



BUYER'S GUIDE FOR HOSPITALS, CLINICS, ASCS AND MULTI-SITE MEDICAL GROUPS

Healthcare Security Systems Guide

Plan converged video surveillance, access control, duress alerting and the network beneath them, with current regulations and dated, sourced facts.

Written for healthcare CIOs, facilities and security directors, compliance leaders and COOs. It answers the questions buyers ask first: what to protect, which systems to use, what regulators and surveyors expect, and how to roll out across many sites.

INSIDE THIS GUIDE

- 2026-2027 regulatory picture: HIPAA, Joint Commission, Cal/OSHA
- Area-by-area access-control and camera plan for clinical spaces
- Panic buttons vs. wearable duress badges: how to choose
- Cyber-physical controls for cameras, door controllers and medical IoT
- Maturity scorecard, FAQ and a 90-day action plan

Talk to a BTI business advisor

Get a converged security and compliance readiness review for your hospitals, clinics and outpatient sites.

National
800-435-7284
info@btigroup.com

LOS ANGELES 323-510-8002 **CHICAGOLAND** 312-432-5300 **PHOENIX** 602-733-6807

www.btigroup.com/contact • www.btigroup.com/business-security-systems/healthcare/

Serving businesses since 1985 • Integrated security since the 2010s • ISO 27001 compliant • GSA, CMAS & TESMA contracts • ACO licensed in CA, AZ & IL

At a glance

SHORT ANSWER

A modern **healthcare security system** combines access control, video surveillance, duress and panic alerting, visitor management and intrusion detection on a segmented, monitored network, managed under one set of policies. The goals are to protect staff and patients, control who enters clinical and medication areas, produce evidence for surveyors, insurers and HIPAA reviews, and keep cameras and door controllers from becoming cyber entry points.

70%

Share of private-industry workplace-assault injuries with days away from work that occur in health care and social assistance

NCCI analysis of BLS data, 2023-24 (Apr 2026)
[1]

\$7.42M

Average cost of a healthcare data breach, highest of any industry for the 14th straight year

IBM Cost of a Data Breach 2025[2]

July 2027

Projected final action on the proposed HIPAA Security Rule update; current rule enforceable

reginfo.gov, RIN 0945-AA22[3]

What changed since the 2026 edition

- Breach-cost figures corrected and dated: IBM reports \$10.93M (2023), \$9.77M (2024) and \$7.42M (2025) for healthcare.[2]
- Regulatory status updated: HIPAA Security Rule proposal delayed to July 2027; Cal/OSHA general-industry workplace-violence rule still not adopted, while Labor Code §6401.9 (SB 553) has been enforceable since July 1, 2024. [3][4]
- New sections on duress alerting, cyber-hardening of physical-security devices (including AXIS OS 13) and Axis cameras managed in the Cisco Meraki dashboard.[5][6]

Contents

The 2026-2027 risk and regulatory picture	3
What a converged healthcare security architecture looks like	4
Access control for clinical areas	5
Video surveillance and AI analytics	6
Duress, panic buttons and workplace-violence prevention	7
Cyber-physical risk: securing cameras and door controllers	8
Multi-site operations and business continuity	9
Maturity scorecard	10
How BTI helps	11
Frequently asked questions	12
Sources and change log	13

The 2026-2027 risk and regulatory picture

Driver	Status (as of Oct 2026)	What it means for security systems
HIPAA Security Rule (45 CFR Part 164, Subpart C)	Current rule enforceable. The Jan 2025 proposed update is projected for final action in July 2027.[3]	Physical safeguards (§164.310) require facility access controls, workstation security and device and media controls. Keep access logs and video retention policies documented.
Joint Commission workplace-violence standards	In effect since Jan 1, 2022 for accredited hospitals: a designated leader, incident reporting and trend analysis (LD.03.01.01), and an annual worksite analysis (EC.02.01.01).[7]	Use access-control, video and duress data in the annual worksite analysis and corrective actions.
California: Cal/OSHA §3342 (health care) and Labor Code §6401.9 (SB 553)	§3342 covers hospitals and many health-care settings; SB 553 requires written plans, incident logs and training for most other California employers since July 1, 2024.[4]	Lockdown, visitor control, alerting and incident logs support both. The general-industry Title 8 standard was still in rulemaking in Oct 2026.[4]
Breach landscape	804 healthcare breaches of 500+ records were reported to HHS for 2025.[8]	Cameras, door controllers and building systems are network devices and belong in the HIPAA risk analysis.
Workplace violence	Health care and social assistance accounts for about 70% of private-industry workplace-assault days-away cases, at 11.9 per 10,000 FTE vs. 2.6 overall (BLS 2023-24, NCCI analysis).[1]	Prioritize emergency departments, behavioral health, front desks and parking structures.

What a converged healthcare security architecture looks like

Identity & access Card, mobile and PIN credentials; role-based door schedules; integration with HR and directory for automatic offboarding.	Video IP cameras with analytics, VMS or cloud video, retention policy, privacy masking where required.	Alerting Fixed panic buttons, wearable duress badges, lockdown triggers, mass notification and paging.	Network Segmented VLANs for security devices, PoE switching, SD-WAN between sites, monitored firewalls.	Operations Central monitoring, health alerts for cameras and doors, audit reports, quarterly access reviews.
---	--	--	---	--

Why converge? When access control, video and alerting share one platform or are integrated, a forced door or duress alert automatically pulls up the nearest cameras, logs the event and notifies the right responders. Separate, unintegrated systems leave staff switching between screens during an incident and produce weaker evidence afterward.

Platforms BTI designs, installs and supports

Category	Platforms (examples)
Video surveillance	Avigilon Unity and Avigilon Alta (Motorola Solutions), Axis Communications cameras, Milestone XProtect, IQSIGHT (formerly Bosch Video Systems), Cisco Meraki MV, YourSix cloud video
Access control	Software House C•CURE 9000, Kantech EntraPass, Avigilon Alta and Unity Access, Brivo, RS2, HID credentials and readers
Network foundation	Cisco Meraki switching, Wi-Fi and MX SD-WAN; Axis devices managed in the Meraki dashboard

BTI is a Bosch dealer for video products only (now IQSIGHT).

Talk to a BTI business advisor about your healthcare security plan

A BTI business advisor will review your sites, current systems and requirements, then outline options, timelines and budget ranges. No obligation.

[Contact a BTI business advisor](#)
[Healthcare security systems](#)

Call **800-435-7284** (national) · Los Angeles **323-510-8002** · Chicagoland **312-432-5300** · Phoenix **602-733-6807** · info@btigroup.com

Access control for clinical areas

SHORT ANSWER

Start with a **door-by-door zoning plan**: public entrances, clinical units, medication rooms and pharmacies, behavioral health, labs, records and IT closets, and staff-only corridors. Each zone gets a lock type, credential method, schedule, alarm response and camera coverage.

Area	Recommended controls	Notes
Main entrances and ED	Scheduled unlock, after-hours card access, visitor check-in, intercom with video, lockdown capability	Integrate with duress and lockdown buttons at triage and reception
Medication rooms and pharmacy	Card plus PIN or biometric, door-held alarms, camera on entry	Supports DEA controlled-substance security expectations; keep access reports
Behavioral health units	Secure vestibules, controlled egress per fire and life-safety codes, staff duress	Design with the authority having jurisdiction (AHJ)
Labs, records, IT and telecom rooms	Card access, audit logs, cameras	Map to HIPAA facility access controls (§164.310(a))[9]
Maternity and pediatrics	Controlled access, visitor badging, camera coverage of exits	Infant-protection systems are specialty systems; plan integration points with the vendor
Parking structures and exterior	Lighting, cameras with analytics, emergency call stations	Common workplace-violence location

Credentials in 2027: move readers to **OSDP Secure Channel** (encrypted reader-to-controller communication) rather than legacy Wiegand, and consider mobile credentials for staff who float between sites. Tie provisioning to HR so departing staff lose access the same day.

Video surveillance and AI analytics

- **Coverage priorities:** entrances and exits, ED and waiting rooms, pharmacy and medication rooms, elevators and stairwells, parking, loading docks and server rooms.
- **Privacy:** avoid capturing exam and treatment areas unless clinically justified and documented; use privacy masking; restrict who can view and export video, and log exports.
- **Retention:** define retention by area (for example 30 days general, longer for pharmacy and ED) in a written policy that legal and compliance approve.
- **Analytics:** current platforms offer natural-language search and alerts. For example, in Jan 2026 Motorola Solutions announced on-premises Avigilon Visual Alerts, which lets teams create custom detections in plain language; its hospital examples include spotting patient falls and watching restricted zones.[10] Treat AI alerts as decision support: a person reviews before acting.
- **Cloud and hybrid:** cloud VMS (Avigilon Alta, YourSix, Meraki MV) simplifies multi-site viewing; on-premises VMS (Avigilon Unity, Milestone) suits large campuses. Axis cameras can now also be managed in the Cisco Meraki dashboard (Essentials since Apr 14, 2026; Advantage since Jun 23, 2026).[5]

Duress, panic buttons and workplace-violence prevention

SHORT ANSWER

Panic button vs. duress badge: a fixed panic button is best where staff work at a known spot (reception, triage, pharmacy counter). A wearable duress badge follows the employee and can report location, which suits clinical staff, behavioral-health staff and security officers who move between rooms. Most hospitals need both, tied to the same response workflow and camera call-up.

Factor	Fixed panic button	Wearable duress badge
Best for	Fixed workstations: front desk, triage, pharmacy, cashier	Mobile staff: clinical units, ED, behavioral health, home-visit staff on campus
Location reporting	Known by device location	Depends on the locating infrastructure (for example BLE or Wi-Fi based)
Infrastructure	Wired or wireless input to the alarm or access-control panel	Badges, locating receivers or APs, software, charging and assignment process
Discreet activation	Under-desk or wall mount	Pull cord or button on the badge
Integration	Camera call-up, door lockdown, notification	Same, plus responder location display
Operational load	Low; test on a schedule	Higher; badge assignment, charging, battery and testing

Program elements regulators and surveyors look for: a written plan, hazard and worksite analysis, incident logs and trend review, training, and post-incident follow-up (Joint Commission LD.03.01.01 and EC.02.01.01; Cal/OSHA §3342 in California hospitals).[4][7] Security systems supply much of the evidence: alarm logs, access reports, video clips and drill records.

Ready to scope your healthcare security plan?

A BTI business advisor will review your sites, current systems and requirements, then outline options, timelines and budget ranges. No obligation.

[Contact a BTI business advisor](#)

[Healthcare security systems](#)

Call **800-435-7284** (national) · Los Angeles **323-510-8002** · Chicagoland **312-432-5300** · Phoenix **602-733-6807** · info@btigroup.com

Cyber-physical risk: securing cameras and door controllers

Cameras, NVRs, door controllers, intercoms and building systems are network endpoints. Include them in the HIPAA risk analysis and manage them like IT assets.

- ☐ Put security devices on dedicated VLANs; allow only the VMS and access-control servers to reach them.
- ☐ Remove default passwords; use unique credentials stored in a password vault; enforce MFA on VMS and access-control admin portals.
- ☐ Keep a firmware calendar. Example: **AXIS OS 13** (first release scheduled Sept 2026) enforces HTTPS by default, stricter passwords, signed video and signed ACAP apps; test integrations before upgrading.[6]
- ☐ Retire unsupported recorders and operating systems; track end-of-support dates.
- ☐ Forward security-device logs to your SIEM or monitoring service; alert on camera offline and door-forced events.
- ☐ Review vendor remote-access paths; replace always-on remote tools with controlled VPN access.
- ☐ Check camera procurement against the NDAA Section 889 restrictions if you receive federal funding.

Network foundation

Security systems depend on PoE switching, Wi-Fi coverage for mobile devices and reliable links between sites. BTI's companion guide, *Meraki MX SD-WAN for Healthcare*, covers WAN resilience and segmentation. Cisco Wi-Fi 7 access points (CW917x) include BLE radios that can support locating use cases.[11]

Multi-site operations and business continuity

- **Standardize** a site template: door hardware, reader type, camera models, VLAN plan, naming, retention and alarm-response procedures.
- **Centralize** visibility: one access-control database (or federated system) and one video platform view across sites; health monitoring for every camera and controller.
- **Plan for failure:** UPS on head-end and network gear, controller-level decision making if the server is offline, cellular or dual-path alarm communicators as copper (POTS) lines are retired, and documented manual procedures.
- **Test:** lockdown drills, duress-alert tests and failover tests on a schedule, with records kept for surveyors and insurers.

Maturity scorecard

Domain	Reactive	Managed	Mature
Access control	Keys and local systems	Card access at key doors	All sites on central platform, HR-linked offboarding, quarterly reviews
Video	Standalone DVRs	IP cameras, local VMS	Central VMS or cloud, health monitoring, written retention, logged exports
Duress and alerting	None or ad hoc	Fixed buttons at reception	Buttons plus badges in high-risk units, integrated with video and lockdown
Device security	Default passwords	Some VLANs	Segmented, MFA, firmware calendar, SIEM logging
Evidence	Manual	Periodic reports	Scheduled reports mapped to Joint Commission, HIPAA and insurer questions

90-day action plan

1. **Days 1-30:** inventory doors, cameras, alarm and duress devices, recorders and firmware; collect last year's incident logs.
2. **Days 31-60:** risk-rank areas (ED, behavioral health, pharmacy, parking); close quick wins (passwords, VLANs, failed cameras).
3. **Days 61-90:** approve a multi-year roadmap and budget; schedule drills; set reporting for surveyors and insurers.

How BTI helps

BTI plans, installs, integrates and supports healthcare security systems and the networks under them. BTI's security and IT teams work from the same project plan, so camera VLANs, door-controller firewall rules and help-desk support are designed together. Services include site surveys, design, installation, integration, monitoring options and ongoing service through [GlobalView support services](#).

Related BTI pages: [Healthcare security systems](#) · [Healthcare technology](#) · [Hospital access control](#) · [Video surveillance in hospitals](#) · [Biometrics in healthcare](#) · [Business continuity in healthcare](#) · [Converged security](#)

About BTI Communications Group

BTI Communications Group (BTI Group) has served businesses since 1985 (40 years) and has delivered integrated security systems since the 2010s, alongside managed IT, cybersecurity services, networking and business communications. BTI focuses on high-security, regulated and multi-site organizations in healthcare, financial services, logistics, manufacturing, education and the public sector.

Credential	Detail
Security management	ISO 27001 compliant information security practices
Public-sector contracts	GSA, CMAS and TESMA contract vehicles
Licensing	Alarm Company Operator (ACO) licenses in California, Arizona and Illinois
Offices	Los Angeles 323-510-8002 · Chicagoland 312-432-5300 · Phoenix 602-733-6807 · National 800-435-7284

Frequently asked questions

What security systems does a hospital need?

At minimum: electronic access control with audit logs, IP video surveillance with a written retention policy, panic or duress alerting tied to response procedures, visitor management, intrusion detection for after-hours areas, and a segmented network for these devices.

Panic button or duress badge: which is better for hospital staff safety?

Use fixed panic buttons at known workstations and wearable duress badges for staff who move between rooms or work in high-risk units. Integrate both with camera call-up and a single response workflow.

Do cameras and access control fall under HIPAA?

They can. Video may capture protected health information, and access-control logs support HIPAA physical safeguards (§164.310). Include security devices in your risk analysis.[9]

Is the new HIPAA Security Rule final?

No. As of Oct 2026 HHS lists final action for July 2027. The current rule remains enforceable.[3]

What does Cal/OSHA require for workplace violence?

California hospitals and many health-care settings fall under Title 8 §3342. Most other employers must follow Labor Code §6401.9 (SB 553), in force since July 1, 2024.[4]

Cloud or on-premises video for a health system?

Cloud suits many distributed clinics; on-premises or hybrid suits large campuses with many cameras. Many systems run hybrid.

How long should hospitals keep video?

There is no single federal number. Set retention by area in a written policy approved by legal and compliance, and make sure storage is sized for it.

Can BTI support sites in several states?

Yes. BTI has offices in Los Angeles, Chicagoland and Phoenix, holds ACO licenses in California, Arizona and Illinois, and supports multi-state programs.

Next step: a healthcare security plan conversation with BTI

A BTI business advisor will review your sites, current systems and requirements, then outline options, timelines and budget ranges. No obligation.

[Contact a BTI business advisor](#)[Healthcare security systems](#)

Call **800-435-7284** (national) · Los Angeles **323-510-8002** · Chicagoland **312-432-5300** · Phoenix **602-733-6807** · info@btigroup.com

Sources and change log

1. NCCI, "Workplace Violence: Part 1, Assault Trends, Drivers, and Demographics," April 2026 (analysis of BLS SOII 2023-24). <https://www.ncci.com/Articles/Documents/Workplace-Violence-Part1-Assault-Trends-Drivers-Demographics.pdf>
2. IBM, Cost of a Data Breach Report 2025; IBM Newsroom, July 30, 2025. <https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls>
3. Unified Agenda, RIN 0945-AA22, HIPAA Security Rule NPRM (01/06/2025) with final action 07/2027. <https://www.reginfo.gov/public/do/eAgendaViewRule?RIN=0945-AA22&pubId=202510>
4. California DIR / Cal/OSHA, "Workplace Violence Prevention in General Industry" (Labor Code §6401.9; §3342 for health care), accessed Oct 11, 2026. <https://www.dir.ca.gov/dosh/Workplace-Violence/General-Industry.html>
5. Cisco Meraki Documentation, "Axis Device Onboarding with Meraki Dashboard," accessed Oct 11, 2026. https://documentation.meraki.com/IoT/MV_-_Smart_Cameras/Install_and_Get_Started/Installation_Guides/Axis_Device_Onboarding_with_Meraki_Dashboard
6. Axis Communications, "AXIS OS 13 breaking changes," Nov 27, 2025. <https://www.axis.com/en-us/for-developers/news/AXIS-OS-13-breaking-changes>
7. The Joint Commission, Workplace Violence Prevention Program resources (requirements effective Jan 1, 2022). <https://www.jointcommission.org/en-us/knowledge-library/workforce-safety-and-well-being-resource-center/workplace-violence-prevention/workplace-violence-prevention-program>
8. HIPAA Journal, "Healthcare Data Breach Statistics" (OCR portal data), accessed Oct 11, 2026. <https://www.hipaajournal.com/healthcare-data-breach-statistics/>
9. eCFR, 45 CFR Part 164 Subpart C (§164.310 physical safeguards). <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C>
10. Motorola Solutions press release, Jan 12, 2026, "Motorola Solutions expands AI-powered security platform." <https://www.motorolasolutions.com/newsroom/press-releases/motorola-solutions-expands-ai-powered-security-platform.html>
11. Cisco Meraki Documentation, CW9178I Datasheet (BLE radio), accessed Oct 11, 2026. https://documentation.meraki.com/Wireless/Product_Information/Overviews_and_Datasheets/CW9178I_Datasheet

Not legal advice. Requirements vary by state, accreditation and facility type; confirm with counsel and your AHJ.

Change log. 2027 edition proof v1 (Oct 11, 2026): full rewrite, condensed from 34 to 13 pages. Corrected breach-cost statistics; added dated regulatory table, duress comparison, cyber-physical checklist and FAQ. Removed unsourced percentages ("94% ransomware increase", "60% fewer incidents"), anonymous case-study outcomes and the list of cybersecurity technology partners.