CBE INC. | IT SOLUTIONS FOR SMALL BUSINESS

Compliance-Ready IT Management with SuperOps

How CBE Inc. Protects Healthcare and Financial Services Clients with Enterprise-Grade Compliance Tools

Serving the Greater Philadelphia, Delaware County, and South Jersey Regions

Why Compliance Matters for Your Business

If your organization handles patient health records or client financial data, you are subject to strict federal regulations that govern how that information is stored, accessed, and protected. Non-compliance is not a theoretical risk — it carries real consequences that can threaten the survival of your business.

HIPAA: Protecting Patient Health Information

The Health Insurance Portability and Accountability Act (HIPAA) requires every organization that touches electronic Protected Health Information (ePHI) to implement specific safeguards:

- **Technical Safeguards:** Encryption of data at rest and in transit, access controls limiting who can view patient records, and audit logs tracking every interaction with ePHI.
- **Administrative Safeguards:** Written security policies, workforce training, risk assessments, and incident response procedures.
- **Physical Safeguards:** Workstation security, device controls, and facility access limitations.
- **Breach Notification:** Organizations must notify affected individuals, the Department of Health and Human Services, and in some cases the media, within 60 days of discovering a breach.
- **Business Associate Agreements (BAAs):** Any vendor that accesses ePHI on your behalf must sign a BAA, accepting shared responsibility for protecting that data.

FINRA: Safeguarding Financial Records and Client Data

The Financial Industry Regulatory Authority (FINRA) holds broker-dealers and financial advisory firms to rigorous standards for recordkeeping, supervision, and cybersecurity:

- **Rule 3110 — Supervision:** Firms must establish and maintain a system of supervision, including written procedures, to ensure compliance with securities laws. This extends to technology systems and electronic communications.

- **Rule 4511 — Books and Records:** Firms must make and preserve books and records as required by FINRA rules, the Securities Exchange Act, and applicable regulations — including electronic records stored on IT systems.
- **Rule 4370 — Business Continuity Planning:** Firms must create and maintain a written business continuity plan that addresses data backup, recovery, and the identification of mission-critical systems.
- **Cybersecurity Expectations:** FINRA has issued extensive guidance urging firms to implement access controls, encryption, patch management, and ongoing risk assessment as core components of their compliance programs.

> ⚠ **The Cost of Non-Compliance**
>
> HIPAA penalties can reach up to **$2.13 million per violation category per year**. FINRA fines regularly exceed **$1 million** for supervisory and recordkeeping failures. Beyond fines, non-compliance leads to reputational damage, loss of client trust, and operational disruption that can take years to recover from.

The good news: **you do not have to navigate this alone.** CBE Inc. partners with small businesses across the Greater Philadelphia area to take the complexity of IT compliance off your plate — using enterprise-grade tools and proactive management to keep you protected and audit-ready every day of the year.

What Is SuperOps?

SuperOps is a modern, unified platform purpose-built for managed service providers like CBE Inc. It combines two critical capabilities into a single system:

- **Professional Services Automation (PSA):** Streamlined service desk, ticketing, and client management — so nothing falls through the cracks.

- **Remote Monitoring and Management (RMM):** Real-time visibility into every managed device, with the ability to deploy patches, run scripts, enforce policies, and respond to issues proactively.

Unlike older tools that bolt together separate systems, SuperOps was designed from the ground up as a unified platform. This means every action — from a helpdesk ticket to a remote session to a policy deployment — is tracked in one place, creating a seamless audit trail.

Built-In Security and Compliance Features

- **HIPAA-Compliant Architecture:** Data is encrypted at rest, in transit, and in storage within the platform.
- **Single Sign-On (SSO):** Centralized identity management reduces password sprawl and unauthorized access.
- **SSL/TLS Encryption:** All communications between endpoints and the platform are secured.
- **Two-Factor Authentication (2FA):** Required for platform access, preventing unauthorized logins even if credentials are compromised.
- **IP Whitelisting:** Platform access can be restricted to approved network locations only.
- **Centralized Dashboard:** One pane of glass for managing every client endpoint, policy, and alert.

When CBE Inc. manages your IT through SuperOps, you get the benefit of an enterprise-grade compliance platform — without the enterprise price tag or complexity.

Device Hardening

What it means: Device hardening is the process of locking down computers, laptops, and servers so that only authorized software, settings, and configurations

are in place. Think of it as reinforcing every door, window, and lock on your digital property.

How CBE Inc. Uses SuperOps to Harden Your Devices

- **Automated Security Policies:** Scripting and automation policies are applied uniformly across all managed devices — ensuring every workstation meets the same security baseline, whether it sits in your main office or a remote employee's home.
- **Baseline Security Configurations:** Industry-standard configurations are deployed to disable unnecessary services, close unused ports, and remove default accounts that attackers exploit.
- **Firewall and Antivirus Monitoring:** SuperOps continuously monitors the status of endpoint firewalls and antivirus software, alerting CBE Inc. immediately if protection lapses on any device.
- **Encryption Enforcement:** BitLocker (Windows) and FileVault (macOS) disk encryption are enforced and verified across all endpoints — ensuring that even a lost or stolen laptop cannot expose your sensitive data.

> **Compliance Benefit**
>
> Device hardening directly satisfies **HIPAA Technical Safeguard requirements** (§164.312) for encryption and endpoint protection, and aligns with **FINRA cybersecurity best practices** for securing systems that store or process client financial data.

Access Control

Controlling who can access sensitive information — and under what conditions — is one of the most fundamental requirements of both HIPAA and FINRA. CBE Inc. enforces access control at every layer through SuperOps.

Platform-Level Access Controls

- **Role-Based Permissions:** Every CBE Inc. technician has access only to the clients and systems they are authorized to manage. Client environments are fully isolated within the platform.
- **IP Whitelisting:** Platform access can be restricted to approved IP addresses, ensuring that management tools are only accessible from trusted locations.
- **Multi-Factor Authentication:** All platform logins require 2FA, adding a critical second layer of verification beyond passwords.

Endpoint-Level Access Controls

- **Password Policy Enforcement:** CBE Inc. deploys and enforces strong password policies across your workstations — minimum length, complexity requirements, and expiration schedules.
- **Screen Lock Policies:** Automatic screen locking after periods of inactivity prevents unauthorized access to unattended workstations.
- **MFA on Client Workstations:** Where supported, multi-factor authentication is enforced on endpoint logins and critical applications.

Compliance Benefit

Satisfies the **HIPAA Access Control standard (§164.312(a))**, which requires unique user identification, emergency access procedures, automatic logoff, and encryption. Also supports **FINRA Rule 3110 supervisory requirements** by ensuring only authorized personnel can access regulated systems and data.

Audit Logging & Reporting

When regulators or auditors come calling, the question is never *if* you have controls — it is whether you can *prove* it. CBE Inc. ensures you always have the documentation to back up your compliance posture.

Comprehensive Activity Tracking

- **Technician Activity Logs:** Every action taken by a CBE Inc. technician is logged within SuperOps — remote sessions, script executions, configuration changes, software installations, and policy modifications.
- **Session Recording:** Remote support sessions can be recorded and archived, providing a visual record of exactly what was done on any device.
- **Timestamped Audit Trails:** Every log entry includes the technician's identity, the target device, the action taken, and a precise timestamp.

Audit-Ready Reporting

- **Exportable Reports:** Audit trails and compliance reports can be exported for review by your compliance officer, legal counsel, or regulatory examiners.
- **On-Demand Documentation:** Need to show an auditor six months of patch history for a specific workstation? CBE Inc. can generate that report in minutes — not weeks.

Compliance Benefit

Provides the documentation trail that **HIPAA auditors** expect under the Audit Controls standard (§164.312(b)). Directly supports **FINRA Rule 3110** supervisory requirements, which mandate that firms maintain evidence of their supervisory systems and procedures.

Patch Management

Unpatched software is one of the most common entry points for cyberattacks. Every day a security patch goes unapplied is a day your systems remain vulnerable to known exploits. CBE Inc. eliminates this risk through automated, policy-driven patch management.

How It Works

- **Automated Patch Policies:** Patches for Windows, macOS, and third-party applications (browsers, PDF readers, productivity suites) are deployed automatically according to schedules you approve.
- **Granular Control:** Policies can be configured per client, per site, or per individual device — giving CBE Inc. the flexibility to accommodate unique operational requirements.
- **After-Hours Scheduling:** For healthcare environments where systems must remain available during patient care hours, patches are scheduled for evenings, weekends, or maintenance windows.
- **Intermittently Connected Devices:** Laptops used by visiting clinicians, field agents, or remote workers receive patches the next time they connect — no device is left behind.

Compliance Benefit

Addresses the **HIPAA Security Rule requirement** to maintain security updates and protect against reasonably anticipated threats. Meets **FINRA expectations** that firms maintain current, secure systems as part of their cybersecurity program.

Software Restriction & Application Control

Unauthorized software on your network is a compliance and security liability. A single unapproved application can introduce malware, create data leakage pathways, or violate regulatory requirements. CBE Inc. monitors and controls what runs on your systems.

Proactive Software Management

- **Software Inventory Monitoring:** SuperOps tracks every application installed across all managed endpoints, providing complete visibility into your software landscape.
- **Unauthorized Software Alerts:** If a non-approved application is installed on any managed device, CBE Inc. is alerted immediately and can take action to investigate and remediate.
- **Approved Software Baselines:** CBE Inc. can define and enforce a list of approved applications via policy, ensuring that only vetted, compliant software operates on your network.

Compliance Benefit

Prevents unauthorized applications that could introduce data leakage or security vulnerabilities — critical for both **HIPAA** (protecting ePHI from unauthorized disclosure) and **FINRA** (maintaining the integrity of systems handling client financial records).

Asset Inventory & Lifecycle Management

You cannot protect what you do not know you have. A complete, accurate inventory of every device and application in your environment is the foundation of any compliance program. CBE Inc. maintains this inventory automatically through SuperOps.

What CBE Inc. Tracks for You

- **Hardware Details:** Make, model, serial number, processor, memory, storage capacity, and warranty status for every managed device.
- **Operating System Information:** OS version, build number, and update status — critical for identifying devices that may be running unsupported software.
- **Installed Applications:** A complete list of every application installed on every device, updated in real time.
- **Network Information:** IP addresses, network adapters, and connectivity status.

Why This Matters for Compliance

Regulators require you to know exactly which devices handle sensitive data. Whether you are conducting a HIPAA risk assessment or updating your FINRA business continuity plan, a current asset inventory is not optional — it is mandatory.

Compliance Benefit

Required for **HIPAA risk assessments** (identifying all systems that create, receive, maintain, or transmit ePHI) and **FINRA Rule 4370** business continuity planning (identifying mission-critical systems and data backup requirements).

Remote Access Auditing

When a technician accesses your systems remotely — whether to resolve a support issue, deploy a patch, or investigate an alert — that access must be documented, secured, and auditable. CBE Inc. ensures complete accountability for every remote session.

Full Session Accountability

- **Technician Identity:** Every remote session is tied to a specific, named technician — no anonymous or shared access.
- **Timestamped Records:** Session start time, end time, and duration are logged automatically.
- **Action Tracking:** Actions performed during each session — files accessed, commands executed, configurations changed — are recorded in the audit trail.
- **Session-Level Controls:** Remote sessions are secured with encryption and require proper authentication before access is granted.

Compliance Benefit

Proves **who accessed what, when, and why** — essential for **HIPAA audit requirements** (§164.312(b) Audit Controls and §164.312(d) Person or Entity Authentication) and **FINRA supervisory obligations** requiring documentation of access to regulated systems.

Business Associate Agreement (BAA) Support

Under HIPAA, any vendor that accesses, stores, or transmits electronic Protected Health Information (ePHI) on behalf of a covered entity must sign a Business Associate Agreement. This creates a legally binding chain of accountability for patient data.

How CBE Inc. Completes the Chain of Custody

- **SuperOps Signs BAAs:** SuperOps, as the underlying platform, executes BAAs with managed service providers, accepting its role as a compliant business associate.
- **CBE Inc. Signs BAAs with Healthcare Clients:** As part of every managed services engagement with healthcare practices, CBE Inc. executes a BAA — formalizing our commitment to protect your patient data.
- **Secure Text Fields:** SuperOps includes a Secure Text Fields feature that encrypts any PHI data stored within the platform — at rest, in transit, and in storage — providing an additional layer of protection for sensitive identifiers.

> ❗ **Why This Matters**
>
> The chain of custody for ePHI runs from **your practice** → through **CBE Inc.** → to the **SuperOps platform**. With BAAs in place at every link, your compliance obligations are documented and enforceable end to end. This is exactly what HIPAA auditors look for.

Compliance Capability Summary

The following table maps each CBE Inc. capability to the specific HIPAA and FINRA requirements it addresses:

Capability	HIPAA Requirement	FINRA Requirement
Device Hardening	Technical Safeguards (§164.312) — Encryption, endpoint protection	Cybersecurity best practices — securing systems handling client data
Access Control	Access Control Standard (§164.312(a)) — Unique user ID, auto logoff, encryption	Rule 3110 — Supervisory systems, authorized access only
Audit Logging & Reporting	Audit Controls (§164.312(b)) — Activity logs, access tracking	Rule 3110 — Evidence of supervisory systems and procedures
Patch Management	Security Rule — Maintain updates, protect against anticipated threats	Cybersecurity guidance — current, secure systems
Software Restriction	Technical Safeguards — Prevent unauthorized ePHI disclosure	System integrity — prevent unauthorized software on regulated systems
Asset Inventory	Risk Assessment — Identify all systems handling ePHI	Rule 4370 — Business continuity planning, mission-critical system identification
Remote Access Auditing	Audit Controls (§164.312(b)) & Authentication (§164.312(d))	Rule 3110 — Documentation of access to regulated systems
BAA Support	Business Associate Requirements (§164.502(e)) — Chain of custody for ePHI	N/A (HIPAA-specific requirement)

Why Choose CBE Inc.?

Compliance is not a one-time checkbox — it is an ongoing commitment. CBE Inc. delivers that commitment through a combination of expert knowledge, proven processes, and the right technology platform.

One Platform. One Partner. Continuous Compliance.

- **Unified Management:** One platform (SuperOps) managing all of your devices, policies, patches, and audit trails — no fragmented tools or visibility gaps.
- **Proactive, Not Reactive:** CBE Inc. does not wait for problems to surface. Automated monitoring, policy enforcement, and patch management keep your systems compliant around the clock.
- **Audit-Ready at All Times:** Detailed logs, exportable reports, and documented procedures mean you are never scrambling to prepare for an examination.
- **Local Expertise:** Based in the Greater Philadelphia area and serving Delaware County, South Jersey, and surrounding communities, CBE Inc. understands the compliance challenges facing small healthcare practices and financial services firms in our region.
- **Trusted Partnership:** We sign BAAs, we maintain documentation, and we stand behind our compliance capabilities — because your regulatory obligations are our responsibility too.

Ready to Get Started?

Contact CBE Inc. today for a **complimentary compliance readiness assessment**. We will evaluate your current IT environment, identify gaps in your compliance posture, and show you exactly how our managed services can close them.

Email: info@cbeinc1.com

Service Area: Greater Philadelphia, Delaware County, and South Jersey

---

CBE Inc. — Compliance-Ready IT Solutions

info@cbeinc1.com | Greater Philadelphia, Delaware County & South Jersey