SAFEGUARDING PATIENT DATA: A COMPREHENSIVE APPROACH TO EPHI SECURITY IN HEALTHCARE IOT ECOSYSTEMS

INTRODUCTION

In an era where digital transformation is revolutionizing healthcare, the protection of patient data has become more critical than ever. Electronic Protected Health Information (ePHI) is at the heart of modern healthcare systems, powering everything from personalized treatment plans to large-scale medical research. However, with this digital evolution comes an increased risk of data breaches and unauthorized access to sensitive patient information.

The proliferation of Internet of Things (IoT) devices in healthcare settings has further complicated the landscape of data security. These devices, ranging from wearable health monitors to sophisticated in-hospital diagnostic equipment, generate vast amounts of ePHI. While they offer unprecedented insights into patient health and streamline care delivery, they also present new vulnerabilities that malicious actors can exploit.

The consequences of a healthcare data breach can be severe and far-reaching. Beyond the immediate financial implications—with the average cost of a healthcare data breach reaching $10.1 million in 2024 [1]—there are profound impacts on patient trust, organizational reputation, and regulatory compliance. Patients whose data is compromised may face risks ranging from identity theft to the exposure of sensitive medical conditions, potentially leading to personal and professional repercussions.

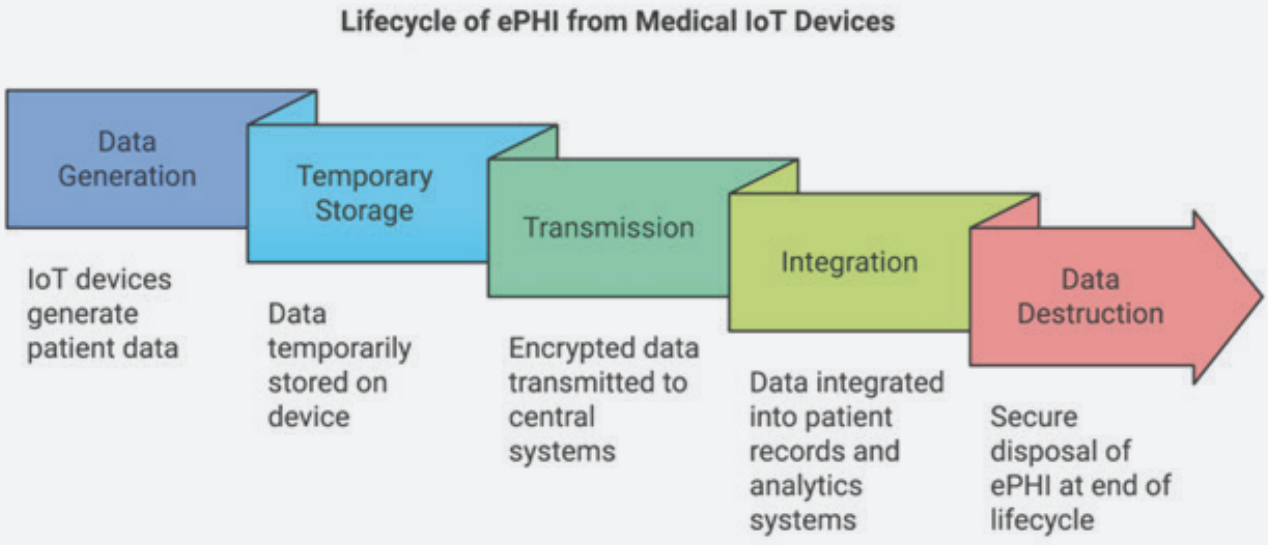
Healthcare organizations that fail to adequately protect ePHI risk violating the Health Insurance Portability and Accountability Act (HIPAA), which can result in significant fines, legal action, and mandatory corrective measures [2]. The reputational damage from such breaches can erode patient confidence, potentially leading to decreased patient retention and difficulty attracting new patients.

This white paper provides a comprehensive overview of the challenges and best practices in safeguarding ePHI, focusing on data generated by medical IoT devices. We will explore the lifecycle of ePHI from its creation to its integration into larger patient data ecosystems, examining the critical role of encryption—especially FIPS-validated cryptography—in maintaining data security. By understanding and implementing robust security measures, healthcare organizations can protect their patients' sensitive information, foster trust, ensure compliance, and pave the way for continued innovation in digital health.

As we take a deeper look into the intricacies of ePHI security, we will address key questions:

- What can medical IoT device manufacturers do to aid healthcare providers in effectively securing data at rest and in transit from their IoT devices?
- What are the best practices for IoT encryption key management?
- How do HIPAA requirements align with or differ from other industry standards and what does this mean for medical IoT devices?
- What are the specific challenges posed by IoT devices in healthcare, and how can they be addressed?
- How can organizations balance the need for data security with the imperative for data accessibility in healthcare settings?

THE LIFECYCLE OF EPHI FROM MEDICAL IOT DEVICES



Understanding the lifecycle of electronic Protected Health Information (ePHI) generated by medical Internet of Things (IoT) devices is crucial for implementing comprehensive security measures. This lifecycle typically consists of five main stages: data generation, temporary storage, transmission, integration into larger patient data ecosystems, and eventual data destruction.

DATA GENERATION AT THE DEVICE LEVEL

Medical IoT devices, ranging from wearable fitness trackers to implantable cardiac monitors, continuously generate patient health data. This data may include:

- Vital signs (heart rate, blood pressure, temperature)
- Activity levels and sleep patterns
- Blood glucose levels
- Medication adherence information
- Diagnostic imaging results

The type and volume of data generated depend on the specific device and its intended use. For example, a continuous glucose monitor might generate readings every five minutes, while a smart pill dispenser might only record data when medication is dispensed.

TEMPORARY STORAGE ON THE DEVICE

Once generated, data is typically stored temporarily on the device itself. This local storage serves several purposes:

1. Buffering data before transmission to conserve power and network resources
2. Ensuring data availability in case of network interruptions
3. Allowing for local processing or analysis before transmission

The duration and capacity of this temporary storage vary widely among devices. Some may store data for just a few minutes, while others might retain information for days or weeks.

It is crucial to note that security measures must be implemented immediately upon data generation and storage, even if temporary. Encryption and access controls should be applied at this early stage to protect the ePHI from unauthorized access or tampering, ensuring the data's confidentiality and integrity from the outset of its lifecycle.

TRANSMISSION TO CENTRAL STORAGE SYSTEMS

Data transmission from the IoT device to central storage systems is a critical phase in the ePHI lifecycle. This process often involves:

1. Establishing a secure connection (e.g., via Wi-Fi, Bluetooth, cellular networks)
2. Authenticating the device and the receiving system
3. Encrypting the data for transmission
4. Sending the data in batches or real-time, depending on the device capabilities and clinical requirements

The frequency and method of transmission can significantly impact both data security and the device's power consumption.

Additionally, data verification and validation is a crucial step in this process. It ensures that all data has been sent and successfully received without errors or corruption. This typically involves:

1. Implementing checksums, hash functions, or digital signatures to detect any changes in the data during transmission and verify its authenticity
2. Using acknowledgment protocols, such as those built into TLS (Transport Layer Security), where the receiving system confirms successful receipt of data
3. Employing error-checking and correction mechanisms to identify and rectify any transmission errors
4. Conducting periodic audits to compare transmitted data with the original source to ensure completeness and accuracy

These verification processes are essential for maintaining data integrity and ensuring that healthcare providers have access to complete and accurate patient information for clinical decision-making. The use of digital signatures, in particular, not only verifies the integrity of the transmitted data but also provides non-repudiation, ensuring that the data originated from the claimed source.

INTEGRATION INTO LARGER PATIENT DATA ECOSYSTEMS

This stage involves integrating the transmitted data into larger patient data ecosystems, such as:

- Electronic Health Record (EHR) systems
- Clinical decision support systems
- Population health management platforms
- Research databases

This integration process often involves:

1. Data validation and cleaning
2. Formatting and standardization
3. Correlation with other patient data
4. Application of access controls and audit trails

Once integrated, the ePHI becomes part of the patient's comprehensive health record, accessible to authorized healthcare providers and potentially used for broader analytics or research purposes.

DATA DESTRUCTION

The final stage in the ePHI lifecycle is the secure disposal of medical IoT data. Once a copy of the medical IoT data has been integrated into a larger ecosystem, the original data or buffer from the IoT device is deleted. The encryption key is typically destroyed, and the IoT data buffer is zeroized to prevent data access.

Throughout this lifecycle, ePHI faces various security risks. Data could be intercepted during transmission, accessed by unauthorized parties on the device or in central storage, or compromised during the integration process. Therefore, robust security measures must be implemented at each stage to ensure the confidentiality, integrity, and availability of this sensitive information.

SECURE ARCHITECTURE FOR EPHI MANAGEMENT

Implementing a robust and secure architecture for ePHI management by medical IoT device manufacturers is crucial for healthcare organizations to utilize when protecting patient data, ensuring regulatory compliance, and maintaining trust. This section outlines key components of such an architecture, with a focus on encryption and key management practices for encryption technologies.

ENCRYPTION AT REST USING FIPS-VALIDATED CRYPTOGRAPHY

Encryption at rest is a critical security measure that protects ePHI when it is stored on devices, servers, or databases.

Importance of AES-256 Encryption

The Advanced Encryption Standard (AES) with 256-bit key length is widely recognized as a secure encryption algorithm for protecting sensitive data. AES-256 offers several advantages:

- Strong security: With a 256-bit key length, AES-256 is considered computationally infeasible to break using current technology.
- Performance: AES-256 provides a good balance between security and encryption/decryption speed.
- Wide adoption: It is supported by most modern systems and devices.
- Future-proofing: While NIST states AES-128 will likely remain secure for years to come, AES-256 is far more resistant to the evolution of Post Quantum Cryptography (PQC) and will remain secure for a very long time [3].

Benefits of FIPS Validation

The Federal Information Processing Standard (FIPS) 140-2 (and its successor FIPS 140-3) provides a benchmark for cryptographic modules used within security systems protecting sensitive information [4]:

- Assurance of security: FIPS validation ensures that cryptographic modules have been tested against stringent security requirements.
- Regulatory compliance: Many regulations—including HIPAA—recommend or require FIPS-validated cryptography.
- Interoperability: FIPS-validated modules often have better interoperability due to standardized implementations.

Key Management Practices for Encryption

Effective key management is crucial for maintaining encrypted ePHI's security:

1. Secure Key Generation and Storage
   - Use cryptographically secure random number generators for key creation.
   - Store keys separately from encrypted data—preferably within hardware security modules (HSMs, TPMs, or other silicon components).
2. Key Rotation and Lifecycle Management
   - Implement regular key rotation schedules.
   - Establish clear processes for key creation, activation, deactivation, and destruction.
3. Access Controls & Separation of Duties
   - Implement strong access controls around key management systems.
   - Enforce separation of duties ensuring no single individual has complete control over key lifecycle processes.
4. Backup & Recovery Procedures for Keys
   - Maintain secure backups of encryption keys.
   - Implement robust recovery processes for emergencies or authorized access requests.

NIST provides a number of recommendations that are extremely useful for guidance in managing certificates and keying material for asymmetric and symmetric cryptography [5][6].

SECURE TRANSMISSION METHODS

Securing ePHI during transmission is as critical as protecting it at rest:

1. Encrypted Data Transmission vs TLS
    - Encrypted Data Transmission: Encrypting before transmission adds an additional layer. This is often referred to as defense in depth and is highly recommended.
    - TLS: Use TLS protocols securing communication channels themselves.
2. Pre-encryption Before Transmission
    - End-to-end security: Data remains encrypted even if TLS channels are compromised.
    - Reduced reliance on network security: Provides protection even on insecure networks.
    - Compliance: Meets regulatory requirements regarding ePHI protection during transmission regardless of TLS implementation.
    - Key management is a critical component of the overall ePHI data security architecture.
3. Meeting FIPS Compliance Requirements
    - The best case scenario would be to employ FIPS-validated cryptography throughout an IoT design; if this is not possible, it's recommended that Pre-encryption Before Transmission (see above) be performed with a FIPS-validated module to ensure end-to-end security.
    - Even if connectivity elements can not meet FIPS compliance, critical ePHI encryption protection adheres to FIPS guidelines.

By implementing these measures on the medical IoT device—strong encryption at rest, robust key management practices, and secure transmission methods—healthcare organizations can significantly enhance the protection of ePHI throughout its lifecycle while maintaining compliance with regulatory requirements.

COMPLIANCE WITH HIPAA AND OTHER REGULATIONS

Ensuring compliance with regulatory requirements is crucial for healthcare organizations handling ePHI. When manufacturers incorporate security measures into IoT devices, the security measures discussed in previous sections play a vital role in helping healthcare delivery organizations (HDOs) meet their ePHI protection requirements. These built-in security features, such as encryption capabilities, secure boot processes, and robust authentication mechanisms, provide HDOs with a solid foundation for HIPAA compliance, reducing the burden of implementing additional security measures alongside medical IoT devices to minimize potential vulnerabilities. This section focuses on how these security measures align with HIPAA requirements and other relevant standards and how they support HDOs in their compliance efforts.

HIPAA REQUIREMENTS FOR EPHI PROTECTION

The Health Insurance Portability Accountability Act (HIPAA) sets standards protecting sensitive patient information within United States' healthcare systems [7]:

Secured Rule:

- Administrative Safeguards: Policies/procedures ensuring proper management of electronic PHI.
- Physical Safeguards: Controls protecting electronic systems/equipment/data.
- Technical Safeguards: Technology/policies protecting PHI controlling access.

Encryption/Decryption:

- While HIPAA doesn't mandate specific methods, it requires "implementing a mechanism to encrypt/decrypt electronic protected health information" (45 CFR § 164312(a)(2)(iv)).
- Using FIPS-validated cryptography meets this requirement effectively [7].

Access Controls:

- HIPAA mandates implementation technical policies/procedures allowing access only authorized persons/software programs maintaining electronic information containing PHI.

Audit Controls:

- Mechanisms recording/examining activity within information systems containing/using PHI ensuring accountability/audit trail exists whenever necessary.

Integrity Controls:

- Policies/procedures ensuring PHI isn't improperly altered/destroyed.

Transmission Security

- Technical security measures to guard against unauthorized access to ePHI being transmitted over an electronic communications network.

OTHER RELEVANT STANDARDS AND GUIDELINES

While HIPAA is the primary regulation for healthcare data in the U.S., other standards and guidelines also influence ePHI security practices:

NIST Guidelines

- NIST Special Publication 800-66: Provides guidance on implementing the HIPAA Security Rule [8].
- NIST Cybersecurity Framework: Offers a comprehensive approach to managing cybersecurity risk [9].

FDA Guidance on Medical Device Cybersecurity

- Provides recommendations for managing cybersecurity in medical devices, including those that generate and transmit ePHI [10].

General Data Protection Regulation (GDPR)

- While primarily applicable in the EU, GDPR can affect U.S. healthcare organizations handling data of EU residents.
- Emphasizes data protection by design and by default, which aligns with many HIPAA principles.

HITRUST CSF (Common Security Framework)

- Provides a comprehensive approach to regulatory compliance and risk management, incorporating HIPAA and other standards [11].

PCI DSS (Payment Card Industry Data Security Standard)

- Relevant for healthcare organizations that process credit card payments, often alongside ePHI.

Aligning security practices with these regulations and standards not only ensures compliance but also provides a comprehensive framework for protecting ePHI. The encryption, key management, and secure transmission methods discussed in previous sections directly support compliance with these requirements.

By implementing robust security measures that meet or exceed these regulatory standards, healthcare organizations can protect patient data, avoid penalties, and maintain trust in their handling of sensitive information.

BEST PRACTICES FOR IMPLEMENTATION

Implementing robust security measures for ePHI protection requires a comprehensive approach that goes beyond just technology. This section outlines best practices for medical device manufacturers to effectively implement and maintain a secure ePHI ecosystem, highlighting how these practices benefit healthcare delivery organizations (HDOs).

RISK ASSESSMENT AND MANAGEMENT FOR DEVICE MANUFACTURERS

1. Conduct Comprehensive Risk Assessments
    - Identify potential threats and vulnerabilities in device design and functionality.
    - Evaluate the effectiveness of existing security controls in the device.
    - Prioritize risks based on likelihood and potential impact on HDOs.
2. Develop a Risk Management Plan
    - Create strategies to mitigate identified risks in device design and operation.
    - Establish clear timelines for security updates and patches.
    - Regularly review and update the plan to address evolving threats, benefiting HDOs with up-to-date security measures.
3. Implement Security by Design
    - Integrate security features into IoT devices from the initial design phase.
    - Provide HDOs with devices that have built-in security features, reducing their implementation burden.

All of the above components should be available to HDOs for review for them to easily facilitate securing medical IoT device data.

DOCUMENTATION AND TRAINING SUPPORT

1. Comprehensive Security Documentation
   - Provide detailed documentation on device security features and best practices for HDOs.
   - Include clear instructions for secure device configuration and maintenance.
2. Training Resources for HDOs
   - Develop training materials on device security features and proper usage.
   - Offer ongoing support and education to HDO staff on security best practices.
3. Transparent Communication
   - Maintain open channels for security-related communications with HDOs.
   - Promptly notify HDOs of potential vulnerabilities and provide mitigation strategies.

The body of resources above should be maintained for the complete lifecycle of the deployed and active product.

REGULAR UPDATES AND SUPPORT

1. Proactive Security Patching
   - Develop and maintain a robust patch management process for all devices.
   - Provide easy-to-implement security updates to HDOs, ensuring their devices remain protected against new threats.
2. Ongoing Security Monitoring
   - Implement systems to monitor for new vulnerabilities affecting manufactured devices.
   - Alert HDOs to potential security issues and provide guidance on mitigation.
3. End-of-Life Planning
   - Clearly communicate device lifecycle and support timelines to HDOs.
   - Provide guidance on secure decommissioning of devices at end-of-life.

SECURE DESIGN AND CONFIGURATION

1. Secure Default Configurations
   - Design devices with secure default settings, reducing the configuration burden on HDOs.
   - Implement strong, unique default passwords or require password changes on first use.
2. Encryption Implementation
   - Integrate FIPS-validated encryption for data at rest and in transit.
   - Provide HDOs with devices that offer robust, built-in data protection.
3. Access Control Features
   - Design devices with strong authentication mechanisms, including support for multi-factor authentication where possible.
   - Allow for easy integration with HDOs' existing access management systems.
4. Data Minimization by Design
   - Design devices to collect and store only the minimum amount of ePHI necessary for their function.
   - Provide HDOs with granular control over data collection and storage settings.

By following these best practices, medical device manufacturers can create a robust security environment for ePHI, significantly benefiting HDOs. These practices not only help in protecting sensitive patient data but also in maintaining compliance with regulatory requirements, reducing the security burden on HDOs, and building trust with healthcare providers and patients.

FUTURE CONSIDERATIONS

As technology continues to evolve rapidly, the landscape of ePHI security in healthcare IoT is constantly changing. This section explores emerging threats, technological advancements, and future trends that device manufacturers and healthcare delivery organizations (HDOs) should consider in their long-term security strategies.

EMERGING THREATS IN HEALTHCARE CYBERSECURITY

Quantum Computing Challenges

- The potential for quantum computers to break current encryption standards poses a significant threat to healthcare data security.
- Quantum computers could potentially crack widely used encryption algorithms like RSA and ECC in a matter of hours or minutes.
- Healthcare organizations must prepare for the "harvest now, decrypt later" threat, where attackers collect encrypted data now to decrypt it when quantum computers become available.
- Device manufacturers need to consider implementing quantum-resistant cryptographic algorithms in future medical device designs to ensure long-term data protection.

AI-Powered Attacks

- The rise of sophisticated, AI-driven cyber attacks targeting healthcare systems is becoming increasingly prevalent.
- AI-assisted phishing attacks can create highly personalized and convincing emails, making it harder for healthcare staff to distinguish between legitimate and malicious communications.
- Machine learning algorithms are being used to automate and scale attacks, allowing cybercriminals to launch more frequent and complex assaults on healthcare networks.
- AI-powered malware can adapt to evade detection, learn from failed attempts, and exploit vulnerabilities more effectively than traditional malware.
- The healthcare industry must develop AI-enhanced defense mechanisms in medical devices and network systems to counter these evolving threats.

Increased Attack Surface with 5G and Beyond

- The proliferation of 5G-enabled medical devices is expanding the attack surface for cybercriminals.
- 5G networks enable a massive increase in connected devices, potentially leading to more entry points for attackers.
- The high bandwidth and low latency of 5G can facilitate more sophisticated and rapid attacks, allowing for faster data exfiltration.
- Healthcare IoT devices leveraging 5G may have reduced power consumption, potentially leading to weaker security measures to conserve battery life.
- Securing high-bandwidth, low-latency communications in healthcare IoT requires new strategies, including edge computing security and AI-driven real-time threat detection.

ADVANCEMENTS IN ENCRYPTION TECHNOLOGIES

Post-Quantum Cryptography (PQC)

- As quantum computing advances, traditional encryption methods may become vulnerable. Post-quantum cryptography aims to develop cryptographic algorithms that can withstand attacks from quantum computers [12].
- Ongoing research by organizations like NIST is focused on standardizing PQC algorithms that can be integrated into existing systems and devices.
- Device manufacturers should begin planning for the integration of PQC into future medical devices to ensure long-term data security and compliance with evolving standards.

Homomorphic Encryption

- Homomorphic encryption allows computations to be performed on encrypted data without decrypting it, enabling secure data analysis while preserving privacy.
- This technology could revolutionize how sensitive health data is processed, allowing healthcare providers to analyze patient data without exposing it to potential breaches.
- While still in its infancy, advancements in homomorphic encryption could lead to new applications in secure cloud computing and collaborative research, where multiple parties can analyze shared data without compromising individual privacy.

Blockchain in Healthcare

- Blockchain technology offers a decentralized and tamper-proof method for storing health records and managing device identities.
- By using blockchain, healthcare organizations can enhance data integrity, as each transaction is recorded in a way that cannot be altered without consensus from the network.
- Potential applications include secure patient consent management, tracking the provenance of medical devices, and ensuring the authenticity of clinical trial data.
- However, challenges remain in terms of scalability, interoperability with existing systems, and regulatory acceptance.

EVOLVING REGULATORY LANDSCAPE

Anticipated Changes in HIPAA and Other Regulations

- As technology evolves, so too must regulations like HIPAA. Future updates may address new threats posed by emerging technologies such as AI and quantum computing.
- Regulatory bodies may introduce stricter guidelines for data protection, requiring organizations to adopt advanced security measures proactively.
- Healthcare organizations must stay informed about potential regulatory changes to ensure compliance and avoid penalties.

Standardization Efforts

- The development of new standards for IoT security in healthcare is essential for establishing best practices across the industry.
- Collaborative efforts among industry stakeholders—including manufacturers, healthcare providers, and regulatory bodies—can lead to robust frameworks that enhance security.
- Standardization can facilitate interoperability between devices from different manufacturers while ensuring a baseline level of security.

EMERGING TECHNOLOGIES AND THEIR IMPACT

Edge Computing in Healthcare

- Edge computing allows data processing to occur closer to the source (e.g., medical devices), reducing latency and bandwidth usage while enhancing real-time decision-making capabilities.
- However, this shift also introduces new security challenges as more devices become interconnected at the edge of networks.
- Ensuring the security of edge devices requires robust authentication mechanisms and continuous monitoring for potential vulnerabilities.

Biometric Authentication Advancements

- The integration of advanced biometric authentication methods—such as facial recognition or fingerprint scanning—into medical devices can enhance security while improving user convenience.

- However, these technologies must be implemented carefully to protect user privacy and comply with regulations regarding biometric data handling.
- Manufacturers need to consider the ethical implications of biometric data collection and ensure that robust safeguards are in place.

Autonomous and AI-Driven Devices

- As medical devices become increasingly autonomous—utilizing AI for decision-making—the need for stringent security measures becomes paramount.
- Ensuring the integrity of AI algorithms is crucial; any manipulation or compromise could lead to incorrect diagnoses or treatment recommendations.
- Manufacturers should implement rigorous testing protocols and continuous monitoring systems to detect anomalies in device behavior.

PREPARING FOR THE FUTURE

Fostering Innovation in Security

- Encouraging research and development in healthcare cybersecurity is essential for staying ahead of emerging threats.
- Collaboration between device manufacturers, HDOs, academia, and cybersecurity experts can lead to innovative solutions tailored specifically for healthcare environments.

Adaptive Security Architectures

- Designing flexible security architectures that can adapt to new threats will be critical as technology continues to evolve rapidly.
- Implementing modular security frameworks allows organizations to update specific components without overhauling entire systems.

Workforce Development

- Addressing the cybersecurity skills gap in healthcare is crucial for maintaining robust security practices.
- Ongoing education and training programs should be established to equip staff with the necessary skills to manage emerging technologies effectively.
- Partnerships with educational institutions can help create a pipeline of skilled professionals ready to tackle cybersecurity challenges in healthcare.

By understanding and preparing for these emerging threats, medical device manufacturers and healthcare organizations can better position themselves to protect sensitive patient data and maintain the integrity of healthcare systems in an increasingly complex technological landscape.

CONCLUSION

As healthcare embraces digital transformation, protecting electronic Protected Health Information (ePHI) remains a paramount concern. Integrating Internet of Things (IoT) devices offers significant benefits but also introduces complex security challenges that must be addressed.

To safeguard sensitive patient data, manufacturers and healthcare delivery organizations (HDOs) must prioritize robust security measures, including encryption, compliance with regulations like HIPAA, and proactive risk management. Embracing emerging technologies and fostering stakeholder collaboration will be essential in navigating the evolving threat landscape.

REFERENCES

1. Olsen, E. (2024, August 1). *Average cost of healthcare data breach nearly $10M in 2024: Report.* Healthcare Dive. https://www.healthcaredive.com/news/healthcare-data-breach-costs-2024-ibm-ponemon-institute/722958/
2. (OCR), O. for C. R. (2021, June 28). *HIPAA compliance and Enforcement*. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html
3. Computer Security Division, I. T. L. (n.d.). *Post-quantum cryptography: CSRC. CSRC*. https://csrc.nist.gov/projects/post-quantum-cryptography/faqs
4. Computer Security Division, I. T. L. (n.d.-a). *Cryptographic module validation program: CSRC. CSRC.* https://csrc.nist.gov/projects/cryptographic-module-validation-program
5. Barker, E. (2020, May 4). *Recommendation for key management: Part 1 – general.* CSRC. https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final
6. Barker, E., & Barker, W. (2018, July 2). *Recommendation for key establishment using symmetric block ciphers.* CSRC. https://csrc.nist.gov/pubs/sp/800/71/ipd
7. (OCR), O. for C. R. (2021a, June 28). *Breach notification guidance.* HHS.gov. https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html
8. Marron, J. (2024, February 14). *Implementing the health insurance portability and accountability act (HIPAA) security rule: A cybersecurity resource guide.* CSRC. https://csrc.nist.gov/pubs/sp/800/66/r2/final
9. The NIST Cybersecurity Framework (CSF) 2.0. (n.d.). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
10. Center for Devices and Radiological Health. (n.d.). *Cybersecurity in medical devices frequently asked questions (faqs).* U.S. Food and Drug Administration. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs
11. *Get more familiar with the HITRUST framework (HITRUST CSF®).* Hitrust. (n.d.). https://hitrustalliance.net/hitrust-framework
12. National Institute of Standards and Technology (NIST). (n.d.). Post-Quantum Cryptography FAQs. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography/faqs