ONCLAVE

Healthcare Cybersecurity Overview 2024

Prepared by Onclave Networks, Inc
August 2024

20868 Channel Court Potomac Falls, VA 20165-7415 703 571-6595

Healthcare Cybersecurity Overview 2024

Executive Summary

The healthcare industry faces unprecedented cybersecurity challenges at a critical juncture in its digital transformation. This overview provides a comprehensive look at the current state of healthcare cybersecurity, highlighting key trends, risks, and protection strategies.

The Critical Need for Zero Trust Cybersecurity in Healthcare

As healthcare becomes increasingly digitized, the security of patient data and critical systems has never been more important. This section outlines why Zero Trust cybersecurity is becoming essential in the healthcare sector.

U.S. healthcare systems continue to integrate advanced technologies like IoT and OT devices, and the need for robust cybersecurity has never been more critical. Over the next 36 months, hospitals and healthcare systems are expected to rapidly adopt Zero Trust cybersecurity due to increasing cyber threats, data breaches, compliance requirements, and the shift towards value-based care.

Data breaches in 2024 include Change Healthcare (February), Kaiser Permanente (April), Ascension Health (May) and Michigan Hospital systems, suffered its second breach in a year (August 2024, September 2023).

The cyber threat extends beyond medical devices. In addition to medical devices in recent years, cybersecurity attacks targeting devices that manage critical infrastructure within hospitals—such as HVAC systems, door controls, lighting, and other building management systems—have become increasingly prevalent. These devices, which are essential for maintaining a safe and operational environment in healthcare facilities, present unique cybersecurity challenges.

Healthcare Landscape and Financial Overview

To understand the scale of the cybersecurity challenge in healthcare, it's crucial to first grasp the industry's size and complexity. This section provides key statistics on healthcare infrastructure and financial scale.

Hospital Infrastructure (2024)

- Registered hospital beds: ~916,752
- Hospitals/healthcare systems: 5,129
- Military hospitals: 48
- Veterans Affairs hospitals: 171
- Additional facilities: 10,000+ urgent care centers, ambulatory surgery centers, long-term care hospitals, outpatient clinics, rehabilitation facilities, hospice centers, and dialysis centers

Financial Scale

The total annual spend in 2023 for healthcare in the US was approximately $4.5 trillion or 18.3% of our GDP for 2023.

- Patient revenue (hospitals only): $1.3 to $1.4 trillion
- Government supported healthcare $1.6 trillion
- Private insurance over $1 trillion
- Out-of-Pocket $450 billion

Cybersecurity Investment

As the threat landscape evolves, healthcare organizations allocate more resources to cybersecurity. This section outlines current investment trends in the industry.

- Percentage of net patient revenue spent on cybersecurity: 0.5% to 2%
- Percentage of IT budget allocated to cybersecurity:
    - Small to mid-sized hospitals: 4% to 7%
    - Larger hospitals and health systems: 6% to 10%

Projected Growth in IoT and OT Device Use in Hospitals (2025-2030)

The rapid adoption of the Internet of Things (IoT) and Operational Technology (OT) devices in healthcare is both a boon for patient care and a challenge for cybersecurity. This section projects the growth of these technologies and their impact on healthcare operations.

- CAGR of healthcare IoT market: 20% to 25%
- Total IoT devices: Expected to grow from ~10 billion (2025) to ~30 billion (2030)
- OT device growth: 15% to 20% annually
- Increased dependency on IoT/OT for core operations: 50% to 70% by 2030

Key Drivers for Adopting Zero Trust Cybersecurity

Several factors are pushing healthcare organizations towards adopting Zero Trust cybersecurity frameworks. This section outlines the primary motivators behind this shift.

- Increasing cyber threats
- Data breaches and ransomware attacks
    - Average total reported costs of a cyberattack: $10 to $13 million
- Compliance requirements (Federal and State)
- Leadership and management liability
- Digital transformation
- Value-based care model shift

Indirect Drivers Reinforcing the Need for Zero Trust

Beyond the direct cybersecurity concerns, several indirect factors underscore the importance of robust cybersecurity measures in healthcare. This section explores these additional motivators.

- Board of Directors and legal liability
- Public relations and reputation management

- Operational impact
- Regulatory impact
- Increased cybersecurity investment

Cyber Insurance Considerations

The healthcare industry is facing significant challenges regarding cyber insurance due to the increasing frequency and severity of cyberattacks, particularly ransomware. Here are some key business issues and trends.

- Rising Premiums and Reduced Coverage
- Challenges in Policy Definitions
- Difficulties in Risk Assessment
- Impact of Emerging Threats

Compliance Requirements

Healthcare organizations must navigate the complex landscape of federal and state regulations. This section provides an overview of key compliance requirements that impact cybersecurity strategies.

Federal Compliance

Federal regulations set the baseline for healthcare cybersecurity across the United States. Here are some of the most important federal requirements:

- HIPAA (Health Insurance Portability and Accountability Act)
- HITECH Act (Health Information Technology for Economic and Clinical Health Act)
- 21st Century Cures Act
- FISMA (Federal Information Security Management Act)
- FDA (Food and Drug Administration) Guidance
- CISA (Cybersecurity and Infrastructure Security Agency) Initiatives

State Compliance Examples

In addition to federal regulations, state-level compliance requirements add another layer of complexity to healthcare cybersecurity. This section examines some of the most notable state-level regulations.

- California Consumer Privacy Act (CCPA)
- New York SHIELD Act
- Texas Medical Records Privacy Act
- Massachusetts Data Privacy Law (201 CMR 17.00)

ONCLAVE

Onclave Healthcare Solutions

Onclave's TrustedPlatform has been recognized for its potential to enhance security in the healthcare industry. Specifically, Onclave has been referenced in NIST SPECIAL PUBLICATION 1800-30C for securing Telehealth Remote Patient Monitoring Ecosystems. This recognition highlights the platform's ability to provide secure and reliable communication in the transmission of sensitive patient information and data between healthcare providers, patients, and medical devices.

Furthermore, Onclave's TrustedPlatform has also been included in the NATO “Zero-Trust Architectural Framework Enterprise” (ZAFE) pronounced SAFE, hospital in a box. This designation highlights the platform's ability to support secure communication and data management in austere and high-threat environments, making it ideal for deployment in disaster response and military medical operations.

In summary, Onclave's TrustedPlatform provides a secure and reliable solution for the healthcare industry, ensuring the protection of sensitive patient information and data. Its recognition by NIST and NATO showcases its ability to enhance security in telehealth and medical operations, making it a valuable asset for healthcare organizations looking to improve their cybersecurity posture.

ZAFE

Onclave's TrustedPlatform can be used to secure healthcare in several ways:

1. Confidentiality of patient data: With the integration of NIST post-quantum cryptography algorithms, the TrustedPlatform provides strong encryption and secure communication of sensitive patient data, ensuring its confidentiality.
2. Secure data exchange between healthcare providers: The TrustedPlatform can be used to establish secure network overlays between healthcare providers, enabling them to exchange patient data securely and comply with regulations such as HIPAA.
3. Remote patient monitoring: The TrustedPlatform can be used to secure the transmission of patient data collected from remote monitoring devices, ensuring the privacy and security of this information.
4. Clinical trial management: The TrustedPlatform can be used to secure the exchange of trial data between research institutions, ensuring the confidentiality of sensitive information and enabling compliance with regulatory requirements.
5. EHR systems: Onclave's TrustedPlatform can be integrated into electronic health record (EHR) systems, providing a secure and robust infrastructure for storing and exchanging patient data.
6. Telemedicine: The TrustedPlatform can be used to secure the communication between patients and healthcare providers during telemedicine consultations, ensuring the confidentiality of sensitive information.

Overall, Onclave's TrustedPlatform can play a crucial role in securing healthcare by providing robust encryption and secure communication, enabling healthcare organizations to comply with regulations and protect patient privacy.

Conclusion

Adopting a Zero Trust cybersecurity framework is essential for healthcare organizations to protect sensitive data, comply with regulations, and ensure the safe delivery of patient care. Investing in robust cybersecurity solutions is a strategic move that safeguards the future of healthcare in an increasingly digital and connected world.

Supporting Information

Leadership and Management:

Boards and executives are under increasing scrutiny to manage cybersecurity risks effectively. Failure to do so can lead to significant legal and financial repercussions, as seen in recent high-profile cases involving cyberattacks on healthcare facilities. Over the last few years cases such as Uber's CSO, Yahoo's Directors and Officers where courts have found individuals guilty with fines from cyber breaches.

For healthcare organizations, the implications of these legal precedents are significant. As healthcare systems increasingly rely on connected devices and digital platforms, the role of board members and executives in ensuring robust cybersecurity practices becomes even more critical. Failure to do so not only risks financial penalties and reputational damage but also personal legal liability, particularly in cases where negligence or failure to act can be demonstrated

---

Non-Medical Targeted Areas in Hospitals OT/IoT Systems

- HVAC: systems have been attacked seeking to disrupt operations or demand ransoms.
- Door Controls and Access Systems: Cybercriminals have targeted these to gain unauthorized access to restricted areas or to lock down parts of a hospital during an attack.
- Lighting Systems: With the increasing use of Smart Lighting (controlled by IoT devices)
- Building Management Systems (BMS): Building management systems control various aspects of a hospital's infrastructure, including energy management, elevators, water supply, and more. These systems are crucial for the day-to-day operations of a hospital.

Breakdown of Costs for a Cyber Breach:

In 2023, U.S. hospitals and healthcare systems experienced significant financial losses due to cybersecurity breaches, primarily driven by ransomware attacks and data breaches. The average cost of a data breach in the healthcare sector reached a record high of approximately $10.93 million per incident. This is the highest among all industries, reflecting the sensitive nature of healthcare data and the complex regulatory environment hospitals must navigate.

Overall, the financial impact of breaches on U.S. hospitals is substantial. It is estimated that these breaches collectively cost the healthcare sector billions of dollars annually. For instance, the total costs associated with ransomware attacks, which include not just the ransom payments but also the recovery expenses, lost revenue due to operational disruptions, and legal fees, have surged significantly.

Some high-profile cases have reported losses in the tens of millions per attack. For example, a single major ransomware attack can result in costs exceeding $50 million for a healthcare system, including lost revenue and the cost of restoring services.

- Response and Recovery: Includes costs for IT services to restore systems, data recovery, and cybersecurity consultants.
- Lost Revenue: Revenue lost due to disruption in services, patient diversion, and reduced patient trust.
- Legal and Regulatory Costs: Legal fees, regulatory fines, and costs associated with settlements or penalties.
- Operational Disruption: Costs associated with the disruption of normal hospital operations, including delays in patient care.

Projected Growth in IoT and OT Device Use in Hospitals (2025-2030)

Annual Growth Rate: CAGR (Compound Annual Growth Rate): The healthcare IoT market is expected to grow at a CAGR of approximately 20% to 25% between 2025 and 2030. This rapid growth is driven by the increasing adoption of connected devices for patient monitoring, smart infrastructure, and operational efficiency.

Increase in Connected Devices: Total Devices: The number of IoT devices in healthcare is projected to more than double by 2030, with estimates suggesting a growth from about 10 billion devices in 2025 to nearly 30 billion devices by 2030. This includes a wide range of devices from wearable health monitors to smart infusion pumps and automated surgical tools.

Operational Technology (OT) Integration: OT Device Growth: The integration of OT in hospitals, such as smart HVAC systems, automated lighting, and security systems, is expected to grow by 15% to 20% annually. By 2030, it's anticipated that a majority of hospitals will have fully integrated OT systems, enhancing both patient care and operational efficiency.

Increased Dependency on IoT/OT: Dependency Growth: Hospitals' dependency on IoT and OT for core operations is expected to increase by 50% to 70% by 2030. This dependency reflects the critical role these technologies will play in patient monitoring, data collection, and the management of healthcare facilities.

The primary challenges to growth include ensuring seamless integration, managing cybersecurity risks, and handling the increasing complexity of IoT and OT ecosystems. The integration of AI, data analytics, and telemedicine is reshaping the healthcare landscape, offering potential efficiencies and cost saving but also requiring significant investment.

All of these new capabilities will require secure communications based on zero trust standards.

Compliance Requirements

Federal and state regulations, including the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act), impose stringent requirements on healthcare organizations to safeguard patient data. Non-compliance can lead to substantial fines, making Zero Trust essential for meeting these obligations. Below are examples of the increasing requirements for cybersecurity within healthcare facilities.

Expanded Sample of Federal Compliance Requirements

HIPAA (Health Insurance Portability and Accountability Act)

HITECH Act (Health Information Technology for Economic and Clinical Health Act)

- Increased Penalties: Enhances the penalties for non-compliance with HIPAA and expands requirements for breach notifications.
- Recognized Cybersecurity Practices: Recent amendments allow for reduced penalties for organizations that demonstrate the implementation of recognized cybersecurity practices.

21st Century Cures Act

- Information Blocking Provisions: Imposes penalties on entities that engage in information blocking, which includes inadequate cybersecurity measures that prevent the sharing of electronic health information.
-

FDA (Food and Drug Administration) Guidance

- Cybersecurity for Medical Devices: The FDA provides guidelines for the cybersecurity of medical devices throughout their lifecycle, which impacts hospitals using these devices. Compliance ensures devices are secure against cyber threats.

Expanded State Compliance Requirements

California Consumer Privacy Act (CCPA)

- Extends to healthcare organizations in California, requiring stringent data protection measures and providing consumers with rights over their personal information, including the right to know what data is being collected and how it is used.

New York SHIELD Act (Stop Hacks and Improve Electronic Data Security)

- Expands data breach notification requirements and mandates reasonable cybersecurity protections for private information held by organizations, including hospitals.

Texas Medical Records Privacy Act

- Enhances protections for medical records, requiring specific safeguards for the handling and storage of patient information and imposing penalties for non-compliance.

Massachusetts Data Privacy Law (201 CMR 17.00)

- Imposes strict requirements on the protection of personal information, including encryption of personal data stored on portable devices and robust cybersecurity measures.

Sources

1. American Hospital Association (AHA): Provides detailed annual reports on hospital types, bed counts, and financial performance.
2. Centers for Medicare & Medicaid Services (CMS): Offers data on healthcare spending and facility classifications.
3. National Healthcare Expenditures (NHE): Tracks and reports on the financial aspects of the U.S. healthcare system, including total revenue figures.
4. Marsh & McLennan Companies: As a leading insurance broker, they provide insights and reports on cybersecurity insurance trends in healthcare.
5. Advisen: Specializes in insurance data and analytics, often providing detailed reports on cybersecurity insurance costs by industry sector, including healthcare.
6. Beazley Breach Insights Report: Provides insights into the cost of breaches and how they affect insurance premiums.
7. National Association of Community Health Centers (NACHC): Provides data on community health centers, which are a subset of outpatient clinics.
8. U.S. Census Bureau: Occasionally releases data on healthcare facilities, including outpatient clinics.
9. Healthcare IT News: Discusses trends in the adoption of IoT devices in various healthcare settings, including outpatient clinics.
10. Frost & Sullivan Reports: Provide detailed market analysis and technology adoption trends in healthcare, including outpatient settings.
11. ECRI Institute: Publishes reports on the use and safety of medical devices in clinical settings.
12. Healthcare Cost and Utilization Project (HCUP): Offers statistical data on hospital characteristics, including the distribution of ORs and ER beds across different hospital sizes.
13. U.S. Department of Health & Human Services (HHS): Provides information on HIPAA and HITECH compliance.
14. Food and Drug Administration (FDA): Offers guidance on cybersecurity for medical devices.
15. Cybersecurity and Infrastructure Security Agency (CISA): Plays a role in managing cybersecurity risks for critical infrastructure, including healthcare.
16. State Government Websites: Provide details on state-specific regulations like CCPA, SHIELD Act, and others.
17. IBM Security and Ponemon Institute's "Cost of a Data Breach Report" (2023) indicates that the average cost of a healthcare data breach is nearly **$11 million**, up significantly from previous years. This report is one of the leading sources for understanding the financial impact of cyber incidents in healthcare.
18. Beazley Breach Insights Report also supports these figures, showing that healthcare breaches tend to be among the most expensive, given the sensitive nature of the data involved and the complexity of healthcare IT systems.
19. Becker's Hospital Review: Regularly publishes articles on significant cyber incidents affecting hospitals, including financial costs.
20. Healthcare Dive: Offers in-depth analysis of healthcare trends, including the costs and impacts of cyberattacks on hospital systems.