MAVIN TECHNOLOGIES

Mavin Insights

Developed by Seibold Security and Mavin Technologies.

HOSPITALS CAN MITIGATE RISK
DIGITAL PASSWORDLESS ACCESS CONTROL

Mavin Technologies is on the forefront of innovation, integration, and reliability for Hospital Security Solutions

Bad Actors (internal and external)

According to an article from The HIPPA Journal - Security Breaches in Healthcare in 2023 - with healthcare data breaches increasing year-over-year, something needs to be done to help healthcare organizations improve resilience. Aside from cyber-hacking incidents, there are several other types of security breaches in healthcare. There was a 10.4% increase in unauthorized access and disclosure incidents in 2023 and a 13.6% increase in impermissibly accessed or disclosed records. 127 Unauthorized access/disclosure incidents were reported in 2023 and 8,598,916 records were accessed or disclosed across those incidents. These HIPAA breaches may be smaller than the hacking incidents, averaging 67,708 records per incident (median 1,809 records), but they can be just as harmful.

Identity Access Management (IAM)

According to Texas Healthcare Association - One area of critical focus that spans both external and internal security strategy concerns is Identity access management. The stronger the organizational commitment to Identity and access management, the tougher it is for threat actors to breach an organization passively.

Many cyber exploits are carried out via simple end-user exploits, the most common being phishing emails in their many forms. Implementing dual-factor authentication is a very effective countermeasure against most phishing exploits that target harvesting credentials. In addition to being an effective countermeasure, dual-factor authentication also serves to alert the organization of cyber threats through failed log-in attempts by threat actors who have harvested credentials but can't provide the second-factor credential in the authentication process. These failed attempts are logged and if properly monitored can alert the IT team to suspicious activity.

Conducting periodic access reviews of privileged network access accounts, and privileged users, is also a strong measure for ensuring that access to network resources and applications is limited to the appropriate employees and organizational roles, and that said access is being used appropriately. Routinely auditing access to information systems to ensure that only the right roles and individuals have access, and that the degree of access is appropriate for the role, is a critical activity that serves the dual purpose of ensuring that identity access is appropriate, and that organizational controls are working as intended.

A Partial List of Overarching Threats Related to IAM

Hospitals face many types of risk and threats. Here we focus on elements related to IAM:

- Ransomware Attacks: Cybercriminals target hospital systems to encrypt data and demand a ransom for its release.
- Data Breaches: Unauthorized access to sensitive patient data can lead to identity theft and financial fraud.
- Phishing Attacks: Employees may be tricked into revealing confidential information or downloading malicious software.
- Shared passwords or shared credentials to access records.
- The constant evolution of security policies, password expiration, complexity to administer and support.
- The battle between security & usability.
- Changes in Healthcare Regulations: New laws and regulations can impose additional burdens on hospital administration and operations.
- Security Breaches: Unauthorized access to hospital premises can endanger patients, staff, and sensitive equipment.
- IT System Failures: Downtime in hospital information systems can disrupt patient care, billing, and administrative functions.

Many hospitals are implementing comprehensive risk management strategies to mitigate these threats and ensure the safety and well-being of patients and staff. One place to start or focus on is related to streamlining systems access for hospital employees.

Passwordless Authentication for Hospital Employees

As hospital workers grapple with the dual challenge of maintaining robust security protocols while needing instantaneous access to sensitive patient data. Existing password systems further heighten the risk of breaches and slow down critical response times.

A passwordless solution, leveraging advanced authentication methods such as facial recognition and access cards, can fortify the security infrastructure and ensure seamless, hygienic, and rapid access to necessary information - effectively enhancing operational efficiency and safeguarding patient data.

Such a solution enables:

- Frequent Authentication – allowing doctors and nurses rapid and continuous access to secured systems.
- Improved hygiene through dramatic reductions in physical interactions with security systems.
- Enhance smooth transition between shifts through quick yet secure authentication methods to avoid delay in patient care.
- Hospital staff use a range of devices, through an authentication solution that is both secure and versatile.
- Better adherence to strict regulatory guidelines, including those governing access to patient data.
- Quick access to systems in emergencies – this can be a matter of life and death.

Mavin Technologies has the Solution

Mavin affords hospitals a comprehensive platform with their HR application being the source of truth (including capturing the users' image). Physical access to the building, nested areas, labs, pharmacies, emergency rooms, radiology, surgery, and others can be properly secured and real-time updated. Then access privileges are enhanced with logical access "your" applications on "any shared device".

Accomplished through facial recognition there are no passwords to manage, and security is vastly improved as employees/contractors access records, RX requests, critical technology and machines (MRI, EKG, etc.), and email, HR employee systems, and other applications. Our solution will eliminate pin numbers, or passwords that get hacked, or improperly shared.

Through physical and IT convergence, if a doctor or RN hasn't physically entered the building, access to secure applications on the network can be denied. Or security video can be tied to denied application login requests. There's a great deal of security synergies yet to be explored...

Mavin can help hospital IT and security leaders address overall business-organization strategy, productivity, security, and risk management objectives.

Our customers tell us our knowledge, process, and follow-through for service are innovative and unusually comprehensive, providing the highest Return on Investment and reducing the Total Cost of Ownership.

Contact a subject matter expert at hospital-security@go-mavin.com