



**Enhancing
Security and
Efficiency in
Healthcare Facilities
Through Integrated
Access Control**

acresecurity.com

Enhancing Security and Efficiency in Healthcare Facilities Through Integrated Access Control

Executive Summary

The healthcare industry faces unique challenges in balancing security with accessibility. The requirements to protect patient data, ensure the safety of both patients and staff, create a welcoming environment for visitors, and maintain compliance with regulatory standards necessitate a sophisticated approach to access control. This document outlines a comprehensive solution leveraging integrated access control systems to enhance both security and operational efficiency in healthcare facilities.

The integration of access control solutions not only safeguards sensitive areas but also provides valuable data for improving facility operations and patient experiences. With the adoption of these integrated systems, healthcare facilities can not only meet but exceed the evolving standards of safety, privacy, and efficiency required in today's fast-paced medical environments and achieve a secure environment that supports streamlined workflows and fosters a focus on patient care.



Introduction

The rise in violence against healthcare workers is a critical factor driving the adoption of robust and integrated access control systems. According to the Occupational Safety and Health Administration (OSHA), incidents of serious workplace violence were nearly five times more common in healthcare than in private industry on average. A survey conducted by the American College of Emergency Physicians revealed that 85% of emergency physicians reported an increase in physical assaults at work with more than 70% of nurses in emergency departments experiencing physical or verbal assaults by patients and visitors annually. These alarming statistics underscore the urgent need for healthcare facilities to implement effective security measures to protect their staff and patients alike.

Security Challenges in Healthcare Facilities

Healthcare facilities are unique environments with specific security challenges that must be addressed when selecting an access control system. These include:

Protecting sensitive and restricted areas such as drug storage rooms, medical supply closets, and patient records which require limited access to only authorized personnel.

Ensuring the safety of all patients, especially those with limited mobility or cognitive impairments.

Managing visitor access for hundreds of visitors a day while balancing between providing a welcoming environment and maintaining security.

Complying with regulations that govern the privacy and security of personnel and patient health information to avoid penalties or legal consequences.

Integrating with other security systems such as video surveillance, intrusion detection, and emergency response procedures for a comprehensive and streamlined security solution.

With escalating incidents of violence, infant abduction, and cybersecurity threats, access control systems form an essential line of defense in a hospital's security strategy. These systems must be efficient, adaptable, and integrated to ensure the safety of individuals and the security of sensitive information.



Prioritizing Data Protection in Access Control Solutions

In an era when digital threats are increasingly sophisticated, safeguarding personnel records, sensitive patient data, building security details, and other confidential information is imperative. It is crucial that the access control system employs the latest in data security protections to safeguard sensitive data.

A comprehensive security strategy for access control not only protects against unauthorized access but also ensures that patient confidentiality is maintained, reinforcing the trust between healthcare providers and their patients.

A secure network must incorporate the following key features:

End-to-End Encryption:

All data transmitted between the access control devices and the cloud server, including sensitive information such as access codes and personal identification details, must be encrypted to prevent interception and unauthorized access.

Two-Factor Authentication (2FA):

To enhance security levels, two-factor authentication should be mandatory for system administrators and users accessing the control system remotely. This adds an extra layer of security beyond just a password, often combining something the user knows (a password) with something the user has (such as a mobile device).

Regular Software Updates and Patches:

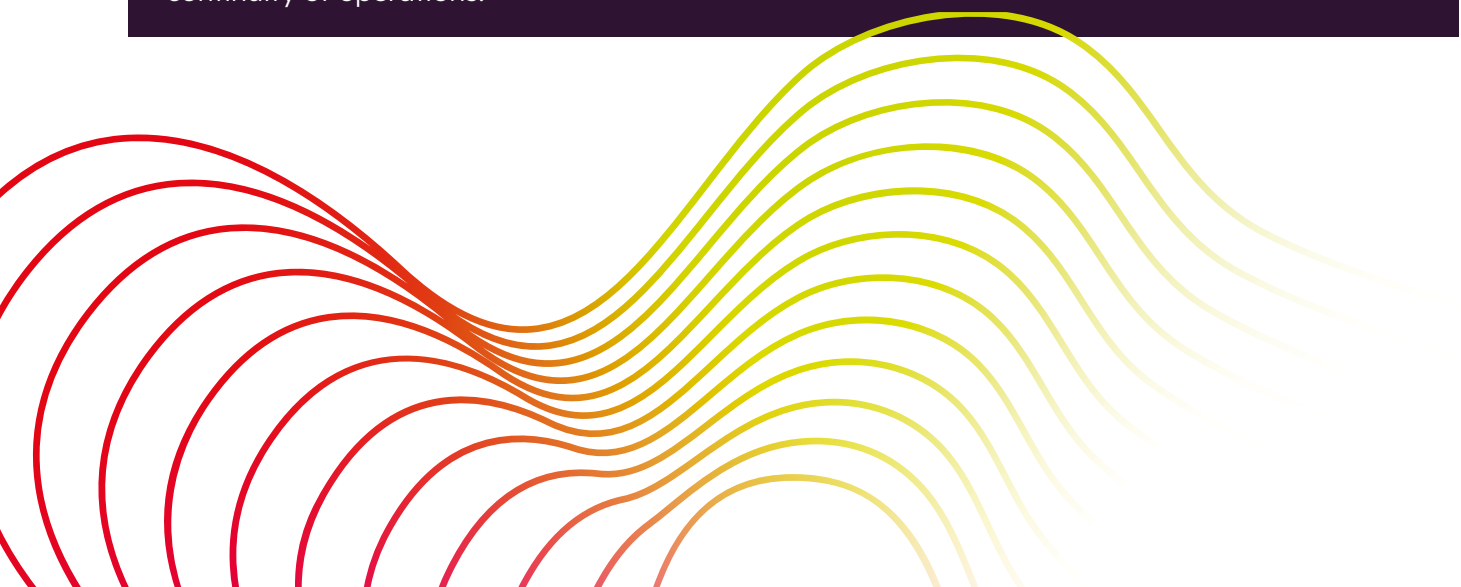
The cloud-based system should automatically receive the latest software updates and security patches to protect against newly discovered vulnerabilities and security threats.

Advanced Threat Detection and Response:

The network should be equipped with tools that continuously monitor for suspicious activities or anomalies, with the capability to respond immediately to potential threats to minimize possible damage.

Redundant Data Backups:

Regular, redundant backups of all system data ensure that, in the event of a cyberattack or system failure, crucial information is not permanently lost and can be restored to maintain continuity of operations.



Compliance with Security Regulations

Ensuring a hospital's access control system aligns with security regulations and best practices for both physical security and cybersecurity is essential. Below are some key security compliance requirements to consider for access control:

1. HIPAA

The HIPAA (Health Insurance Portability and Accountability Act) Privacy Rule applies to all forms of individuals' protected health information, regardless of whether it's electronic, written, or oral.

HIPAA §164.310 "Standard: Facility Access Control" establishes the requirement for healthcare organizations to implement policies and procedures that restrict physical access to facilities and electronic systems containing ePHI (electronic Protected Health Information). This standard aims to safeguard the confidentiality, integrity, and

availability of patient data by controlling access to physical areas and electronic records within healthcare facilities.

This measure involves the use of various mechanisms, such as ID badges, biometric identification, and secure access points, to regulate entry to areas where ePHI is stored or accessed. Furthermore, the standard emphasizes the importance of maintaining an audit trail of physical access to facilities and electronic systems to monitor and track individuals' movements within the premises.

2. Joint Commission Standards

Hospitals seek accreditation by the Joint Commission as a testament to their commitment to maintaining high standards of patient care and safety. This accreditation is not just a mark of prestige but serves as an essential benchmark for operational excellence.

Given the evolving landscape of healthcare security, it's imperative to align hospital access control systems with the stringent regulations set out by the Joint Commission, including:

Environment of Care (EC.02.01.01)

The Environment of Care (EC) standards require that hospitals maintain a safe, secure, and functional environment. Specifically, EC.02.01.01 calls for the management of safety and security risks in the hospital environment. This includes implementing access control measures to restrict unauthorized entry and protect sensitive areas, ensuring that patients, staff, and assets are safeguarded against security breaches.

Controls for Security Sensitive Areas (EC.02.01.01 EP 8)

For critical access hospitals, the standard EC.02.01.01 EP 8 emphasizes the control of access to and from areas identified as security sensitive. Implementing robust controls in these areas is essential for maintaining a secure environment.

Information Management (IM.02.01.03)

This standard mandates that hospitals implement policies and procedures to secure electronic and physical information. Access control systems are a key component of complying with this standard as they prevent unauthorized access to electronic health records and areas where patient information is stored or accessed.

3. Healthcare Cybersecurity Regulations

In addition to regulatory compliance with HIPAA and the Joint Commission standards, ISO 27001 certification plays a critical role in enhancing the security of hospital access control and visitor management systems. ISO 27001 is a widely recognized standard for information security management systems, focusing on the protection of confidential data and the integrity and availability of information.



Streamlining Systems for Optimized Workflow

Integrating access control systems with disparate systems significantly helps improve operational efficiency, resource allocation, and response times during emergencies. It's noteworthy that trends indicate a shift toward cloud-based and IP/POE-based systems due to their scalability and ease of management.

The integration of access control systems with other security technologies such as video surveillance, alarms, and visitor management systems is critical in creating a comprehensive and efficient security ecosystem. This enables seamless communication between various components, providing real-time information to administrators, and improving response times during incidents.

Specifically, the joining of access control with visitor management systems not only secures a

facility but also streamlines check-in processes, minimizes administrative burdens, and creates a more welcoming experience for visitors. By linking visitor management software with access control, hospitals can automate the issuance of temporary access credentials to guests, contractors, and other non-staff members, effectively controlling who enters the premises and when. This synergy not only enhances the security of patients and staff by minimizing potential risks but also improves the visitor experience, making it more convenient and less time-consuming to gain entry. Furthermore, the combined data from both systems provide valuable insights for security audits and compliance reporting, ensuring that the facility remains vigilant and proactive in its security measures.

Extending Access Control Measures Beyond Perimeter Doors

The conversation about hospital security often gravitates towards safeguarding external entry points, yet the protection of internal doors is equally crucial. Interior door security plays a pivotal role in creating a holistic security architecture, ensuring that sensitive areas within the hospital—such as neonatal units, operating rooms, and medication storage facilities—are fortified against unauthorized access and potential threats. This measure not only mitigates risks associated with external intrusions but also addresses internal threats, maintaining a safe and secure environment for patients, staff, and visitors, as well as sensitive information.

To enhance security for internal doors that may presently be controlled by mechanical keypads, the most cost-effective approach is the installation of wireless locks. Hospitals benefit from this upgrade in various ways. Firstly, it boosts security significantly by enabling real-time monitoring and control over access rights. Administrators can promptly grant or revoke access, adjust schedules, and monitor door status from a centralized platform. This agility is vital during emergencies or when dealing with sensitive areas.

Secondly, wireless systems mitigate risks linked to lost keys or compromised codes, as changes to access rights can be swiftly implemented without the need for physical alterations to locks or key reissuance. Additionally, the integration of wireless locks with broader security systems like video surveillance and alarms offers a comprehensive security strategy. This not only enhances the effectiveness of security operations but also ensures a seamless user experience, guaranteeing uninterrupted patient care amidst security protocols.



The Versatility of Multifunctional ID Cards

Multifunctional ID cards enhance hospital security and operational efficiency, serving multiple purposes beyond simple identification. These ID cards, equipped with smart technology, not only facilitate secure and restricted access to sensitive areas but also promote a streamlined workflow.

Employees can use them to access locked doors within the hospital, particularly in high-security zones such as the medication storage rooms and cabinets, neonatal units, and private patient records archives.

Beyond access control, these ID cards are integrated with time and attendance systems, medication tracking and management systems, and cafeteria and vending machines for financial transactions. In emergency situations, multifunctional ID cards can expedite the identification process, ensuring that only authorized personnel are granted access to critical areas, thereby streamlining the response to incidents.



The Future of Access Control in Healthcare

The trajectory of access control in healthcare is steering towards highly customized and adaptable solutions, reflecting the sector's dynamic needs. Emerging trends such as cloud-based solutions enable remote management and scalability, revolutionizing how healthcare facilities secure their premises.


Additionally, the integration of mobile access technology allows for more streamlined and user-friendly authentication processes, enabling staff and authorized personnel to access secured areas effortlessly. Biometric controls, utilizing unique individual traits for identification, further bolster security measures, ensuring that access is granted only to verified individuals.

Together, these advancements are setting new benchmarks for security within the healthcare sector, promising enhanced protection and accessibility while addressing the complex challenges and vulnerabilities unique to healthcare environments.

Securing Healthcare: The Acre Commitment

Acre is reshaping security with the convenience of one innovative, flexible, and secure solution. Widgets and custom dashboards make your Access Control user experience simple, easy, and customizable to the way you want it. Deployed in the cloud or on-premises, you can engage your best software experience from anywhere with your choice of Windows, macOS, iOS, Android, or any modern browser.

Our RESTful API enables users to deploy an extensive range of technologies through a straightforward process for easy integrations between acre Access Control and a multitude of systems:

- Single card solutions for photo ID badge, access control, time and attendance, payment, and medication management systems
 - Blue light emergency phones to enhance parking garage safety
 - Wireless locks to secure common spaces
 - Mobile credentials for a convenient and modern access control experience
 - Biometric readers for high-security areas
 - Video cameras throughout the hospital
 - Visitor management systems
 - Intrusion and fire systems
 - Active directory connection to streamline HR operations
- 

In conjunction with our open API, users gain unrealized operational efficiency with the unique acre FITS (Functional Integration Toolkit Scripts) process automation capabilities. FIT Scripts combine programming, integrations, and workflows to deliver maximum efficiency daily, and reporting for event, system, and process analysis.

Our company holds the ISO 27001 certification for our cloud-based access control and visitor management solutions, demonstrating our dedication to implementing robust Information Security Management Systems (ISMS) that meet the highest standards set by the International Organization for Standardization. This certification underscores our commitment to safeguarding data with utmost security and reliability.

We pride ourselves on being the experts backed by 45 years as a physical security industry leader. As a trusted name in safeguarding assets worldwide, acre security is known for our proficiency and our unwavering pledge to security excellence. Our state-of-the-art technology is scalable to worldwide enterprise levels and strikes the perfect balance between advanced security features and user-centric operability.

At acre security, our commitment to you is simple: We want to eliminate your risk. We don't want you guessing if you're secure. We want you to know. And, we have the experience, expertise, & execution to do it, with 21% of our company resources focused on R&D. The technology we choose, driven by the end user experience we desire, impacts the software we develop, and adheres to our go-to-market strategy of being a disruptor. Reshape your security perspective, explore new possibilities for productivity, and find innovative ways to meet your strategic business goals by simply choosing acre.





**Enhancing
Security and
Efficiency in
Healthcare Facilities
Through Integrated
Access Control**

acresecurity.com