

Securing the Future of Healthcare: Insights into Security and Resilience Across the Organization

Table of Contents

Introduction	3
The Survey:	
A Snapshot of Healthcare Security in 2024	4
The State of Healthcare Security	5
Dissatisfaction and Insufficiency	
with the Status Quo	6
Cybersecurity:	
The Growing Threat in Healthcare	7
Evolving Security Practices: From Physical to Digital	
Identity Management and Beyond	8
Securing Visitor Access:	
Enhancing Safety and Streamlining Compliance	10
Manual vs. Automated Security:	
The Shift Towards Real-Time Responses	11
Barriers to Technological Adoption:	
Budget Constraints and Beyond	12
The Future of Healthcare Security	13
Looking Ahead	15



Introduction

Healthcare facilities are the cornerstone of community health and safety, where the protection of patients, staff, and sensitive data is paramount. As healthcare institutions continue to evolve, they face an increasingly complex landscape of both physical and digital threats. In the first eight months of 2024, there was a surge in cyberattacks targeting healthcare, with 428 breaches reported to the U.S. Department of Health and Human Services. More than 53 million individuals¹ have been identified as affected by these breaches, underscoring the critical need for robust, integrated security strategies.

Drawing on a comprehensive survey of healthcare security professionals and a review of recent, high-profile security incidents, this report provides insights into the current state of healthcare security, revealing both challenges and opportunities for improvement.



The Survey: A Snapshot of Healthcare Security in 2024

To understand the current state of security in healthcare, a survey was conducted by HID in early 2024, engaging over 200 security and IT professionals across a broad range of healthcare facilities. The survey aimed to capture the realities of security practices, challenges, and perceptions within the industry, offering a detailed view of the current landscape.

The survey attracted responses from a wide range of healthcare institutions, reflecting the diverse nature of the industry. A significant portion of respondents, **40%, were**

from large network hospitals (Q1), which are often at the forefront of adopting new technologies but face unique security challenges due to their size and complexity. **Another 13% of respondents represented urban/suburban university hospitals (Q1)**, known for their advanced research capabilities and specialized care.

Rural healthcare facilities accounted for 20% of the responses, distributed across various facility types (Q1), from small rural clinics to larger regional hospitals. This inclusion provides a comprehensive

view of security practices across different geographical settings, highlighting the unique challenges faced by rural healthcare providers. In terms of organizational size, **28% of respondents were from institutions with fewer than 500 employees (Q2)**, while **36% were from large organizations employing over 10,000 staff members (Q2)**. This diversity underscores the need for adaptable, layered security solutions that can scale to meet the demands of both small and large healthcare providers, in both urban and rural environments.

The State of Healthcare Security

As healthcare providers increasingly adopt digital technologies, they inadvertently expand the avenues through which threats can penetrate. These technologies have brought significant benefits, including improved patient care, enhanced operational efficiency, and more effective data management². This shift has also made healthcare facilities prime targets for cyberattacks, as evidenced by the alarming rise in breaches reported in 2024. Large network hospitals, often hubs of medical innovation, are particularly vulnerable due to their complex IT environments and the vast amounts of sensitive data they manage.

However, the challenges to healthcare security extend beyond digital threats. Physical security in healthcare facilities, particularly hospitals, presents significant and growing risks. Unauthorized entry into sensitive areas, whether through physical breaches, tailgating, or the use of forged credentials, poses an ongoing threat. Hospitals, by nature, are open and accessible environments, which makes managing entry points more difficult. Emergency rooms, patient wards, and administrative areas can all become vulnerable when physical access control systems are insufficient or inconsistently enforced. According to the **International Association for Healthcare Security and Safety (IAHSS)**³, maintaining proper control over patient

and visitor movement is essential for preventing violence and unauthorized access to restricted areas. In addition to external threats, hospitals must also protect patients and staff from internal risks, including violent individuals. IAHSS emphasizes the growing risk of patient and visitor violence, noting that security personnel must be trained to handle hostile or aggressive situations effectively. This highlights the need for comprehensive security policies and integrated physical security systems that include surveillance cameras, biometric access controls, and automated alert systems to mitigate threats before they escalate.

Recent advances in security technologies, such as the integration of facial recognition and artificial intelligence-driven surveillance, are increasingly being adopted by healthcare facilities to track and manage individuals entering and moving within the healthcare facility. These systems can flag unauthorized individuals, monitor unusual behavior, and assist security personnel in responding to potential breaches in real time.

However, implementing these physical security measures comes with its own set of challenges. Many hospitals struggle with maintaining up-to-date physical security infrastructure due to budget constraints or logistical

complexities. In addition, managing the large number of daily visitors including patients, families, contractors, and vendors, creates a constant security challenge that is difficult to manage without advanced systems. Modern healthcare facilities need to strike a delicate balance between providing an open, welcoming environment and ensuring that only authorized individuals have access to sensitive areas.

Securing both physical and digital environments is further complicated by the diversity and number of individuals interacting with healthcare systems daily. Each of these touchpoints, whether they involve staff, patients, visitors, or contractors, represents a potential vulnerability that can be exploited if not adequately secured. The need to manage these interactions securely, while ensuring the seamless flow of operations, places immense pressure on healthcare institutions to adopt comprehensive security strategies that encompass both physical and digital control measures.



Dissatisfaction and Insufficiency with the Status Quo

Despite the widespread recognition of the importance of security, the survey reveals a concerning level of dissatisfaction with current measures. A total of **32% of respondents reported not being satisfied with their existing security frameworks**, indicating feelings of neutrality, dissatisfaction, or extreme dissatisfaction. Additionally, **45% of respondents indicated they were only somewhat satisfied (Q4)**. These figures highlight an industry that is acutely aware of the risks but is still searching for effective solutions to mitigate them.

The dissatisfaction reported in the survey reflects a broader industry struggle to keep pace with the evolving threat landscape. **Many healthcare institutions surveyed (71%) (Q5) have implemented basic cybersecurity measures, such as firewalls and antivirus software**, yet these are no longer sufficient to defend against

sophisticated cyber threats that target both digital data and the physical operations of healthcare facilities. The integration of physical and digital security measures, while increasingly recognized as necessary, remains a work in progress for many organizations. This ongoing search for effective solutions underscores the need for innovation and adaptability in healthcare security strategies, particularly as institutions continue to expand their digital footprints.





Cybersecurity: The Growing Threat in Healthcare

The increasing digitization of healthcare has made it a prime target for cybercriminals. High-profile attacks such as the **Change Healthcare Attack⁴ (February 2024)** and the **Ascension Health System Attack⁵ (May 2024)** have brought to light the vulnerabilities inherent in current systems. In the Change Healthcare incident, a ransomware attack crippled operations across the United States, exposing sensitive patient data and forcing the company to pay approximately \$22 million in ransom.

Similarly, the Ascension Health System attack led to the shutdown of critical patient care systems, disrupting services and delaying surgeries across multiple states. These incidents are not isolated; in **May 2021, Scripps Health⁶**, a major healthcare provider in Southern California, fell victim to a ransomware attack that forced the shutdown of its IT systems across all five hospitals.

The attack severely disrupted patient care, including emergency services, as staff were forced to revert to manual processes. This incident also led to the temporary diversion of critical care patients and the cancellation of non-emergency procedures. These cases highlight the urgent need for healthcare facilities to strengthen their cybersecurity frameworks and adopt more resilient systems to safeguard against such threats.



Evolving Security Practices: From Physical to Digital Identity Management and Beyond

The healthcare industry is witnessing a significant shift in how it manages both identity and security. This shift is twofold: first, from physical methods to digital solutions in identity management, and second, toward a more integrated approach that blends physical and cyber security measures. These transitions are designed to enhance patient care and experience, improve staff safety so they can perform their best work, efficiently manage visitors, and streamline workflows with future-proof solutions.

Transitioning from Physical to Integrated Digital Identity Management

Traditional methods such as visual ID badges and lanyards remain widely used in the healthcare industry, serving as a key component of many facilities' security strategies. However, these methods are increasingly being supplemented or, in some cases, replaced by digital credentials like mobile and biometric authentication.

According to the survey, **32% of healthcare facilities already utilize biometric authentication, and 11% have adopted facial recognition technologies (Q5)**. This trend reflects a broader move towards more secure, scalable, and mobile-first identity management solutions, particularly in large urban hospitals where operational efficiency is paramount.

Despite these advancements, the shift towards digital identity methods introduces new challenges. While **74% of facilities continue to leverage physical access control systems, and 80% use surveillance cameras to monitor their environments (Q5)**, healthcare facilities must carefully balance digital solutions with traditional visual identification methods such as badges, which remain crucial in many areas. The continued reliance on visual ID methods is particularly important in environments where physical confirmation of identity remains a key security measure, such as high-traffic zones and sensitive areas.

As healthcare facilities continue to embrace digital identity solutions, it is essential to integrate these with existing physical security measures to ensure a layered security approach that mitigates potential vulnerabilities. This combination of visual identification, physical access control, and digital credentials creates a more comprehensive and resilient security framework that safeguards both physical and digital environments.

Integrating Cyber and Physical Security Systems

As healthcare facilities evolve, the need to integrate cyber and physical security systems has become increasingly critical. **A significant 77% (Q11) of survey respondents believe that it is important for their facilities to achieve this integration**, reflecting the growing recognition that comprehensive security strategies must address both the digital and physical environments where care is delivered. While many institutions have implemented cybersecurity measures such as firewalls and antivirus software, these digital protections alone are not enough. Effective security strategies must also encompass the physical environments where care is delivered, ensuring a comprehensive defense against threats that span both domains.⁷

The convergence of cyber and physical security, often referred to as cyber-physical systems, enables healthcare facilities to respond more effectively to a wide range of threats. For example, integrating cybersecurity systems with physical access control, visitor management solutions, and real-time location systems (RTLS) can prevent unauthorized access to sensitive areas by detecting and responding to potential threats in real time. RTLS further enhances security by allowing facilities to track the precise location of assets, staff, and visitors in real time, helping to manage security risks more effectively.

This layered security approach ensures that healthcare facilities are not only protecting digital assets but also securing the physical spaces where those assets are utilized. Incorporating physical security measures, such as surveillance cameras, biometric access controls, and RTLS, into a unified security framework can significantly enhance a facility's ability to protect both its people and its data.

For instance, secure access to sensitive areas and easy, secure workstation login for staff are critical components of protecting patient data and improving staff safety. By streamlining workflows through the use of these integrated systems, healthcare facilities can reduce the loss, theft, and mismanagement of assets, while also supporting disaster recovery and compliance efforts.



Securing Visitor Access:

Enhancing Safety and Streamlining Compliance

The ability to easily and effectively manage visitors through these integrated systems is essential. Currently, **38%** of healthcare facilities still rely on paper forms and badges to manage visitor access (Q12). While **30%** have implemented access control systems and **24%** use electronic patient management solutions, many healthcare facilities are still in the process of upgrading their visitor management practices.

Providing visual identification for visitors and preventing bad actors from accessing sensitive areas or data helps ensure that healthcare environments remain safe and secure. This enhances the visitor experience and facilitates compliance and reporting needs, which are increasingly important as healthcare regulations become more stringent.

As the healthcare sector continues to expand its digital footprint, the importance of a holistic, layered security strategy cannot be overstated. This approach not only helps in safeguarding critical infrastructure but also in maintaining the trust and safety of patients, staff, and visitors alike. By adopting future-proof solutions that integrate multiple security layers, healthcare facilities can ensure they are prepared to meet both current and future challenges.





Manual vs. Automated Security: The Shift Towards Real-Time Responses

Security in healthcare is also evolving from traditional, manual interventions to more automated, technology-driven solutions. The survey highlights this shift, with **56%** of healthcare facilities now utilizing automated alert systems that can **provide real-time notifications of potential threats (Q7)**. These systems allow staff to respond efficiently to emerging situations, often before they escalate into full-scale incidents.

A valuable addition to these automated systems is the duress badge, which allows healthcare workers to discreetly signal distress by pressing a button on their badge. Unlike traditional panic buttons, which are still in use at **58% of facilities (Q7)** and may draw attention, the duress badge is inconspicuous. It enables staff to alert security without escalating a potentially dangerous situation. By integrating with Real-Time Location Systems (RTLS), security personnel can pinpoint the exact location of the distressed worker and respond quickly and effectively. This system provides an additional layer of security by offering a discreet and immediate response to incidents, enhancing staff safety without disrupting patient care or escalating the situation.

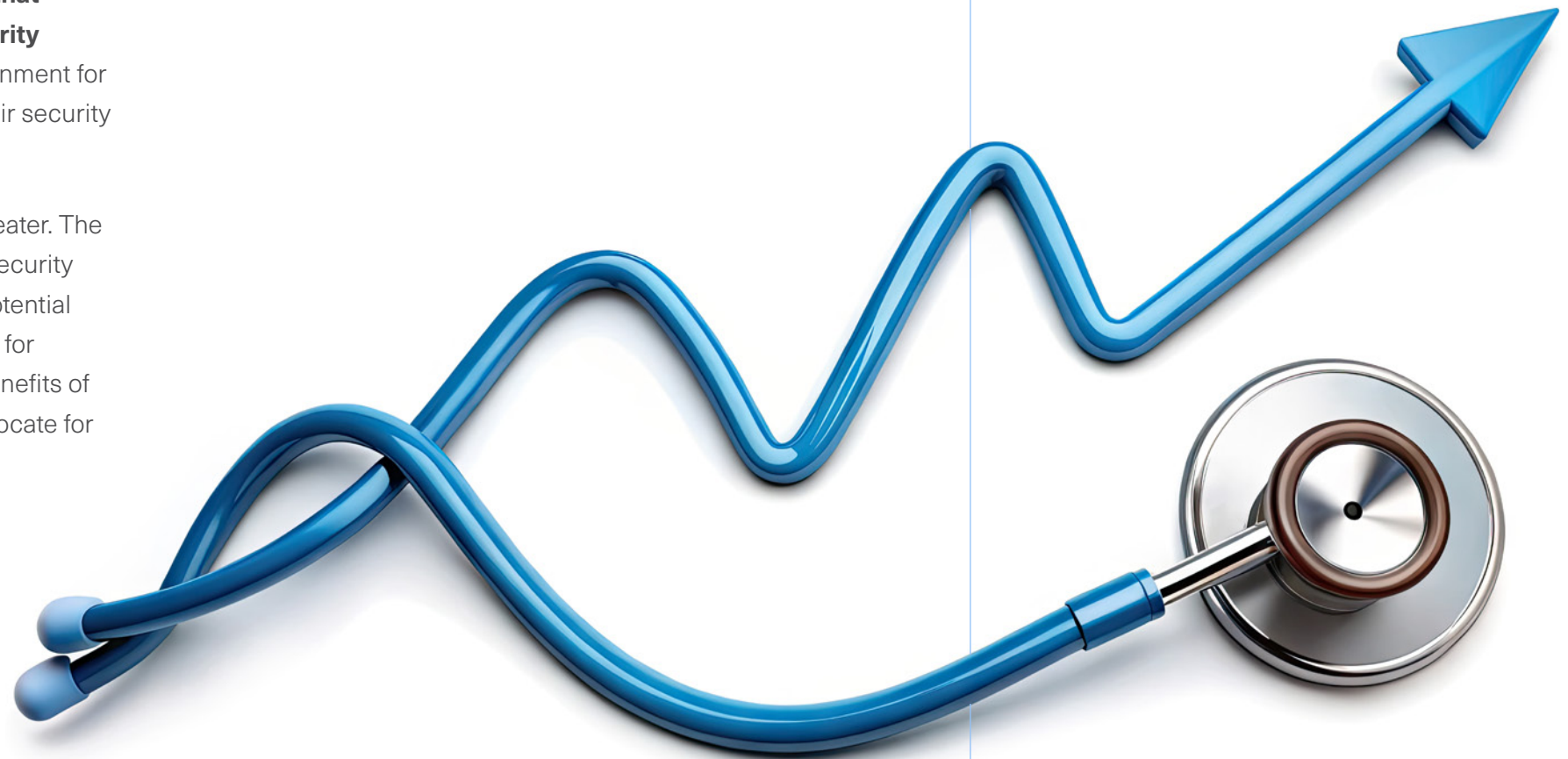
While manual duress buttons remain an important tool, particularly in situations where immediate physical action is necessary, they are inherently reactive, responding only after an incident has already begun. In contrast, the duress badge, when combined with automated alert systems, shifts security towards a more proactive model, allowing incidents to be addressed before they escalate further.

The data suggests a clear trend towards automating security processes, as **53% of survey participants foresee this evolution (Q15)**, providing a more comprehensive approach to safeguarding healthcare environments. As facilities continue to adopt automated systems, the reliance on manual interventions alone will decrease, enhancing overall response times and reducing the likelihood of incidents escalating. As these automated systems become integrated with both cyber and physical security measures, they will contribute to a more resilient and responsive healthcare security environment.

Barriers to Technological Adoption: Budget Constraints and Beyond

While the need for advanced security measures is clear, the path to implementation has many challenges. **The survey revealed that budget constraints are the most significant barrier, cited by 74% of respondents (Q9). This financial pressure is compounded by a lack of executive support (31%) and the perception that security upgrades are not a top business priority (24%).** These factors create a challenging environment for healthcare organizations seeking to enhance their security infrastructure.

However, the cost of inaction is likely to be far greater. The financial and reputational damage caused by a security breach can be devastating, not to mention the potential impact on staff and patient safety. It is imperative for healthcare leaders to recognize the long-term benefits of investing in robust security measures and to advocate for the necessary resources to protect people and their institutions.



The Future of Healthcare Security

Looking to the future, the survey results suggest that healthcare facilities are preparing to embrace a diverse range of new technologies designed to enhance security. AI-driven solutions are at the forefront of these plans, with **53% (Q15)** of respondents anticipating greater reliance on AI and automation over the next five years, and **35% (Q14)** already expressing interest in adopting these technologies in the next 12-24 months. AI offers the potential to revolutionize healthcare security by enabling faster, more accurate threat detection and response, providing a critical advantage in the fight against cyber threats.

Integration of physical and cybersecurity

In addition, **67% (Q15)** of respondents foresee an increased integration of physical and cybersecurity systems, highlighting the importance of a unified approach to protecting both digital assets and physical environments. This convergence is essential for creating a comprehensive security framework that can adapt to the complexities of modern healthcare facilities.

There is also significant interest in integrated security management systems, with **33% (Q14)** of facilities planning to adopt these solutions. These systems allow for the seamless integration of both cyber and physical security measures, enhancing the overall security posture of healthcare facilities.

Cloud-based platforms

Cloud-based security platforms are another area of focus, with **31% (Q14)** of respondents planning to adopt these platforms due to their scalability and flexibility, which are crucial for managing the complex and dynamic environments of healthcare institutions.

Enhanced data protection

The survey also highlights a strong focus on enhancing patient data protection measures, with **48% (Q14)** of respondents planning to adopt new strategies to safeguard sensitive information. As healthcare institutions handle vast amounts of personal data, the need for robust data protection protocols is more critical than ever.



Advanced biometrics

Advanced biometric technologies, including fingerprint biometrics (considered by **20% (Q14)** of respondents) and passive live facial recognition (**19% (Q15)**) offer highly secure form factors for healthcare access control and user authentication. Unlike traditional passwords or keycards, these biometric attributes are unique to each individual's physical characteristics and nearly impossible to replicate. These technologies ensure a high level of security, reducing the risk of unauthorized access to restricted locations and sensitive patient information. Additionally, they streamline the access process, improving efficiency and enabling faster, more accurate authentication for healthcare staff.

Digital ID from birth

The concept of "Digital ID from Birth," though still emerging with **11% (Q15)** interest, refers to the creation of a secure digital identity from the moment of birth that is carried throughout an individual's life. This unique digital identifier can be used for secure interactions across healthcare systems, ensuring that patient information is always accurate and accessible, regardless of age or location. The "Digital ID from Birth" approach could significantly streamline patient interactions by reducing the need for multiple forms of identification and ensuring continuity of care, while improving security by preventing identity fraud from an early age.

Enhanced cybersecurity

Moreover, **43% (Q14)** of respondents plan to enhance their existing cybersecurity measures, reflecting an ongoing commitment to protecting digital assets. However, the successful implementation of these technologies will largely depend on comprehensive staff training, a priority for **47% (Q14)** of respondents. Without effective training, even the most advanced technologies can fail to protect against threats, underscoring the importance of pairing new tools with robust education initiatives.

Improved compliance and training

As healthcare facilities continue to expand their digital footprints, improving compliance with regulations remains a key concern, with **28% (Q14)** of respondents focusing on this area. The adoption of these technologies, along with the emphasis on training and compliance, highlights the sector's proactive approach to security in an increasingly complex threat landscape.



Looking Ahead

As healthcare institutions continue to digitize their operations, the need for robust, integrated security strategies has never been more critical. Survey data underscores the industry's recognition of this need, with a clear majority of respondents prioritizing the convergence of cyber and physical security systems as essential to safeguarding both digital assets and physical environments.

The shift from physical to digital identity management, coupled with the adoption of AI-driven solutions, integrated security management systems, real time location systems and more, marks a pivotal moment for healthcare security. These advancements promise to enhance patient care and

experience, improve staff safety, streamline workflows, and ensure the effective management of visitors. However, these benefits can only be fully realized through a comprehensive approach that includes robust policies, ongoing staff training and a commitment to regulatory compliance.

The barriers to adopting these advanced security measures, particularly budget constraints and a lack of executive support, highlight the financial and operational challenges facing healthcare organizations. Yet, the potential cost of inaction, both in terms of financial loss and the safety of patients and staff, demands that healthcare leaders prioritize investments in security. Future-proof solutions that integrate

multiple layers of protection are not just a response to current threats but a necessary strategy for maintaining resilience in the face of an increasingly complex threat landscape.

By adopting a layered security approach and embracing innovation, healthcare institutions can ensure they are safeguarding their patients, staff, and data while building a resilient foundation for the future.

References:

1. [HHS.gov - U.S. Department of Health and Human Services Office for Civil Rights Breach Portal](#)
2. [Yeung et al 2023 - The promise of digital healthcare technologies](#)
3. [IAHSS - Violent Patient/Patient Visitor Management](#)
4. [The HIPAA Journal Change - Healthcare Reports Ransomware Data Breach to HHS](#)
5. [Forbes - Ascension Attack Intensifies Scrutiny Of Healthcare Cyber Defenses](#)
6. [Tech Target - Scripps Health Reaches \\$3.5M Settlement After Ransomware Attack](#)
7. [Integrated Cyber-Physical Security Approach for Healthcare Sector](#)



hidglobal.com

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

© 2024 HID Global Corporation/ASSA ABLOY AB.
All rights reserved.

2024-10-22-cc-securing-future-of-healthcare-eb-en
PLT-08044

Part of ASSA ABLOY