BTI COMMUNICATIONS GROUP · HEALTHCARE ADVISORY SERIES · 2026

Healthcare Security Systems Guide 2026

How Healthcare Organizations Modernize Physical Security, Cybersecurity, Compliance, and Infrastructure Without Creating Operational Chaos

A comprehensive operational guide for healthcare CIOs, IT Directors, Compliance Leaders, Facilities Directors, and Security Leadership navigating the convergence of physical security, cybersecurity, and infrastructure governance.

24	$10.9M	2026
Chapters covering the full healthcare security lifecycle	Average cost of a healthcare data breach in 2024	Current edition - updated for today's threat and compliance environment

Converged IT · Cybersecurity · Physical Security · VoIP · Compliance

btigroup.com · 800-435-7284 · info@btigroup.com

NAVIGATION

Table of Contents

This guide covers the full spectrum of healthcare security infrastructure - from physical access control and video surveillance to cybersecurity, compliance, and AI-enabled operations.

EXECUTIVE AUDIENCE

Who This Guide Is For

This guide is written for the leaders responsible for healthcare security, compliance, infrastructure, and operational resilience.

Healthcare CIOs & IT Directors

Responsible for infrastructure strategy, vendor governance, and technology investment decisions across the organization.

Compliance & Privacy Leaders

Navigating HIPAA, HITECH, and emerging regulatory requirements with documented controls and audit-ready systems.

Facilities & Security Directors

Managing physical access, surveillance, workplace safety, and the operational security of clinical environments.

Multi-Site Healthcare Groups

Regional health systems, physician groups, and networks operating across multiple campuses or locations.

Ambulatory Surgery Centers & Imaging Organizations

High-acuity outpatient environments requiring enterprise-grade security with lean operational teams.

Regional Clinic Networks

Primary care and specialty networks scaling security and compliance infrastructure across distributed sites.

If you are responsible for protecting patients, data, staff, or operations - this guide was written for you.

2026 EDITION

Executive Summary

Healthcare organizations face rising pressure from ransomware, workplace violence, compliance demands, and aging infrastructure. Fragmented security tools and siloed vendors no longer provide enough visibility or control. The result is higher risk, higher cost, and slower response.

Key Findings

Healthcare has the highest average breach cost of any sector.

Ransomware activity against healthcare has nearly doubled since 2020.

Surveyors and insurers are demanding stronger logs, controls, and proof of readiness.

Multi-site operations require centralized oversight, not disconnected local systems.

Cybersecurity, physical security, and infrastructure now depend on one another.

Strategic Recommendation

Adopt a converged security model that unifies physical security, cybersecurity, IT infrastructure, VoIP, and compliance under one governance structure. Prioritize shared visibility, standardized policies, and centralized incident response. Reduce vendor sprawl before expanding new tools.

INDUSTRY INTELLIGENCE · 2026

Strategic Themes Defining Healthcare Security in 2026

Ten converging forces are reshaping how healthcare organizations design, govern, and operate their security and infrastructure environments.

Cyber-Physical Convergence

Physical security systems are now cyber assets. IP cameras, badge readers, and access control servers require the same governance as any managed network endpoint.

AI-Assisted Monitoring

Artificial intelligence is enabling continuous behavioral detection, forensic search, and anomaly identification at a scale no human monitoring team can match.

Centralized Governance

Multi-site healthcare organizations are consolidating security oversight into unified platforms, replacing fragmented vendor relationships with single-pane operational visibility.

Compliance Automation

Manual audit preparation is giving way to automated log retention, continuous compliance dashboards, and real-time documentation aligned to HIPAA and OCR requirements.

Operational Resilience

Security infrastructure is now evaluated not just for protection capability, but for its ability to maintain clinical operations during ransomware events, power failures, and natural disasters.

Infrastructure Standardization

Healthcare organizations are replacing legacy, site-specific deployments with standardized architecture frameworks that ensure consistent security posture across every location.

Multi-Site Visibility

Centralized dashboards and cloud-managed platforms are enabling security and IT leaders to monitor, manage, and respond across distributed environments from a single interface.

Insurer-Driven Controls

Cyber insurance underwriters are now requiring documented MFA, segmentation, audit trails, and DR testing as conditions of coverage - effectively setting minimum security architecture standards.

IoT Governance

The proliferation of connected medical devices, cameras, and building systems has created a new governance discipline: managing firmware, credentials, and network isolation for every connected endpoint.

Zero-Trust Architecture

Healthcare organizations are moving away from perimeter-based security toward identity-verified, least-privilege access models that assume breach and limit lateral movement.

SELF-ASSESSMENT TOOL

Healthcare Security & Compliance Maturity Snapshot

Use this scorecard to benchmark your organization's current security posture across ten critical operational domains.

Assessment Domain	Reactive	Managed	Mature	Optimized
MFA Deployment	No MFA on critical systems	MFA on select systems	MFA enforced org-wide	Adaptive MFA with risk scoring
VLAN Segmentation	Flat network architecture	Basic segmentation	Security VLANs isolated	Zero-trust micro-segmentation
SIEM Integration	No centralized logging	Partial log aggregation	SIEM deployed and monitored	AI-enhanced threat correlation
Visitor Management	Paper logs or no system	Digital check-in at entry	Integrated with access control	Real-time credentialing + audit trail
Firmware Governance	Unknown device firmware	Ad hoc patching	Scheduled firmware cycles	Automated patch management
Centralized Audit Logs	Siloed or no audit logs	Partial log retention	Centralized, searchable logs	Automated compliance reporting
Disaster Recovery Testing	No formal DR plan	DR plan exists, untested	Annual DR testing	Quarterly tested + documented
Credential Lifecycle Mgmt	Manual provisioning	Basic offboarding process	Role-based access control	Automated lifecycle management
Backup Connectivity	Single ISP, no failover	Secondary ISP available	Automatic failover configured	SD-WAN with real-time monitoring
Compliance Reporting	Manual, reactive	Periodic manual reports	Scheduled compliance reports	Continuous automated reporting

> Organizations at the Optimized tier consistently outperform peers on cyber insurance terms, OCR audit outcomes, and operational incident response times.

SECTION ONE

Understanding the Threat Environment

Ransomware. Workplace violence. Regulatory pressure. Aging infrastructure. The healthcare threat landscape has never been more complex - or more consequential.

> **Healthcare data breaches cost an average of $10.9 million per incident in 2024 - the highest of any industry for the 14th consecutive year.**

Covers: The Healthcare Threat Landscape · Why Traditional Security Models Fail

RISK INTELLIGENCE

The Healthcare Threat Landscape

Healthcare faces simultaneous physical and cyber threats that are deeply interconnected. A propped door, an unpatched camera, or an unsecured network can all become entry points. Modern risk requires a converged response.

> Healthcare data breaches cost an average of $10.9 million in 2024 - the highest of any industry for the 14th consecutive year. (IBM Cost of a Data Breach Report)

Ransomware

Healthcare ransomware attacks increased 94% from 2021 to 2023, with average recovery costs exceeding $1.27M per incident.

Workplace Violence

Healthcare workers experience workplace violence at rates 5x higher than other industries.

Medication Diversion

Inadequate access control and surveillance in pharmacy and medication storage areas create patient safety and compliance risks.

HIPAA Exposure

OCR enforcement actions increasingly cite insufficient technical and physical safeguards as primary findings in breach investigations.

The healthcare threat landscape is not a series of isolated incidents - it is a system of interconnected vulnerabilities that compound each other.

> "The healthcare threat environment is no longer separable into physical and cyber categories. Security strategy must reflect this reality."

A ransomware attack that locks clinical staff out of EHR systems is simultaneously a safety event - and a tailgating incident can also be a cybersecurity event.

> "A disconnected security system is also a cybersecurity risk. Physical and digital threats do not operate in silos - and neither should your defenses."

CRITICAL ANALYSIS

Why Traditional Security Models Fail Healthcare

Most healthcare organizations have built security and IT environments incrementally over years. The result is a fragmented technology stack with no unified governance, limited visibility, and weak accountability. That structure creates operational and compliance risk.

Fragmented Model

Separate Vendors

Multiple contracts with no integration or clear ownership.

Siloed Systems

No centralized logging, shared dashboards, or cross-system correlation.

Compliance Gaps

Disconnected tools create incomplete logs, delayed fixes, and audit risk.

Operational Risk

These gaps increase downtime, incident exposure, and financial impact.

Converged Model

Unified Platform

Physical Security, Cybersecurity, IT Infrastructure, VoIP, and Compliance connected in one operating model.

Central Management Dashboard

Unified reporting, shared visibility, and a single source of operational truth.

Single Accountability

Clear ownership across systems, vendors, and governance responsibilities.

HIPAA-Aligned Governance

Integrated controls support consistent oversight, faster response, and stronger compliance posture.

> "Fragmented technology is not a budget-saving strategy. It is an unmanaged liability that compounds over time."

Strategic Recommendation: Before purchasing new security technology, conduct a full-environment assessment that maps existing systems, identifies integration gaps, documents compliance posture, and produces a prioritized remediation roadmap.

SECTION TWO

Converged Security Infrastructure

Physical security, cybersecurity, IT infrastructure, communications, and compliance - unified into a single, governed operational framework.

> *"Converged security infrastructure is not a technology decision. It is an organizational governance commitment - one that determines how effectively a healthcare organization can detect, respond to, and recover from operational threats."*

Covers: Converged Infrastructure · Access Control · Video Surveillance · Cyber-Physical Convergence

---

btigroup.com · 800-435-7284 · info@btigroup.com

CORE FRAMEWORK

What Is Converged Security Infrastructure?

Converged Security Infrastructure is the deliberate integration of physical security, cybersecurity, IT infrastructure, communications, and compliance governance into a unified operational framework. It replaces isolated vendor silos with one coherent enterprise system. For executive teams, the key shift is to treat security as an architectural decision and a governance commitment.

> **Converged infrastructure is not a product. It is an architectural decision - and a governance commitment.**

Physical Security

Cameras, access control, perimeter protection

Cybersecurity

SIEM, MFA, patching, zero trust

IT Infrastructure

Switching, Wi-Fi, SD-WAN, UPS

Comms & Compliance

VoIP paging, unified comms, audits

Physical Security

Access control, video surveillance, visitor management, and perimeter protection are managed on one platform with centralized audit trails.

Cybersecurity

Network segmentation, MFA, SIEM integration, and zero trust treat every connected security device as a managed cyber asset.

IT Infrastructure

Managed switching, enterprise Wi-Fi, SD-WAN, and failover connectivity support continuity across all locations.

VoIP & Emergency Comms

Unified communications, emergency paging, and mass notification keep teams connected during operational events.

Compliance Relevance: HIPAA's Security Rule requires reasonable and appropriate safeguards for ePHI. Converged infrastructure provides unified audit trails, correlated access logs, and documented network segmentation across administrative, physical, and technical safeguards.

> **Healthcare resilience depends on operational convergence. Fragmented tools create fragmented outcomes - and fragmented risk.**

REFERENCE ARCHITECTURE · BTI FRAMEWORK

The Converged Healthcare Security Architecture

BTI Converged Security Reference Architecture

Five Integrated Pillars - One Unified Operations Hub

Physical Security

Access control, video surveillance, visitor management, and intrusion detection - unified under one governance framework

Cybersecurity

Endpoint protection, SIEM, zero-trust architecture, and email security integrated with physical systems

IT Infrastructure

Network switching, SD-WAN failover, UPS power resilience, and cloud infrastructure

Communications

VoIP, emergency notification, cellular failover, and unified communications

Compliance & Governance

HIPAA audit trails, risk assessment, incident documentation, and cyber insurance readiness

> A converged architecture does not just improve security. It creates the operational foundation for compliance, resilience, and scalable governance across every location.

Unified Audit Trail

Single, tamper-evident log across all systems and locations

Compliance Automation

Continuous HIPAA documentation, always audit-ready

Operational Resilience

Redundant connectivity and failover across all critical systems

Lifecycle Governance

Firmware, credentials, and access managed proactively

This reference architecture illustrates the integration of physical security, cybersecurity, IT infrastructure, communications, and compliance governance into a unified operational framework. Actual deployments are customized to each organization's environment, scale, and governance requirements.

---

btigroup.com · 800-435-7284 · info@btigroup.com

PHYSICAL SECURITY

Access Control for Healthcare Organizations

Healthcare access control is a core compliance, security, and patient safety system across every physical touchpoint in your organization. Under HIPAA Physical Safeguards, covered entities must control and validate facility access based on role or function. For healthcare teams, access control is not optional - it is a required safeguard.

Key Access Control Capabilities

- Credential lifecycle management from onboarding to offboarding
- Restricted access for pharmacy, data center, and behavioral health areas
- Mobile credentials via smartphone apps
- Remote lockdown and emergency access controls
- Multi-site administration from a single console
- Visitor management and contractor tracking
- Audit trails synchronized with SIEM and compliance systems
- HR system integration for automated provisioning

Pharmacy access control must document who entered controlled areas and when. A cloud-based platform with immutable audit logs supports DEA inspections, pharmacy board reviews, and internal compliance needs.

Visitor management integration connects front desk workflows, contractor credentials, and patient escort protocols into one documented chain-of-custody. That makes day-to-day operations cleaner and access decisions easier to audit.

01

Assess

Audit door hardware, credential inventory, and access zones across all locations.

02

Design

Map access zones to roles, compliance needs, and emergency protocols.

03

Deploy

Install enterprise hardware and cloud management with minimal disruption.

04

Manage

Maintain credential governance, audit reporting, and system lifecycle oversight.

> When a staff member is terminated, their credentials should be revoked across every location within minutes - not discovered as still-active during a compliance audit.

PHYSICAL SECURITY

Video Surveillance for Healthcare

Healthcare video surveillance has shifted from a reactive evidence tool to an operational intelligence platform. It now delivers real-time situational awareness, AI-enabled analytics, and forensic-grade documentation. For healthcare organizations, that shift is both an operational opportunity and a compliance obligation.

> Every IP camera is a network endpoint. Healthcare organizations that treat cameras as "just hardware" are operating with a fundamental cybersecurity blind spot.

AI-Enabled Analytics

Modern platforms detect anomalies, loitering, unauthorized access attempts, and crowd density in real time.

Perimeter & Parking Safety

AI-enabled perimeter cameras extend security coverage to parking lots, loading docks, and building exteriors.

Cloud vs. On-Premise Storage

Cloud storage reduces NVR vulnerability while supporting encrypted retention and remote forensic search.

Evidence retention policies must align with HIPAA, state law, and legal hold requirements. An enterprise video surveillance platform should provide configurable retention schedules, role-based access, chain-of-custody documentation, and encrypted storage.

Compliance Impact

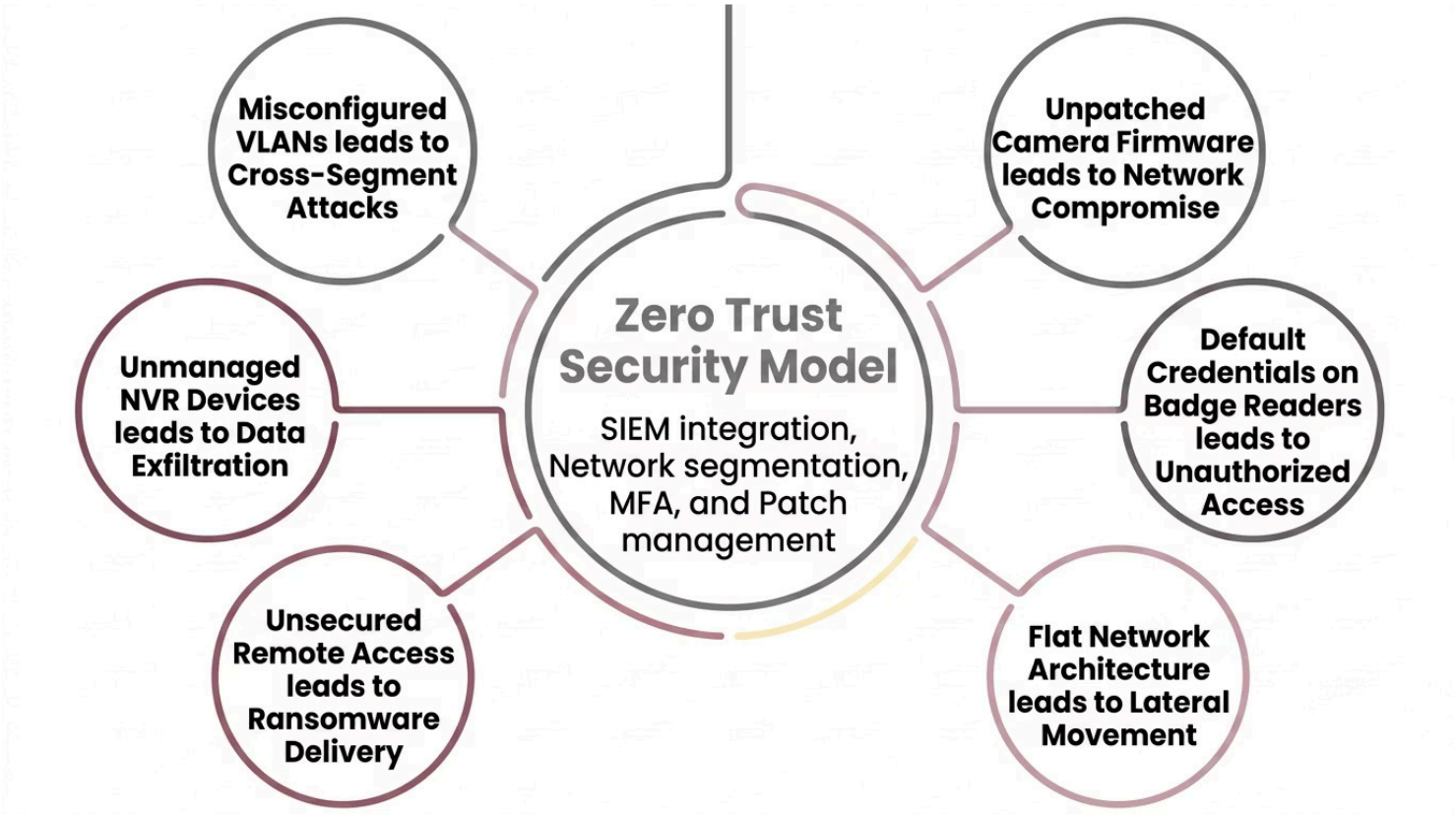
Video surveillance records are often requested in HIPAA breach investigations, Joint Commission surveys, and workplace violence reviews. Organizations without documented retention policies, access logs, and audit trails face significant compliance exposure.

> "The question is no longer whether your healthcare organization has cameras. The question is whether your cameras are managed, patched, integrated, and compliant - or whether they are an unmanaged cyber liability posing as a security asset."

CYBER-PHYSICAL CONVERGENCE

Cybersecurity & Physical Security Systems: The Inseparable Connection

Every IP camera, badge reader, access control server, and NVR on your network is a cyber asset. These devices run firmware, authenticate to network infrastructure, and store or transmit sensitive data. In healthcare, that makes physical security systems both an operational tool and a cybersecurity responsibility.



Network Segmentation

Place security devices on dedicated VLANs isolated from clinical systems, with firewall rules controlling any inter-VLAN access.

Firmware Lifecycle

Track firmware versions and patch security devices on a documented schedule tied to manufacturer updates and CVE advisories.

MFA & Zero Trust

Require MFA and role-based access for VMS, access control consoles, and NVRs.

SIEM Integration

Send authentication, access, and device health events into the SIEM for correlation and alerting.

> Physical security devices are IoT endpoints. They require the same cybersecurity discipline as any other network-connected asset.

Recommended Action

- Inventory all IP-connected security devices.
- Document firmware versions and patch status.
- Verify network segmentation and changed default credentials.
- Confirm SIEM monitoring coverage for these devices.

CYBER INSURANCE & GOVERNANCE

Why Cyber Insurance Underwriters Are Scrutinizing Healthcare Security Infrastructure

Cyber insurance underwriters have fundamentally changed their evaluation criteria. What was once a questionnaire about antivirus software and firewalls is now a rigorous operational audit of your security architecture, governance practices, and documented controls. For healthcare organizations, the stakes are especially high - and the scrutiny is intensifying.

What Underwriters Are Now Requiring

Multi-Factor Authentication - MFA must be enforced on all privileged accounts, remote access, and clinical systems. Absence of MFA is now a primary coverage denial trigger.

Network Segmentation - Underwriters require documented VLAN segmentation separating clinical, administrative, IoT, and guest traffic. Flat networks are considered uninsurable at scale.

Audit Trails & Logging - Centralized, tamper-evident audit logs with defined retention periods are required for both cyber and physical security systems.

Unmanaged IoT Governance - IP cameras, badge readers, and medical devices on unmanaged networks represent unquantifiable risk. Underwriters require documented device inventories and firmware governance.

Disaster Recovery Testing - Documented, tested, and dated DR plans are required. Untested plans are treated as non-existent.

Compliance Documentation - HIPAA-aligned policies, risk assessments, and training records must be current, accessible, and audit-ready.

The Operational Governance Imperative

The requirements above are not cybersecurity checkboxes. They are operational governance requirements - the same disciplines that define a mature, resilient healthcare organization. Organizations that treat cyber insurance compliance as a standalone IT exercise consistently underperform on both coverage outcomes and operational security posture.

BTI frequently designs phased modernization strategies that address the highest-priority underwriter requirements first - MFA, segmentation, and audit logging - while building toward a fully optimized governance posture over time.

67%

of healthcare organizations that experienced a ransomware event had no documented network segmentation at time of breach

3×

higher premiums for organizations without MFA on privileged access

$10.9M

average cost of a healthcare data breach in 2024 (IBM Security)

> "The organizations that earn the best cyber insurance terms are the same ones that have built operationally mature security infrastructure - not the ones that filled out a form."

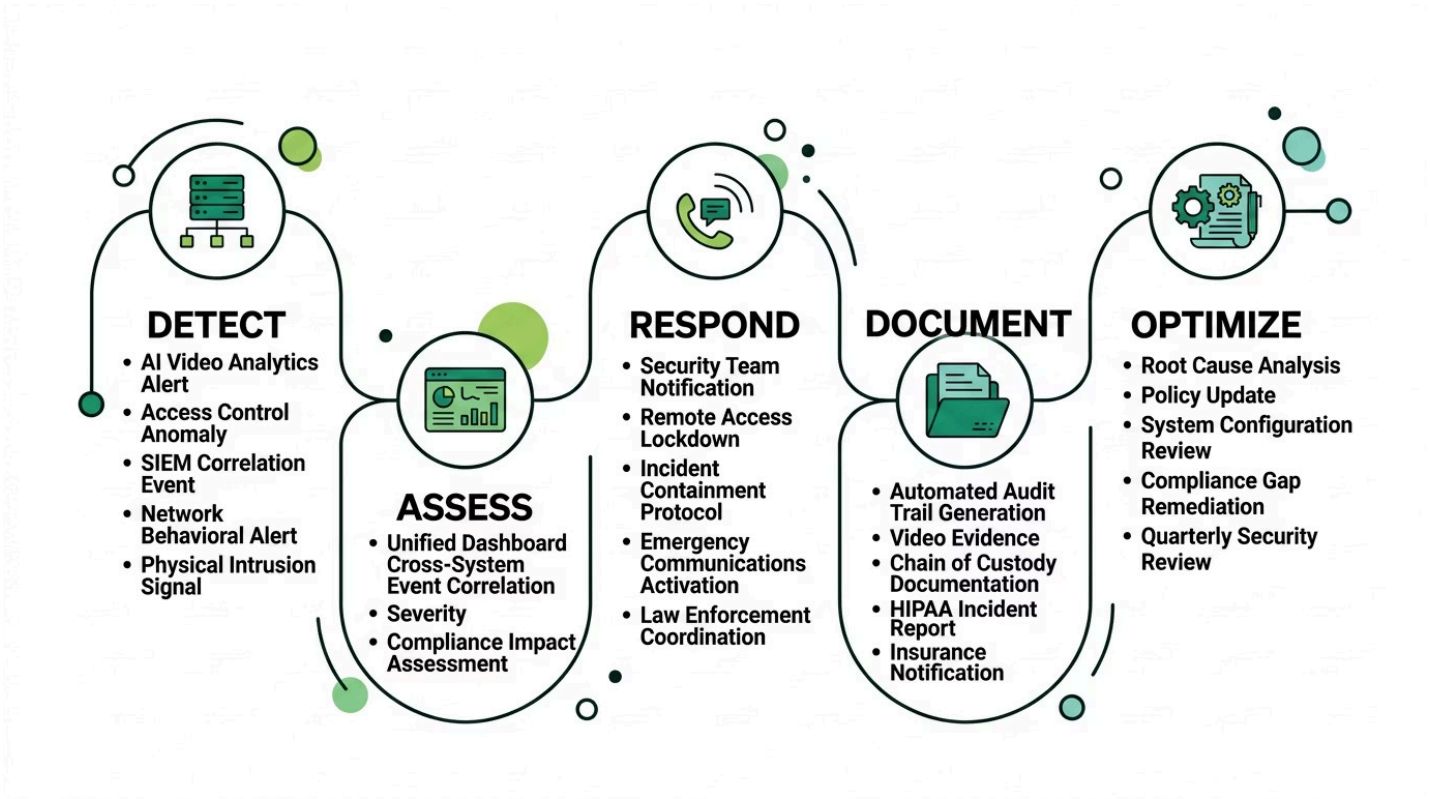
Source: IBM Cost of a Data Breach Report 2024; industry underwriting data. Statistics cited for informational purposes.

btigroup.com · 800-435-7284 · info@btigroup.com

OPERATIONAL FRAMEWORK

Healthcare Security Operations: From Detection to Resolution

How a converged security infrastructure transforms incident detection, response, and compliance documentation across the healthcare enterprise.



> *"A converged security infrastructure compresses the time between detection and resolution - and ensures every incident generates the documentation required for compliance, insurance, and operational review."*

---

btigroup.com · 800-435-7284 · info@btigroup.com

SECTION THREE

Compliance, Operations & Resilience

HIPAA. Multi-site visibility. Network infrastructure. Business continuity. The operational disciplines that keep healthcare organizations compliant, connected, and resilient.

4

Disciplines

Compliance, operations, infrastructure, continuity

1

Framework

Governance across sites and systems

> "Compliance, operational continuity, and infrastructure resilience are not separate disciplines. In a mature healthcare security environment, they are the same discipline - governed by the same architecture, the same audit trails, and the same operational team."

Covers: Compliance & Audit Readiness · Multi-Site Operations · Network Infrastructure · Business Continuity

COMPLIANCE & GOVERNANCE

Healthcare Compliance & Audit Readiness

HIPAA compliance is not a checkbox - it is an ongoing operational discipline that requires documented policies, technical controls, audit trails, and continuous governance. OCR enforcement actions have also made clear that physical access controls and audit logs are required, and organizations that cannot produce evidence of these controls can face significant civil monetary penalties. The result is a compliance environment that demands integrated, automated, and auditable systems.

Compliance Domains Requiring Technology Controls

- **HIPAA Technical Safeguards**

  Access, audit, integrity, and transmission controls require documented implementation and ongoing monitoring.

- **Physical Safeguards**

  Facility access, workstation security, and device controls require badge systems, surveillance, and visitor management.

- **Cyber Insurance Requirements**

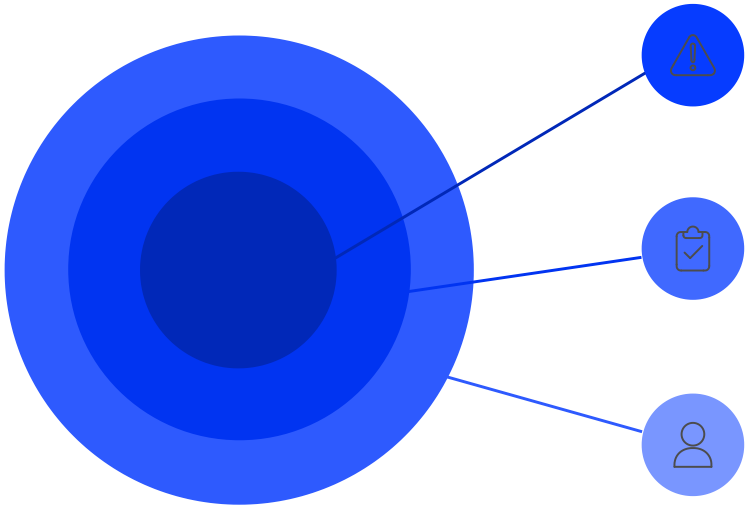
  MFA, endpoint protection, network monitoring, backup, and training are increasingly required for coverage renewal.

- **Joint Commission Standards**

  Environment of care, workplace safety, and emergency management require documented access and response capabilities.

Audit Readiness Checklist

- Unified access control audit logs across all locations
- Video evidence retention policy documented and enforced
- Credential lifecycle documentation (hire to terminate)
- Network segmentation diagrams current and accurate
- Firmware patch history for all connected security devices
- Incident response plan tested and current
- Business associate agreements with all technology vendors
- SIEM alerts and investigation logs retained per policy
- Annual risk assessment completed and documented
- Cyber Insurance application data current and accurate



Reactive

Manual processes, fragmented systems, audit failures.

Structured

Documented policies, integrated systems, scheduled audits.

Optimized

Automated governance, real-time monitoring, AI detection.

> Audit readiness is not a project. It is an operational posture - maintained every day, not assembled when a surveyor calls.

> Compliance is now architectural. It cannot be retrofitted into a system that was never designed to support it.

ENTERPRISE OPERATIONS

Multi-Site Healthcare Operations: Centralized Visibility at Scale

For healthcare organizations operating across multiple locations, each site multiplies risk, compliance burden, and operational complexity. A 15-location group without centralized visibility can end up with separate systems at every site and no way to correlate events across locations. In practice, that creates both a security liability and a measurable cost challenge.

> A multi-site organization without centralized logging cannot demonstrate HIPAA audit control compliance. Each disconnected location is a separate compliance gap.

Centralized Management Platform

A unified platform consolidates access control, video, alarms, and network health into one dashboard. Authorized teams can monitor and respond from any device, anywhere.

Standardized Deployment Framework

A master design specification helps replicate a consistent security and infrastructure stack across new sites. That creates repeatable compliance documentation and more predictable operations.

Remote Management & Support

BTI's GlobalView platform provides 24/7 monitoring, proactive health checks, firmware management, and rapid response support. It reduces the need for on-site IT staff while preserving enterprise-grade visibility.

> Centralized visibility is not a convenience. For multi-site healthcare organizations, it is a compliance requirement and an operational imperative.

BTI frequently designs phased multi-site modernization strategies that prioritize the highest-risk locations first, establishing a repeatable deployment standard that reduces cost and complexity with each subsequent site.

> Multi-site healthcare organizations that standardize their security architecture across locations gain a compounding governance advantage - each new site opens compliant, not remediated.

---

btigroup.com · 800-435-7284 · info@btigroup.com

BTI GLOBALVIEW PLATFORM

Unified Visibility Through GlobalView

A centralized operations platform purpose-built for multi-site healthcare security, compliance, and infrastructure management. GlobalView capabilities may be deployed individually or as part of broader managed services engagements, depending on organizational requirements and operational preferences.

Platform Capabilities

Centralized Dashboards

Unified visibility across all sites, systems, and security domains from a single operational interface. Real-time status, alerts, and system health at a glance.

Intelligent Alerting

Configurable alert thresholds with escalation workflows. Critical events surface immediately; routine notifications are filtered and prioritized.

Remote System Management

Manage access control, video surveillance, network infrastructure, and security devices across all locations without dispatching on-site personnel.

Compliance Visibility

Automated compliance dashboards aligned to HIPAA Physical Safeguards, audit log requirements, and access control documentation standards.

Multi-Site Oversight

Normalized views across disparate sites, vendors, and system generations. Consistent governance regardless of location or legacy infrastructure.

Incident Escalation Workflows

Structured escalation paths from detection to resolution, with documented response timelines for compliance and post-incident review.

Operational Analytics

Trend analysis, utilization reporting, and security posture scoring to support strategic planning and board-level reporting.

Why GlobalView Matters

Most healthcare organizations manage security reactively - responding to incidents after they occur, with limited visibility into what is happening across their environment. GlobalView changes the operational model. Instead of fragmented dashboards, siloed alerts, and manual reporting, security and IT leaders gain a single, authoritative view of their entire security and infrastructure posture.

GlobalView is not a one-size-fits-all platform. Organizations may deploy individual capabilities - such as compliance dashboards or alerting - or leverage the full platform as part of a managed services engagement. Monitoring scope, escalation workflows, and reporting cadences are configured to match each organization's internal structure and governance model.

> Visibility is not a feature. It is the foundation of operational governance.

GlobalView Delivers

- Configurable security posture visibility across selected sites and systems
- Compliance documentation support, continuously updated based on engagement scope
- Proactive incident detection and response options aligned to organizational needs

btigroup.com · 800-435-7284 · info@btigroup.com

IT INFRASTRUCTURE

Network Infrastructure: The Foundation of Healthcare Security

Every physical security system, cybersecurity tool, clinical application, and communication platform in your healthcare organization runs on your network infrastructure. In healthcare, the network is clinical infrastructure, and when it fails or is compromised, patient care and patient data are at risk. That is why network gaps create some of the most dangerous operational and security exposures.

Compliance Relevance

Network segmentation documentation is increasingly required by cyber insurance underwriters and HIPAA auditors. Organizations that cannot produce a current, accurate network architecture diagram showing ePHI system isolation face compliance and insurance exposure.

Cisco Meraki Managed Switching

Cloud-managed switching provides VLAN segmentation, port security, and centralized visibility across all locations.

Enterprise Wi-Fi

Healthcare-grade wireless architecture isolates clinical, IoT, guest, and security traffic while supporting mobile workflows.

SD-WAN Connectivity

Software-defined WAN prioritizes clinical applications and security systems with automatic failover for continuity.

UPS & Power Resilience

Managed UPS systems keep security, communications, and network infrastructure operational through power events.

> Network infrastructure is not a utility. In healthcare, it is a patient safety system.

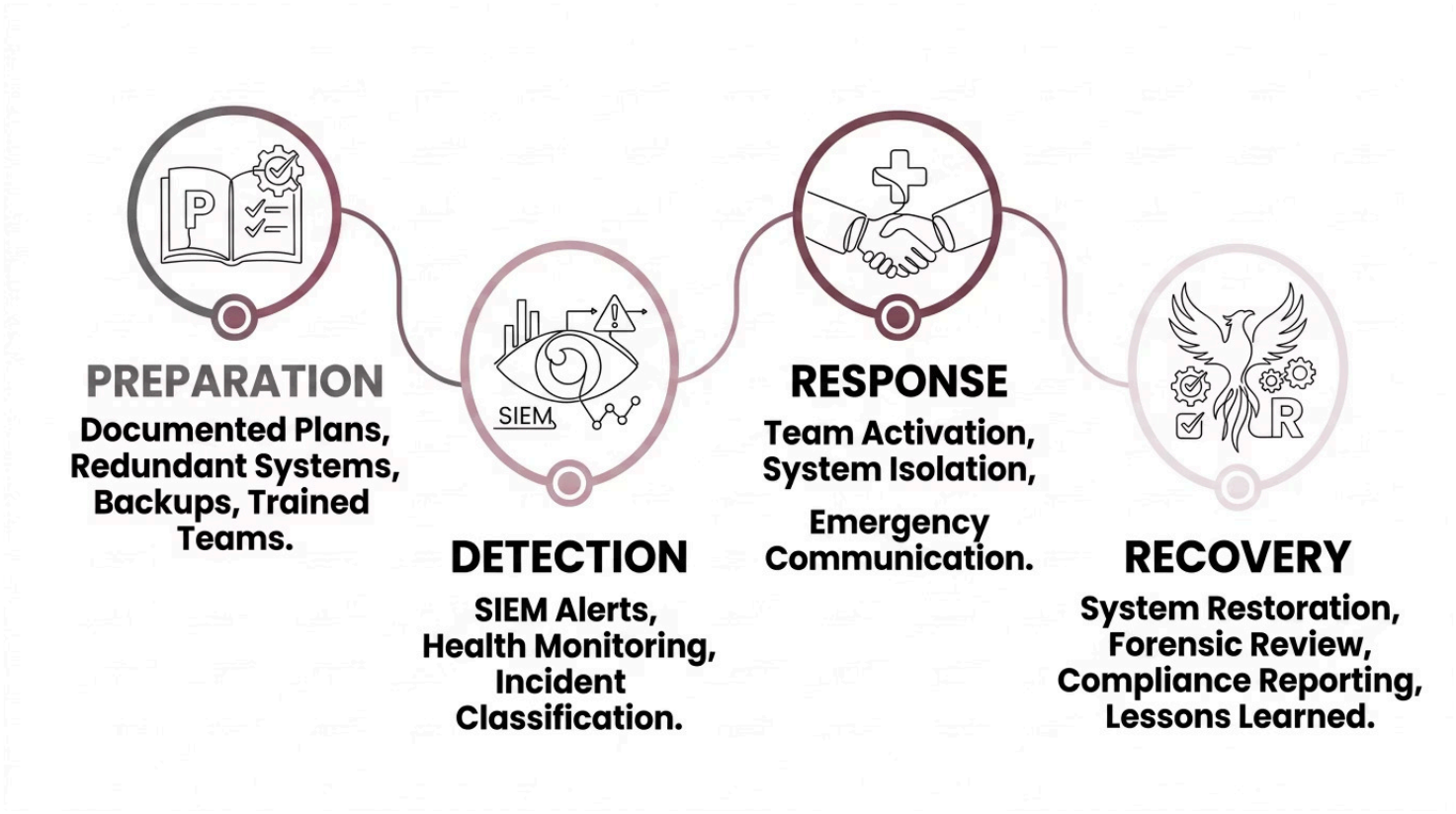
---

btigroup.com · 800-435-7284 · info@btigroup.com

OPERATIONAL RESILIENCE

Business Continuity & Disaster Recovery for Healthcare

Healthcare organizations cannot afford downtime. When systems fail - due to ransomware, power failure, natural disaster, hardware failure, or vendor abandonment - patient care, staff safety, and regulatory compliance are all at risk. Ransomware recovery can take 18-21 days, and the cost of downtime is multi-dimensional: diverted patients, delayed procedures, safety incidents, and manual workarounds.



Critical Continuity Capabilities

- Redundant recording - local + cloud backup for video surveillance
- Offline access control - credential caching for door operation during network outages
- VoIP failover to cellular or PSTN during internet outages
- SD-WAN automatic failover between primary and backup WAN circuits
- UPS runtime sufficient for ordered shutdown or generator transfer
- Cloud-based security management accessible during on-site infrastructure failures

Rapid recovery requires documented procedures, trained personnel, and tested response playbooks. BTI's managed services model includes quarterly continuity testing and documented recovery procedures for all managed systems.

Cyber insurance carriers increasingly require documented business continuity and disaster recovery plans. Organizations without tested recovery capabilities face premium increases, coverage limitations, or denied claims after cyber incidents.

> Business continuity is not a technology project. It is a patient safety obligation.

BTI designs business continuity and disaster recovery capabilities as modular components - organizations may implement individual elements or a comprehensive continuity framework based on operational requirements and risk tolerance.

SECTION FOUR

AI, Intelligence & the Future of Healthcare Security

Artificial intelligence is transforming what is operationally possible - from predictive threat detection to automated compliance monitoring.

By 2027, AI-assisted monitoring is projected to reduce mean time to detection for physical security incidents by over 60% in enterprise healthcare environments.

Covers: AI & The Future of Healthcare Security · The BTI Approach

FORWARD-LOOKING INTELLIGENCE

AI & the Future of Healthcare Security

Artificial intelligence is reshaping what is possible in healthcare security operations. Tasks that once required constant human monitoring can now run continuously, automatically, and at scale. For healthcare organizations with limited staff and growing complexity, AI-enabled security is becoming an operational necessity.

> The most significant near-term AI impact in healthcare security is operational, not dramatic. Fewer false positives. Faster detection. Automated compliance documentation.

Behavioral Detection

AI detects anomalies such as unauthorized entry, after-hours access, and aggressive behavior in real time.

Forensic Intelligence Search

AI search cuts investigation time by letting teams query footage by appearance, time, location, or behavior.

Operational Intelligence

Occupancy and flow analytics improve patient experience, staffing, and workflow efficiency.

AI Governance

Healthcare AI requires clear rules for privacy, retention, bias, and regulatory compliance.

Executive recommendation

- Prioritize explainability so the system can document why it flagged an event.
- Verify HIPAA alignment and privacy controls before deployment.
- Confirm integration with your SIEM and compliance reporting workflows.

> The future of healthcare security is not more cameras or more alerts. It is intelligent infrastructure that knows the difference between noise and threat.

BTI FRAMEWORK

The BTI Approach: From Assessment to Optimization

BTI Communications Group uses a PMO-driven methodology for healthcare security and infrastructure projects. The process starts with a vendor-neutral assessment and carries through design, deployment, and ongoing optimization. This creates a consistent operational outcome across projects of different complexity and scale.

Flexible Operating Models

BTI aligns services to each organization's internal capabilities, staffing model, compliance requirements, and operational preferences.

Fully Managed Services

BTI assumes full operational responsibility for monitoring, maintenance, and compliance governance.

Co-Managed Operations

BTI works alongside internal IT, facilities, or security teams with clearly defined responsibilities.

Internal Team Augmentation

BTI supplements existing staff with specialized expertise, project management, or lifecycle support.

Project-Only Deployments

Scoped design, procurement, and installation engagements with no ongoing managed services requirement.

Lifecycle Support Engagements

Ongoing firmware governance, credential management, and compliance reporting without full managed services.

Hybrid Governance Structures

Custom service structures combining elements of managed, co-managed, and project-based support.

BTI's converged model creates one vendor relationship, one support contract, and one accountability structure. It also gives healthcare teams one operational partner who understands the full technology environment and the context it serves. BTI frequently designs phased modernization strategies that preserve operational continuity while prioritizing the highest-risk operational and compliance areas first. This approach aligns technology investment to organizational risk tolerance, budget cycles, and internal resource capacity.

> The assessment comes first. The design follows the assessment. The deployment follows the design. Managed services ensure the investment performs over time.

1. Assess

Evaluate infrastructure, security posture, compliance gaps, vendor landscape, and operational requirements.

2. Design

Develop converged security and infrastructure architecture with clear documentation standards.

3. Procure

Source enterprise-grade hardware and software through BTI's manufacturer partner ecosystem.

4. Configure & Install

Manage installation, configuration, testing, and commissioning with documented quality controls.

5. Secure

Harden deployed systems with credential controls, VLANs, firmware updates, MFA, and SIEM integration.

6. Support & Optimize

BTI can provide ongoing monitoring, maintenance, lifecycle management, compliance reporting, and optimization through GlobalView.

> The right partner does not sell you products. They build you a system - and stand behind it operationally.

Not every healthcare organization requires the same operational model. BTI designs solutions around existing internal capabilities, regulatory requirements, geographic footprint, and organizational risk tolerance.

SECTION FIVE

Client Success Stories

Real-world outcomes from healthcare organizations that have modernized their security and infrastructure.

> *Healthcare organizations that have modernized their security infrastructure report measurable improvements in compliance audit outcomes, cyber insurance terms, and operational incident response times.*

Covers: Multi-Site Clinic Network Modernization · Regional Ambulatory Surgery & Imaging Group

94%

Audit Outcomes

of healthcare organizations report improved audit outcomes after security infrastructure modernization

18-21 days

Operational Disruption

average operational disruption following an unmitigated ransomware event

3x

Insurance Terms

improvement in cyber insurance terms for organizations with documented, tested security governance

CLIENT SUCCESS | MULTI-SITE HEALTHCARE

Case Study: Multi-Site Clinic Network Modernization

Organization Type: Regional primary care and specialty clinic group

Locations: 12 clinics across 3 states

Staff Count: 340 clinical and administrative employees

Core Challenge: Fragmented security and IT infrastructure with no centralized visibility and active compliance concerns

12 clinics. 3 states. 7 camera vendors. Zero centralized visibility.

The Challenge

This clinic network had grown through acquisition, leaving each location with different cameras, access control systems, and network configurations. The result was credential sprawl, inconsistent oversight, and a compliance posture that exposed the organization to HIPAA and insurance risk.

BTI designed a phased modernization strategy that preserved operational continuity while prioritizing the highest-risk compliance and security gaps first.

The Solution

BTI standardized access control governance across all locations, established centralized compliance visibility, and documented network segmentation to strengthen oversight. Managed monitoring and GlobalView services were aligned to support ongoing governance, response consistency, and audit readiness.

Strategic Outcomes

Centralized Governance

Unified oversight across all clinic locations

Compliance Maturity

Standardized posture aligned to HIPAA Physical Safeguards

Operational Resilience

Unified incident response workflows improved speed and consistency

Scalable Modernization

Infrastructure foundation supports future multi-site expansion

Key Outcomes

12
Locations unified

23
HIPAA findings remediated

65%
Faster incident response

$180K
Annual vendor cost reduction

> The organization renewed its cyber insurance at favorable terms. The compliance consultant who identified the original 23 findings provided a formal clearance letter following modernization.

CLIENT SUCCESS | ASC & IMAGING

Case Study: Regional Ambulatory Surgery & Imaging Group

Organization Type: ASC and diagnostic imaging group

Locations: 8 ASCs and 4 imaging centers

Staff Count: 220 clinical and operational employees

Core Challenge: Compliance pressure from Joint Commission and state health department, rapid expansion creating infrastructure inconsistency, insecure remote locations with no IT oversight

8 ASCs. 4 imaging centers. Four different camera brands. No central monitoring. Zero standardization.

The Challenge

The organization expanded quickly without a standard technology governance model, leaving each new site with inconsistent cameras, access control, firewall settings, and no central monitoring. Joint Commission surveyors identified access control and surveillance deficiencies, while state inspectors cited visitor management gaps. Cyber insurance reviews also exposed a documentation problem: no clear record of security controls for IoT and physical devices.

The Solution

BTI established a compliance-aligned security architecture across all locations that could be applied to existing sites and future openings alike. The solution centered on Axis Communications AI-enabled cameras, Software House enterprise access control, Cisco Meraki managed networking, and GlobalView 24/7 monitoring. BTI also implemented centralized credential management, medical IoT segmentation, and compliance reporting to create a repeatable operating model.

BTI designed a phased modernization strategy that preserved operational continuity while prioritizing the highest-risk compliance and security gaps first.

Strategic Outcomes

Unified Governance

Security governance standardized across ASC and imaging locations

Audit Readiness

Compliance documentation aligned to HIPAA and accreditation expectations

Operational Continuity

Redundant network architecture supported reliable day-to-day operations

Lifecycle Visibility

Proactive maintenance and firmware governance became manageable

Key Outcomes

12
Locations standardized

100%
HIPAA audit trail coverage

0
Joint Commission findings at next survey

30 days
New location deployment standard

> BTI didn't just improve cameras and badge readers. They established a technology governance framework that can scale as the organization grows.

THE BTI DIFFERENCE

Why BTI Communications Group

Healthcare security and infrastructure is not a product category. It is an operational discipline - and it requires a partner who understands the clinical, regulatory, and technical environment in which these systems must perform. BTI solutions are designed around each healthcare organization's operational structure, internal resources, compliance requirements, and preferred governance model.

> "Some organizations leverage fully managed services, while others operate in a co-managed model alongside internal IT, facilities, compliance, or security teams. All services are scoped with transparent line-item pricing and configurable support structures."

One assessment. One architecture. One deployment team. One managed services contract. One point of accountability - across physical security, cybersecurity, IT infrastructure, VoIP, and compliance.

Assessment-First

Every engagement begins with a documented environment assessment, not a product recommendation.

Healthcare-Specific

Deployments are designed around clinical workflows, regulatory requirements, and operational realities.

PMO-Driven

Projects are managed with formal milestones, documentation standards, and executive-level reporting.

Lifecycle Partnership

BTI supports systems from initial procurement through ongoing optimization and compliance governance, as needed and based on the organization's preferred engagement model.

Request a Strategic Healthcare Security Assessment

Healthcare Security & Compliance Hub

Visit btigroup.com/healthcare for resources, case studies, and compliance guides.

Request a Strategic Assessment

Contact BTI to schedule a vendor-neutral evaluation of your current security posture and infrastructure readiness.

---

btigroup.com · 800-435-7284 · info@btigroup.com

FAQ SECTION

Frequently Asked Questions: Healthcare Security Infrastructure

Authoritative answers to the questions healthcare security and IT leaders ask most.

01 **What security systems do healthcare organizations need?**

Healthcare organizations require a converged infrastructure integrating physical access control, IP video surveillance, cybersecurity, managed IT, VoIP, and HIPAA-aligned compliance governance. Single-point solutions create dangerous gaps. The most resilient environments treat physical and cyber systems as a unified operational framework - not a collection of independent vendor relationships.

02 **What are HIPAA requirements for physical access control?**

HIPAA's Physical Safeguards standard (45 CFR §164.310) requires covered entities to control and validate facility access based on role or function. This includes documented procedures for granting access to areas containing ePHI, workstation security controls, and device and media controls. Access control systems must generate audit logs that can be produced during OCR investigations, Joint Commission surveys, and cyber insurance reviews.

03 **Are IP security cameras a cybersecurity risk?**

Yes. Every IP camera is a network endpoint with firmware, credentials, and a network address. Cameras running outdated firmware, connected to flat networks, or using default credentials are active attack vectors. The 2021 Verkada breach exposed live feeds from 150,000 cameras - including healthcare facilities. Healthcare organizations must apply the same cybersecurity governance to cameras that they apply to any other managed network device.

04 **What is converged security infrastructure?**

Converged security infrastructure is the deliberate integration of physical security, cybersecurity, IT infrastructure, communications, and compliance governance into a unified operational framework. Rather than managing these as separate vendor relationships, converged infrastructure treats them as interdependent systems requiring coordinated design, deployment, and lifecycle management under a single governance structure.

05 **How do healthcare organizations secure multi-site operations?**

Multi-site security requires cloud-managed physical security platforms accessible from a central console, SD-WAN with automatic failover, VLAN-segmented network architecture, centralized SIEM monitoring aggregating events from all locations, and standardized credential governance enabling centralized provisioning and deprovisioning. A standardized deployment framework ensures each new location opens with a consistent, compliant security posture.

06 **Why is network segmentation critical for healthcare security?**

Network segmentation - isolating clinical systems, security devices, medical IoT, and guest traffic into separate VLANs - is the most effective architectural control for limiting ransomware lateral movement. A flat network allows a single compromised endpoint to reach every system, including EHR servers. Proper segmentation contains breaches to the affected segment and provides the network architecture documentation required for HIPAA compliance and cyber insurance underwriting.

CERTIFIED PARTNER ECOSYSTEM

Technology Ecosystem & Manufacturer Partnerships

BTI designs and deploys converged healthcare security infrastructure using enterprise-grade technology from the industry's most trusted manufacturers. Our vendor-neutral assessment process ensures the right technology is selected for each environment - not the technology we happen to carry.

Video Surveillance & Monitoring Platforms

Axis Communications
Enterprise IP cameras, video analytics, and AI-enabled surveillance for healthcare environments

Avigilon (Motorola Solutions)
AI-powered video surveillance with advanced analytics and access control integration

Milestone Systems
Open-platform VMS for multi-site healthcare deployments and third-party integrations

ExacqVision
Flexible VMS with deep integration capabilities and hybrid cloud support

YourSix
Cloud-native video surveillance and AI analytics purpose-built for distributed healthcare environments

Arcules
Cloud video management platform with unified surveillance and analytics across multiple sites

Alarm.com
Cloud-based video monitoring, smart access, and remote management for healthcare facilities

Access Control & Identity Management

Brivo
Cloud-based access control for distributed healthcare organizations with mobile credentialing

Software House (C•CURE)
Enterprise access control and security management for complex healthcare environments

Kantech
Scalable access control solutions with deep integration capabilities for healthcare facilities

RS2 Technologies
Enterprise access control with cloud and on-premise deployment options for healthcare

HID Global (Converged Credentials)
Industry-leading credential technology including smart cards, mobile IDs, and converged physical-logical access for healthcare environments

Network, Cybersecurity & Infrastructure

Microsoft (Tier 1 Partner)
Azure cloud infrastructure, Microsoft 365 security, Defender for Endpoint, and enterprise identity management

Cisco Meraki
Cloud-managed switching, wireless, and SD-WAN for healthcare network infrastructure

Cloudflare
Zero-trust network access, DNS security, and DDoS protection for healthcare environments

CrowdStrike
AI-native endpoint detection and response with real-time threat intelligence

SentinelOne
Autonomous endpoint protection and extended detection and response (XDR)

ConnectWise Asio
Unified IT management and security operations platform for managed service environments

Proofpoint
Email security, threat intelligence, and compliance archiving for healthcare organizations

Galactic Advisors
Healthcare-focused cybersecurity advisory, risk assessment, and compliance guidance

Cradlepoint
LTE/5G failover and backup connectivity for healthcare network resilience

APC by Schneider Electric
Managed UPS and power resilience for critical healthcare infrastructure

BTI maintains certified partnerships with leading manufacturers across physical security, networking, and cybersecurity. All technology recommendations are made following a vendor-neutral assessment of your specific environment, compliance requirements, and operational objectives.

Build a More Secure, Compliant, and Operationally Resilient Healthcare Environment.

One converged partner for healthcare IT, cybersecurity, physical security, VoIP, and compliance.

Request a Healthcare Security & Compliance Readiness Review

Our team will conduct a vendor-neutral evaluation of your current security posture, compliance gaps, and infrastructure readiness - and deliver a prioritized roadmap for improvement.

Executive Advisory

BTI provides board-level guidance across healthcare IT, cybersecurity, physical security, VoIP, and compliance. Our recommendations are shaped by an independent assessment of your environment, regulatory obligations, and operational priorities.

Healthcare Security & Infrastructure Advisory

---

btigroup.com · 800-435-7284 · info@btigroup.com

PUBLICATION INFORMATION

This guide is provided for informational and advisory purposes only. It does not constitute legal, regulatory, or compliance advice. Organizations should consult qualified legal and compliance counsel regarding their specific obligations under HIPAA and applicable regulations.

Healthcare Advisory Series · 2026 Edition

Publication Date: May 2026

Document Version: 1.0

BTI Communications Group

Healthcare Security & Infrastructure Advisory

btigroup.com · **800-435-7284** · **info@btigroup.com**

This document is intended for healthcare executives, IT and security leadership, compliance officers, and facilities directors. Distribution is permitted for internal organizational use and professional advisory purposes.

All content is current as of publication date. BTI Communications Group reserves the right to update this guide as the regulatory and threat environment evolves.