IJBPAS, November, 2025, 14(11): 6064-6074

ISSN: 2277–4998

International Journal of Biology, Pharmacy and Allied Sciences (IJBPAS)

'A Bridge Between Laboratory and Reader'

www.ijbpas.com

REGULATORY INSIGHTS INTO CYBERSECURITY FOR MEDICAL DEVICES IN US

SAHANA S T*, HARSHITHA M, ABHISHEK B V, AMAR S, PUNEETH N

Dept. of Pharmaceutics & Regulatory Affairs, Sri Adichunchanagiri College of Pharmacy, ACU, B.G Nagara, Karnataka,571448-India.

***Corresponding Author: Ms. Sahana S T: E Mail: sahana9148@gmail.com**

Received 18th July 2024; Revised 25th Sept. 2024; Accepted 5th Nov. 2024; Available online 1st Nov. 2025

https://doi.org/10.31032/IJBPAS/2025/14.11.9581

ABSTRACT

In the evolving landscape of medical device cybersecurity, ensuring patient safety during technological advancements is paramount. The FDA and other regulatory bodies play pivotal roles in setting guidelines and standards to mitigate risks associated with interconnected medical devices. Through frameworks like ISO, IEC, and HIPAA, manufacturers are mandated to integrate robust cybersecurity measures throughout the device lifecycle, from design and production to post-market surveillance. Recent updates require manufacturers to adopt a proactive approach, conducting thorough risk assessments and implementing advanced security features such as encryption and AI-driven threat detection. Collaboration among stakeholders-manufacturers, healthcare providers, and cybersecurity experts—is emphasized to fortify device resilience against emerging threats like phishing and ransomware. Continuous updates and adherence to best practices ensure that medical devices remain secure and reliable in the face of modern cybersecurity challenges. It provides a comprehensive understanding of the regulatory landscape, recent updates, and common challenges medical device manufacturers face in achieving cybersecurity compliance.

Keywords: Cybersecurity, Medical devices, FDA, ISO, IEC, Cybersecurity updates

INTRODUCTION:

Medical devices are becoming more interoperable and networked in order to improve patient care. While there are many advantages to interconnectivity and

interoperability, there are also significant cybersecurity threats associated with linked equipment. Device performance as well as the availability and integrity of the device and its data may be impacted by cybersecurity flaws in devices, whether they are actively exploited or unintentionally caused. To guarantee the efficacy and safety of medical devices, strong cybersecurity safeguards are now more crucial than ever **[1]**.

Cybersecurity in medical devices is the **process of stopping unauthorized usage**, access, modification, denial of service, or use of data that is stored, accessed, or sent from a medical device to a third party without authorization **[2]**.

Making sure that patients and healthcare professionals have access to safe and efficient medical devices is the responsibility of the Food and Drug Administration's (FDA) Centre for Devices and Radiological Health (CDRH). To better frame cybersecurity concerns and establish a standard terminology for all critical infrastructure sectors, Executive Order 1363614 instructed the National Institute of Standards and Technology (NIST) to develop a Cybersecurity Framework. The premarket advisory from the FDA lists cybersecurity concerns that medical device manufacturers need to take into account while designing and developing their products. The guidelines stress the importance of evaluating both intentional and inadvertent cybersecurity risks and including specialized controls that address cybersecurity into product design **[3]**.

The portion of legal specifications for device quality and safety, such as those set forth by the **International Organization for Standards (ISO), International Electrotechnical Commission (IEC), Protected healthcare information (PHI)** was established by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Medical Device cybersecurity would have to be improved by manufacturers for the USFDA and HIPAA to be connected through new regulations **[4]**. Every medical device should have its safety and security risks evaluated in relation to the broader system in which it functions, in order to adequately account for cybersecurity threats in medical device systems. Since cybersecurity threats and risks are constantly changing, security risk management procedures are essential in the context of cybersecurity. A manufacturer's whole quality system should include security risk management, which should be handled throughout the TPLC. Design controls (21 CFR 820.30), production process validation (21 CFR 820.70), and corrective and preventive actions (21 CFR 820.100) are among the QS regulation procedures that might be pertinent in this situation. These procedures are meant to

guarantee that safety and security risks are sufficiently addressed. To ensure a more thorough identification and management of patient safety hazards, the FDA advises device manufacturers to conduct both a safety risk assessment and a separate, accompanying security risk assessment as part of their risk analyses under 21 CFR 820.30 **[2]**.

The **FDA's cybersecurity rules** for medical devices stipulate that:

• Design control documentation must be provided. in particular, documentation about risk assessments, software validation, and design validation.

• Verify that no incoming data is altered while it is in transit or at rest. Moreover, it complies with the requirements.

• Apply best practices recognized by the industry. During the code's execution by the device, these uphold and confirm its integrity.

• Create a medical gadget that can recognize and react to cybersecurity threats. Patches and updates for cybersecurity are part of this. Workarounds for emergencies are also included.

• Put in place features on medical devices that safeguard important data and functionality. even if there is a cybersecurity breach on the device **[5]**.

Objectives:

To Clarify Regulatory Landscape - Provide a clear understanding of the current regulatory frameworks governing cybersecurity in medical devices, including key guidelines and standards.

To Address Regulatory Updates - Discuss recent updates in regulatory requirements related to cybersecurity in medical devices and their potential implications for manufacturers.

To Identify Common Challenges - Identify common challenges faced by medical device manufacturers in achieving regulatory compliance related to cybersecurity.

RESULTS AND DISCUSSION:

Regulatory Landscape

The first cybersecurity guidelines for networked medical devices with off-the-shelf software were released in 2005 by the US federal agency Food and Drug Administration (FDA). The FDA (2005) guidelines suggest creating a cybersecurity maintenance strategy and evaluating software modifications made to address cybersecurity vulnerabilities. The FDA released a draft guidance document in June 2013 that discusses cybersecurity management for medical devices at the premarket stage. In October 2014, the FDA published the final guidance. The process of preventing unauthorized access, modification, misuse, denial of use, or the unauthorized use of information that is stored, accessed, or sent from a medical device to an external receiver is what the FDA (2014) describes as cybersecurity in

this final advice. The FDA revised the premarket advice in October 2018. There are also some post-market recommendations in this draft guidance (FDA, 2018). A second set of guidelines, addressing cybersecurity management in medical devices during the post-market phase, was released by the FDA in December 2016 **[6]**.

Table 1: Guidance documents for FDA

Sl No	Guidance Documents	Issued dates	URL
1.	Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software	January 14, 2005	https://www.fda.gov/media/72154/download[7]
2.	Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act	March 13, 2024.	https://www.fda.gov/media/176944/download[8]
3.	Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions	September 27, 2023	https://www.fda.gov/media/119933/download[9]
4.	Post-market Management of Cybersecurity in Medical Devices	December 28, 2016	https://www.fda.gov/media/95862/download[10]

The ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) guidelines for cybersecurity in medical devices are critical frameworks that ensure the safety, security, and reliability of medical technologies. These guidelines, particularly ISO/IEC 80001 and IEC 62443, provide comprehensive standards for managing cybersecurity risks throughout the lifecycle of medical devices. They address various aspects, including risk management, secure software development, and maintenance processes, to protect patient data and ensure the continuous, safe operation of medical devices in healthcare environments. By adhering to these standards, manufacturers and healthcare providers can mitigate vulnerabilities, safeguard against cyber threats, and maintain the integrity and confidentiality of sensitive health information **[6]**.

Some of the important standards concerning cybersecurity are,

Table 2: Major ISO/IEC Standards [11]

IEC 62304	Medical Device software, software life cycle processes
IEC 80001	Application of risk management for IT networks incorporating medical devices
ISO 14971	Application of risk management for medical devices
ISO 60601	Medical electrical equipment, general requirements for basic safety, and essential performance standards
IEC 62366	Medical devices, application of usability engineering for medical devices
ISO 11633	Health informatics, information security management for remote maintenance of medical devices, and medical information systems
ISO 27032	Information technology, security techniques, guidelines for cybersecurity
ISO 29134	Information technology, security techniques, guidelines for privacy impact assessment
ISO 27799	Health informatics information security management in health using ISO/IEC 27002
ISO 10993	Biological evaluation of medical device standards
ISO 81001	Health software and health IT system safety, effectiveness, and security
ISO 13485	Medical device, Quality management system, requirements for regulatory purposes
IEC 82304	Health software, health and wellness apps
ISO 22696	Health informatics Guidance on identification and authentication of connectable Personal Healthcare Devices (PHDs)
ISO 30111	Information technology, security techniques vulnerability handling processes

Some of the important organizations governing cybersecurity concerns are,

Table 3: Organizations governing cybersecurity concerns [11]

Organization	Recommendations
FDA	• Medical device cybersecurity guidance • Pre- and post-market management of cybersecurity in medical devices • FDA cybersecurity safety communications • Workshop and webinars on cybersecurity: Cybersecurity in medical devices
GAO	• Recommendations to FDA regarding medical device information security
HIMSS	• Manufacturer disclosure statement for medical device security
DHS	• ICS-CERT Alert (Medical Devices)
HITRUST	• Practical cybersecurity for medical devices
HIPPA	• Health Insurance Portability and Accountability Act

Regulatory Updates

Recent updates in cybersecurity for medical devices in the USA highlight significant strides in safeguarding patient data and device integrity against escalating cyber threats. Manufacturers are now expected to provide a Cybersecurity Bill of Materials (CBOM) to enhance transparency and vulnerability management. Advancements in encryption, multi-factor authentication,

and real-time threat detection, driven by AI and machine learning, are becoming standard. Activities related to threat modeling are examined during design reviews. The FDA suggests that threat modeling documentation contain enough details about the manufacturer's threat modeling efforts to evaluate and assess the security features integrated into the device so that the device and the system it operates in are assessed holistically for the device's efficacy and safety. The flaws are found in the Known Exploited Flaws Catalog of the Cybersecurity and Infrastructure Security Agency (CISA). Devices ought to be made with "cyber-resiliency," or the ability to withstand potential cyber event situations while maintaining availability. Medical devices should have cyber-resiliency capabilities because they offer a safety net against potential future vulnerabilities **[2]**.

The current threats explored in the Harmonised Indices of Consumer Prices (HICP) document are as follows,

1. Email Phishing: Email phishing is an attempt to deceive a person into divulging personal information via email.
2. Ransomware: Ransomware is a kind of malware (malicious software) that differs from other malware in that it aims to prevent a user's data from being accessed until a ransom is paid.
3. Theft of Data: Sensitive data may be accessed, disseminated, and used illegally or uninvitedly if the lost device is not properly secured or password protected.
4. Accidental or Intentional Data Loss: Any organization that allows workers, contractors, or other users to access its records, network, or technological infrastructure is susceptible to Accidental or Intentional attacks.
5. Attacks Against Connected Medical Devices: Attacks against connected medical devices pose significant risks to patient safety, privacy, and healthcare operations, as these devices are increasingly targeted by cybercriminals seeking to exploit vulnerabilities for malicious purposes **[12]**.

Recent updates for cybersecurity in Medical Devices are,

Table 4: Recent Updates for Cybersecurity in Medical Devices [13]

Recent Updates	URL
Next Steps Toward Managing Legacy Medical Device Cybersecurity Risks	https://www.mitre.org/sites/default/files/2023-11/PR-23-3695-Managing-Legacy-Medical-Device%20Cybersecurity-Risks.pdf
Medical Device Cybersecurity Regional Preparedness and Response Playbook	https://www.mitre.org/sites/default/files/2022-11/pr-2022-3034-medical-device-cybersecurity-regional-preparedness-response-playbook.pdf
Medical Device Cybersecurity Regional Preparedness and Response Playbook Quick Start - Companion Guide	https://www.mitre.org/sites/default/files/2022-11/pr-2022-3616-medical-device-cybersecurity-regional-preparedness-response-companion-guide.pdf
Playbook for Threat Modeling Medical Devices	https://www.mitre.org/sites/default/files/2021-11/Playbook-for-Threat-Modeling-Medical-Devices.pdf
The FDA's Role in Medical Device Cybersecurity-Dispelling Myths and Understanding Facts	https://www.fda.gov/media/123052/download?attachment

The continuous cybersecurity updates are crucial for safeguarding connected medical devices against evolving threats. As the landscape of cyber threats continues to advance, staying proactive with cybersecurity measures is essential for maintaining trust and security in medical technology **[13]**.

Common Cybersecurity Challenges

1. **Legacy Systems:** Many medical devices run on outdated software or operating systems for which there is no longer vendor support. They become vulnerable to security flaws that could be used by hostile actors as a result.
2. **Device Complexity:** The complexity of contemporary medical devices, which are frequently furnished with a plethora of settings and options, makes it difficult to manage vulnerabilities and maintain proper security settings.
3. **Insecure Medical Devices and Equipment:** Healthcare organizations are dependent on an increasing number of networked devices due to the advent of the Internet of Medical Things. IoMT systems, like other Internet of Things (IoT) gadgets, frequently have inadequate security, which opens fresh vulnerabilities that a hacker can take advantage of to access the company's systems and patient information.
4. **Interconnectivity and Integration:** Health IT systems are becoming more and more integrated with medical devices. Because of their

interconnectedness, they are vulnerable to network-based attacks, which could result in data breaches or unauthorized access to private patient information.

5. **Insufficient Security Measures:** Security was not always considered when many medical equipment's were first designed. They are vulnerable to cyberattacks because they lack strong security measures like encryption and safe communication protocols.
6. **Regulatory Compliance:** It can be difficult to ensure compliance with a constantly changing set of legislation in several countries. Furthermore, when it comes to revising policies, regulatory organizations frequently lag technical changes.
7. **Supply Chain Risks:** Medical device supply chains can be complex, involving numerous vendors and other partners. It is difficult to make sure that every link in the supply chain follows security best practices **[14]**.
8. **Insider Threats:** The frenetic pace of healthcare environments often leads to lax security practices by staff members. Insiders, whether inadvertently or through malicious intent, can expose devices to additional risks.
9. **Third-Party Risks:** Reliance on outside suppliers and software may result in vulnerabilities that are not under the direct control of medical professionals or device makers.
10. **Ransomware and Malware:** Healthcare institutions are frequently targets of ransomware attacks because of the importance of their data and the likelihood that they will have to pay to get back up and continue treating patients.
11. **Distributed Denial of Service (DDoS):** The goal of a DDoS assault is to overload systems or applications with more traffic than they can manage to prevent access. DDoS assaults are being used by cybercriminals more frequently as a component of ransom attempts; occasionally, they are combined with malware or data theft **[6, 15]**.

CONCLUSION:

The cybersecurity of medical devices has become a critical focus due to the increasing interconnectivity and reliance on technology within the healthcare sector. Regulatory bodies such as the FDA and standards organizations like ISO and IEC have developed comprehensive frameworks to guide manufacturers in integrating robust cybersecurity measures throughout the

device lifecycle. These measures include the implementation of advanced technologies such as encryption, multi-factor authentication, and AI-driven threat detection to mitigate risks effectively.

One of the key strategies highlighted is the Cybersecurity Bill of Materials (CBOM), which enhances transparency and facilitates vulnerability management. Despite significant advancements, challenges persist, particularly with legacy systems, device complexity, and ensuring compliance with dynamic regulations. Collaboration between device manufacturers, healthcare providers, and cybersecurity experts is essential to build a resilient cybersecurity framework. Regular updates, patches, and real-time monitoring are crucial to adapt to evolving threats. The future of medical device cybersecurity will depend on sustained innovation, adherence to regulatory standards, and a collective commitment to safeguarding patient data and device functionality. By embracing these principles, the healthcare industry can ensure the safe and effective use of medical devices, ultimately enhancing patient care and trust in medical technologies.

ACKNOWLEDGMENT:

The author wants to acknowledge the management of Sri Adichunchanagiri College of Pharmacy for their valuable support.

CONFLICT OF INTEREST:

The authors declared that there is no conflict of interest.

REFERENCES:

[1] Craigen D, Diakun-Thibault N, Purse R. Defining Cybersecurity. Technology Innovation Management Review 2014; 4:13–21. https://doi.org/10.22215/timreview/835.

[2] Contains Nonbinding Recommendations Draft -Not for Implementation Content of Premarket Submissions for [Internet]. Available from: https://www.fda.gov/media/119933/download

[3] Schwartz S, Ross A, Carmody S, Chase P, Coley SC, Connolly J, *et al*. The Evolving State of Medical Device Cybersecurity. Biomedical Instrumentation & Technology. 2018 Mar 1;52(2):103–11.

[4] Cybersecurity For Healthcare Medical Devices - ProQuest [Internet]. www.proquest.com. [cited 2024 Jun 13]. https://www.proquest.com/openview/7934d6bce5e1df3dd3bbb8d856bdfd24/1?cbl=18750&parentSessionId=V2aeg55wWU48AQMRTyR2PlYOUhttvnDlJ8G%2FUalvr18%3D&pq-origsite=gscholar&parentSessionId=EueNkfvryhYlptSTXJR8x3oCewU6wGPGo9XTrBKRCh8%3D

[5] Medical Device Cybersecurity Trends | Perforce [Internet]. www.perforce.com. https://www.perforce.com/blog/sca/cybersecurity-trends-medical-devices

[6] Williams P, Woodward A. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical Devices: Evidence and Research [Internet]. 2015 Jul; 8:305. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/

[7] Health C for D and R. Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software [Internet]. U.S. Food and Drug Administration. 2020. Available from: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-networked-medical-devices-containing-shelf-ots-software

[8] Webinar - Draft Guidance: Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act - 04/30/2024 [Internet]. FDA. 2024. Available from: https://www.fda.gov/medical-devices/medical-devices-news-and-events/webinar-draft-guidance-select-updates-premarket-cybersecurity-guidance-section-524b-fdc-act-04302024

[9] Health C for D and R. Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act [Internet]. www.fda.gov. 2024. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/select-updates-premarket-cybersecurity-guidance-section-524b-fdc-act

[10] Centre for Devices and Radiological Health. Post market Management of Cybersecurity in Medical Devices - Guidance [Internet]. U.S. Food and Drug Administration. 2019. Available from: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

[11] Kim DW, Choi JY, Han KH. Medical Device Safety Management Using Cybersecurity Risk Analysis. IEEE Access. 2020; 8:115370–82.

[12] Chua JA. Cybersecurity in the Healthcare Industry [Internet]. Task Group P CAP, CISSP, and the 405(d) Task Group, editor. podiatrym.com. Podiatry Management; 2021. Available from: https://podiatrym.com/pdf/2021/7/Chua821web.pdf

[13] Centre Cybersecurity [Internet]. U.S. Food and Drug Administration. 2023. https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity#news

[14] Longras A, Pereira T, Amaral A. Cybersecurity Challenges in Healthcare Medical Devices. 2023 Jan 1;66–75.

[15] Leah N. Cybersecurity Challenges Facing Today's Medical Device Industry [Internet]. Nova Leah. 2023 [cited 2024 Jun 13]. Available from: https://www.novaleah.com/cybersecurity-challenges-facing-todays-medical-device-industry/