



Physical Identity and Access Management (PIAM) for Healthcare

Manage the entire physical access lifecycle of **everyone** within a healthcare environment

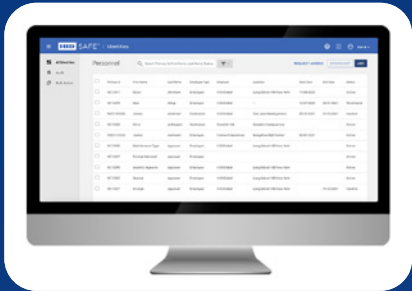
In hospitals and healthcare facilities, the responsibility for safety and security is spread across employees, patients, visitors and diverse groups of people associated with wards, campuses and buildings at any given time. To deliver a secure and future-ready environment that reduces the risk of infection, healthcare organizations must rethink how they manage the lifecycle of **every** identity and their physical access activities — from employees to temporary clinicians, contractors, vendors and more.

While a visitor management solution captures the lifecycle of visitors within a hospital, healthcare organizations are faced with the challenge of managing unique access requirements for many more identities whose needs may change rapidly. As a result, these organizations often use siloed systems and manual processes, which only add complexity when managing physical access activities — such as onboarding, verification, access authorization and management, credential management, reporting and analytics.

The Solution: Complete, Streamlined Physical Identity and Access Management (PIAM) With HID SAFE™

Extend your patient visitor management with a single and highly scalable solution to orchestrate all physical access across various identity types and complex systems — including IT, access control, electronic health systems and more. HID's PIAM for Healthcare solution provides a purpose-built security solution that addresses the operational and compliance challenges unique to a healthcare environment.

PIAM for Healthcare integrates and exchanges information with:	Giving healthcare organizations a simple, single location to:
- Human resources database - IT/Active Directory - Internal and external watch lists and databases - Training systems (LMS) - Emergency notification systems - Physical access control systems (PACS) - Tenant access control - Biometric systems - Other third-party systems	- Provision, manage and validate all identities, not just permanent employees, including temporary clinicians, vendors and more - Screen, authorize, onboard, and badge multiple new workers quickly and efficiently - Coordinate and check in visitors (patients, vendors, contractors) with self-service portals and kiosks - Manage badges and credentials - Manage access requests, changes and approvals from both admin and user self-service portals - Conduct audits and reports - View automated reporting analytics - Identify risks and suspicious activities proactively using the HID SAFE Analytics optional add-on
Which helps to:	
- Break down silos between different operational departments and processes, such as facilities, IT and security - Orchestrate security processes across various campuses, networks, wards and high-risk areas - Gain better control over convoluted controls around physical IDs, including those for extended identities (contractors, partners, visitors, etc.) - Reduce hospital administration and operational costs, in addition to auditing times	- Ease repeated entry and exit with smarter policies and technology, including kiosk onboarding - Establish digital vetting procedures to speed up visits and deny sick visitors, reducing the risk of external infection - Maintain a "banned persons" list enforceable through digital automation to protect patients and staff from specific people - Drive CDC, JCAHO, IAHSS, and HIPAA compliance as well as local health departments and Joint Commission regulation through consistent policies and regular reporting



BENEFITS OF SAFE

- Unifies complex healthcare systems and networks to provide combined cyber and physical security
- Provides an intuitive, web-based interface for administrators to perform all access-related activities — from anywhere
- Saves time and resources onboarding new complexes, buildings, facilities and personnel with its integrated approach
- Provides healthcare organizations with the who, why, where, when and how of all access activities across disparate buildings, locations and campuses
- Minimizes administrative time and resources spent on managing complex identities and their access within a constantly changing environment
- Drives adherence to compliance requirements, including HIPAA, GDPR and ISO27001
- Reduces audit times dramatically through regular automated reporting