Access Control in Healthcare: Rethinking Security in Open, Caring Environments

Introduction

Hospitals and healthcare environments occupy a unique position in our communities. They are places of healing, compassion and continuous care, where openness and a welcoming environment is both a necessity and a virtue.

Yet, these same characteristics present specific challenges when it comes to ensuring safety, managing access and maintaining operational resilience. It involves more than selecting the right products and services – it also requires best practice and an integrated approach to ensure security, safety and convenience for staff, patients and visitors.

As healthcare systems evolve in complexity and as demands on staff and infrastructure increase, the question of how to secure these spaces – without compromising their openness - grows more urgent. Traditional approaches to access control, often designed with corporate, industrial or educational environments in mind, are frequently unfit for the layered and high-pressure world of healthcare.

This white paper explores the evolving access control landscape within the healthcare sector, offering insight into how integrated, flexible systems can support the mission of care while enhancing safety and efficiency.

Drawing on sector trends, real-world examples and a growing body of best practices, it aims to support healthcare professionals, estates teams, security personnel, and decision-makers in navigating this critical area of modern hospital operations.

The Unique Nature of Healthcare Environments

Unlike most public buildings, hospitals never close. They operate 24/7, with critical care and emergency departments functioning continuously. Staff operate in rotating shifts; consultants, surgeons, porters, cleaners and specialist teams work around the clock.

Patients are admitted, discharged, transferred and monitored at all hours. They are placed under medical care to enhance well-being and recovery. And visitors are actively welcomed to attend to aid recovery.

This makes static, one-size-fits-all access strategies ineffective. Instead, solutions must support high levels of adaptability and interoperability, responding to the needs of diverse users and the rhythms of medical care.

Access control in healthcare must support multiple modes of care delivery. From outpatient consultations and community clinics to major trauma centres and psychiatric units, every setting has different demands.

A maternity unit may require high levels of protection to prevent infant abduction, while a day-surgery centre may prioritise fast, seamless movement of staff and patients. Increased attention on mental health units may require added safeguards to manage risk and protect vulnerable individuals, yet these protections must be delivered with dignity and discretion.

This diversity requires access management systems that are not only robust but also responsive. They must allow quick reconfiguration without technical complexity, integrating with wider hospital operations while upholding patient dignity and staff autonomy. The fundamental challenge is to maintain the openness and compassion at the heart of healthcare, while ensuring that safety and control are never compromised.

Evolving Risks and Pressures on Security

In recent years, the healthcare sector has seen growing pressures directly impacting on security and access control. One of the most concerning trends has been the increase in aggression and violence towards staff.

With increased waiting lists[1] for hospital treatments, according to numerous health service reports, assaults on nurses, doctors and support staff have risen significantly. These incidents often occur in high-stress areas like emergency departments, where staff must make difficult decisions quickly, sometimes in the face of emotional or confrontational individuals.

[1] NHS Key Statistics: England. Published 30 May 2025: https://commonslibrary.parliament.uk/research-briefings/cbp-7281/

Staffing shortages[2] have compounded the issue. Under-resourced teams face growing workloads, longer shifts, and mounting emotional strain, making them more vulnerable to both verbal and physical aggression. With fewer staff available to monitor access points or challenge unauthorised entry, the risks of security breaches increase.

Public access to hospitals remains largely unrestricted. Visitors, delivery personnel, patients and contractors enter and move through buildings every day. While this openness is essential to the inclusive ethos of healthcare, it can create opportunities for breaches, unauthorised access and loss of critical items such as medications, records, or high-value equipment.

The threat landscape has expanded to include cybersecurity breaches and information governance concerns. Access control systems are increasingly networked, connected to central servers and IT infrastructure. If not properly secured, these systems may present vulnerabilities. Integration with HR systems, shift management, fire safety, and emergency response add further complexity.

In this environment, access control cannot be treated as a static infrastructure issue. It must be a dynamic part of wider safety planning, risk assessment and operational continuity. Integrated systems need to consider emerging risks while supporting the everyday care routines that define hospital life. By example, a CCTV operator triggering the doors to lock or real-time response to a panic button being pressed.

This level of integration not only strengthens incident response but also ensures routine operations can continue safely and efficiently, even under pressure.

Legacy Systems and the Cost of Inflexibility

Many healthcare providers still rely on outdated or fragmented mechanical systems to manage access. These might include traditional locks and keys, standalone card readers, or a patchwork of technologies introduced over years of incremental upgrades.

[2] Post Brexit reliance on NHS staff is unethical: published 21 March 2025: https://www.theguardian.com/society/2025/mar/21/post-brexit-reliance-on-nhs-staff-from-red-list-countries-is-unethical-streeting-says

While these approaches may function at a basic level, they rarely offer the oversight, management flexibility, or integration needed to support a modern hospital estate.

Mechanical keys pose a particular challenge. They are easily lost, duplicated, or shared without authorisation. Tracking their use is difficult and often not communicated, whilst changing access rights often requires physically changing locks, which can be disruptive and expensive.

In some cases, keys are kept in central stores or signed out manually - systems that depend on human compliance and administrative discipline, both of which can be overwhelmed in busy environments.

Standalone electronic systems can offer improvements but still fall short of what is required. If systems are not integrated or centrally managed, estates teams may face a heavy administrative burden. Updating user credentials, responding to lost badges, managing contractors, and controlling temporary access all become time-consuming tasks.

These legacy systems lack real-time visibility. When incidents occur such as a patient wanders from a dementia ward, or an aggressive visitor attempts to re-enter a restricted area, response can be delayed simply because there is no live data on who is where, and when. In emergency situations, the ability to instantly lockdown or open access to specific zones may not exist.

The cost of inflexible systems is paid not just in time and maintenance budgets, but in missed opportunities with stretched resources to enhance safety, streamline operations, and support the wellbeing of patients, staff and visitors.

Building the Case for Integrated Access Control

Integrated access control offers a way forward, combining physical infrastructure with intelligent software and user-friendly management tools. When designed with the specific needs of healthcare environments in mind, these systems can transform how hospitals approach safety, resilience, and operational continuity.

The key advantage lies in visibility. With centralised management, estates and security teams can monitor access activity across entire sites or networks of hospitals. They can issue, revoke, or amend permissions remotely, tailoring access to departments, zones, or even individual doors. When incidents occur, the response is faster and more informed, based on real-time data.

Flexibility is equally important. Modern access systems allow for user profiles to be linked to staff roles, rather than individuals. This supports shift-based access, temporary credentials, and rapid onboarding of new or agency staff. Contractors, delivery drivers and cleaners can be issued limited access rights that expire automatically after a set period.

Integration with other building systems offers additional benefits. Access control can be linked with fire alarm systems to enable safe evacuation, or with CCTV and intruder alarms to create a comprehensive security picture. When combined with staff ID badges or mobile credentials, access can become a seamless part of daily workflows.

Just as importantly, integrated systems can be designed to reduce disruption. Wireless door controllers, modular components and cloud-based platforms enable staged rollouts and minimise interference with clinical operations. A well-planned upgrade need not involve major downtime or invasive installation.

The result is a smarter, more adaptive hospital environment - one where safety is enhanced without sacrificing the openness and trust that define great healthcare.

Lessons from Real Implementations

Blackpool Victoria Hospital, one of the largest and busiest medical centres in the Northwest recognised the need for a scalable and resilient access control system that could adapt to the complex needs of its various departments. The hospital partnered with Comelit-PAC to deliver a complete infrastructure upgrade.

Comelit-PAC deployed PAC Access Central, enabling centralised control across the site via multiple secure PC workstations. This allowed the hospital’s Digital Identity and

Security teams to manage permissions with greater speed and accuracy, enhancing oversight and incident response.

The project incorporated a server-based architecture to provide failsafe redundancy, a crucial feature for a hospital environment where system uptime and security continuity are paramount. By collaborating from the specification stage, Comelit-PAC ensured the installation aligned with the hospital's operational goals while minimising disruption to daily activities.

Says Martyn McKechnie, Head of Digital Identity at Blackpool Victoria Hospital: "As a busy hospital with multiple departments and critical areas, we required an access control system that could integrate seamlessly while offering high levels of security and administrative control. PAC Access Central provides the scalability and reliability we need to manage hospital-wide access efficiently. The ability to oversee all access points from multiple PC workstations ensures our Digital Identity and Security teams can respond quickly to any situation."

This example demonstrates the tangible benefits of integrated access control: streamlined administration, real-time visibility, and a safer, more responsive environment for staff and patients alike.

Designing for People, Not Just Infrastructure

Technology alone is not enough. Access control in healthcare must begin with a deep understanding of people involved and their roles, behaviours and emotional needs. Systems must support rather than hinder staff, patients and visitors. They must be intuitive, non-intrusive, welcoming and adaptable.

For patients, especially those experiencing anxiety, disorientation, or cognitive challenges, visible security measures can be unsettling. Access systems must blend into the environment, offering safety without imposing a sense of restriction. In paediatric wards or mental health facilities, thoughtful design can make a significant difference.

For staff, systems should enable rather than restrict. Doctors and nurses need to move freely and quickly, sometimes under great pressure. Badges must work reliably. Door releases must be responsive. Access should follow the logic of care, not the limitations of technology. Where security clashes with workflow, it is the system that must adapt.

Visitor management is another sensitive area, where families and friends are vital to the healing process. Systems must allow for safe, respectful visitor access while maintaining clear boundaries. Digital check-in, visitor passes and time-limited credentials can offer a balance between welcome and vigilance.

Above all, access control must be seen as part of the therapeutic environment. It should contribute to a sense of order, safety, and calm. In this way, it becomes not just a security tool, but a part of the culture of care.

Looking Ahead – Future Considerations

As technology advances, new possibilities are emerging. Biometric identification, mobile wallet credentials and real-time AI-driven and machine learning analytics all offer potential benefits. Yet these innovations must be approached with caution in healthcare. Privacy, consent, and reliability are paramount.

Sustainability is also a growing concern. Hospitals are under pressure to reduce carbon footprints and improve energy efficiency. Access systems that minimise power use, support smart building integration, or reduce reliance on disposable credentials can contribute to broader environmental goals.

Cybersecurity will remain a central challenge. As access systems become more connected, they must be protected against intrusion, data loss, and manipulation. This requires robust encryption, regular updates, and strong governance.

Finally, the human dimension must never be lost. As new risks emerge - from pandemics to climate events together with cyberattacks - the role of access control will only grow in importance. Its success will depend on technical capability and an ability to support the values of healthcare: compassion, inclusion, and trust.

In summary, access control in healthcare is concerned with enabling care to happen safely, efficiently and with dignity. It is about protecting those who heal, those who are vulnerable and those who come in search of help. It is about building resilient, adaptive environments that support health in every sense.

Hospital managers must invest wisely in their facilities to maintain high security levels for patients and staff alike.

By rethinking security technology through the lens of compassion, collaboration and innovation, healthcare providers can create safer, more responsive hospitals. And this is not just for today, but also for the healthcare challenges of tomorrow.

How Comelit-PAC Supports Healthcare Environments

In healthcare settings, safety, accessibility and efficient operations are essential. Comelit-PAC understands the unique pressures and demands faced by the sector and works closely with healthcare providers to deliver tailored security and access control solutions that support the delivery of high-quality care.

With extensive experience supplying hospitals, GP surgeries, specialist clinics and care homes, Comelit-PAC takes a consultative approach to system design. This ensures each solution is matched to the specific needs of the site, from initial design and specification through the works programme; whether it's enabling smooth access for authorised personnel, protecting sensitive areas, or providing clear and secure communication systems.

Secure Access, Without Compromise

Access control plays a critical role in managing who can enter different areas of a healthcare facility. Comelit-PAC’s networked and standalone systems give site managers the flexibility to manage access permissions in real time. This is particularly valuable in environments where shift patterns change regularly, and different access rights are required depending on roles.

For example, in hospitals where access must be controlled across multiple zones - from general wards and maternity units to restricted areas like pharmacies or data centres - Comelit-PAC’s access control systems offer powerful yet intuitive control. With

centralised management and integration with HR databases, the system ensures compliance with safeguarding protocols while also supporting operational efficiency.
Integrated Systems for Enhanced Safety

Healthcare facilities often rely on a range of safety and communication tools. Comelit-PAC offers the ability to integrate video surveillance, door entry, fire safety systems and access control into a single, cohesive platform. This not only simplifies visitor management but also improves situational awareness across the site.

Video door entry, for example, is particularly useful in clinics, mental health settings and care homes, where controlled access and patient safeguarding are crucial. Staff can verify visitors before granting entry, reducing the risk of unauthorised access and supporting a safe, welcoming environment.

Supporting Dignity and Independence in Care Homes

In residential care environments, maintaining the balance between security and resident independence is key. Comelit-PAC's systems are designed to be non-intrusive yet effective, enabling staff to monitor movement where necessary while allowing residents to enjoy freedom of movement within safe parameters.

Smart access control can also streamline staff operations, allowing care teams to focus more on providing personalised support rather than managing keys or checking visitor credentials.

Reliable, Scalable and Future-Proof

Comelit-PAC's systems are tailored to evolve with the needs of each healthcare facility. Whether supporting a small local surgery or a large hospital multi-site trust, the technology is scalable and easy to maintain~~.~~

With no annual software licence fees and complimentary updates, systems remain current without incurring additional operational costs. Continued access to software enhancements and new product developments helps ensure the technology remains up to date over time, supporting long-term performance and value.

In summary, as the healthcare landscape continues to develop - driven by digital transformation, regulatory updates, and new models of care - Comelit-PAC remains a trusted partner. Our aim is to deliver security technology and fire safety systems that safeguard people, assets, and sensitive data alike; while helping staff, patients and visitors feel secure in their healthcare environment.

For more information, please visit www.pacgdx.com