of an appropriate non-disclosure or data handling agreement, we can provide:

- HIPAA Security Rule gap assessment and risk analysis summary
- Policies and procedures covering Administrative, Physical, and Technical Safeguards
- Standard Business Associate Agreement (BAA) template for immediate execution
- Completion of standard Vendor Security Questionnaires (VSQs) and third-party risk intake forms

---

Security Security & compliance inquiries:
For questions about our security posture or to request compliance documentation - Contact Us