The State of Healthcare Access Control 2026

Risks, Regulations and the Move to Mobile

EBOOK

Security Moves Front and Center in Healthcare

Healthcare environments operate in constant motion — with authorized personnel, visitors, patients and service providers always moving through facilities. This makes them vulnerable to workplace violence, data compromise and cybersecurity breaches. Recognizing this, legislators across the globe are introducing new accountability measures.

The call for **formal standards** to prevent workplace violence has moved from advocacy to action. For example, proposed **Occupational Safety and Health Administration** (OSHA) mandates in the US and developing frameworks in the UK and Canada require healthcare institutions to adopt more proactive, integrated and auditable approaches to securing people, places and data.

These emerging standards are an opportunity to embed security systems that empower rather than obstruct. A flexible, integrated ecosystem of access solutions — from mobile-ready credentials and smart readers to centralized identity management — allows healthcare organizations to meet regulatory requirements and build a more resilient, efficient and secure environment.

Healthcare Facility Pressures

The security pressure on healthcare environments — open campuses with high foot traffic and 24-hour operations — is increasing while security infrastructure is ageing. At the same time, physical security is becoming a mandatory, auditable component of healthcare operations.

In the US, healthcare organizations face rising physical threats and increasing **mandates** for digital and physical safeguards. This year, European healthcare facilities too face robust physical security requirements for physical access control under the **Critical Entities Resilience (CER) Directive**.

Up to
38% of healthcare professionals
experience physical violence

21% increase in healthcare cyber incidents

45% US healthcare workers
consider leaving their jobs due to safety concerns

These realities point to the need for integrated, audit-ready access systems that protect people, data and reputations. And it's why:

68% say identity and access management
is an investment priority for 2026

HID

Regulatory Momentum

The regulatory landscape for healthcare and life sciences is being shaped by new mandates that go beyond simple policy checklists. Compliance now requires demonstrable, real-time control over physical environments.

HIPAA

Requires facility access controls to limit ePHI exposure. Access must be role-based and strictly audited.

FDA under GxP (Good x Practice) GMP (Good Manufacturing Practice)

Mandates data integrity via ALCOA+ (Attributable, Legible, Contemporaneous, Original, Accurate plus Complete, Consistent, Enduring, Available), where physical access logs are critical for proving lab data is attributable to a specific individual.

The Joint Commission

Demands documented control of sensitive areas, like pharmacies and behavioural health units, to ensure patient and staff safety.

Modern access control makes meeting these obligations simpler; centralizing identity management creates a clear, auditable record of every access event. It proves to regulators that accountability is built into daily operations and demonstrates integrity across hospitals, labs and pharma facilities.

HID

What Does Modern Access Control Look Like?

How do you move from fragmented physical access control to a more unified identity and access ecosystem? Rather than forcing a costly and disruptive ‘rip-and-replace’, many organizations take a modular approach that allows them to modernize at their own pace.

1. Starting with the infrastructure

For some, the logical entry point is at the door. Upgrading to modern, mobile-ready readers like HID Signo, lays the groundwork for future capabilities. These readers support advanced encryption and are designed to work with existing credentials during a transition period.

2. Evolving the credential over time

With a modern reader infrastructure in place or running in parallel, organizations can begin transitioning credentials when the time is right. Migrating from legacy proximity cards to more secure options like Seos (HIDs credential technology) helps eliminate common attack vectors such as card cloning and sniffing.

When ready, introducing mobile credentials offers the ability to use smartphones and wearables as IDs, reducing credential fatigue and enabling new efficiencies like tap-and-go workstation logins.

3. Layering in integration and intelligence

As infrastructure and credentials mature, previously siloed systems can be connected. Integrated platforms bring together access logs, visitor data, HR records and even real-time location tracking into a unified view. This reduces manual administration and enables faster, more coordinated responses when incidents occur.

For compliance officers, integration means automated audit trails and confident regulatory policy enforcement.

The Move to Mobile Credentials

The move to mobile credentials is a natural next step for hospitals, laboratories and pharma campuses, shifting from plastic cards to the smartphones and wearables staff already carry.

Mobile credentials:

- Enable fast, secure access to required spaces
- Reduce administrative burden with instant over-the-air issuance and revocation
- Remove physical card handling, reduce helpdesk calls and automate access policy enforcement
- Provide a software-based identity layer that integrates with AI-driven analytics, increasing threat detection
- Strengthen security with on-device biometrics for MFA
- Reduce the friction of juggling multiple badges and passwords

Solving BYOD's Security and Privacy Weaknesses

Bring Your Own Device policies introduce privacy and security concerns, particularly in unionized environments with protections against employer monitoring. Lost and compromised devices could expose healthcare organizations to unauthorized individuals. HID addresses these concerns by keeping the facility and the employee's personal phone operationally separate.

- The HID Mobile Access app only detects nearby readers to unlock doors and does not store or transmit location information.
- When the app is uninstalled, all personal data is deleted within 30 days.
- Credentials are stored in a trusted execution environment on the phone — hardware-level isolation that prevents other apps and malware from cloning or intercepting it.
- If a device is lost or stolen, administrators can instantly revoke credentials over-the-air, remotely wiping access.

Building a More Secure, Connected Foundation — One Layer at a Time

As 2026 unfolds, healthcare's shift to connected, data-driven operations includes physical access control. Across hospitals, labs and pharma manufacturing, the goal is to move beyond discrete doors and badges towards unified identity.

This means exploring how a single credential (often mobile) can streamline access for overstretched staff: opening patient wings, logging into workstations, unlocking medication cabinets and adjusting permissions as roles change.

The work ahead involves layering modern capabilities over existing infrastructure while keeping compliance front and center, with automated reporting part of the ask.

The need for partners who understand healthcare's complexity is clear. HID continues to work alongside healthcare organizations, offering expertise and modular solutions to help them modernize at their own pace.

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800
Latin America: +52 (55) 9171-1108

For more global phone numbers click here

Part of ASSA ABLOY

hidglobal.com