Int. J. Pharm. Investigation, 2026; 16(4):1312-1322.
https://www.jpionline.org

Review Article

Digital Defence in Healthcare: Medical Device Cyber Security in the EU and USA

Lakshmi Prasanthi Nori, Brahmaiah Bonthagarala, Cherukuri Harsha Vardhan, K.Lalitha Sri N V Sai Lakshmi, Sarapenta Sravani, Gumpati Supriya, Venkateswara Raju Kalidindi*

Department of Pharmaceutical Regulatory Affairs, Professor, Shri Vishnu College of Pharmacy, Vishnupur, Bhimavaram, West Godavari, Andhra Pradesh, INDIA.

ABSTRACT

The healthcare digitization changed the delivery of care to patients but also enhanced the exposure of medical devices to cyberattacks. The recalls of pacemakers and insulin pumps for being vulnerable to flaws underscore the present threats against patient safety. A comparative analysis of regulatory policies in the European Union (EU) and United States (US) reaffirms common priorities including lifecycle integration of cybersecurity, secure-by-design philosophy and post-market surveillance. In EU, technical advice comes from the European Union Agency for Cybersecurity (ENISA) and is in conformity with more extensive legislative tools, such as the Medical Device Regulation (MDR 2017/745), General Data Protection Regulation (GDPR), and the Network and Information Systems Directive (NIS). In US, Food and Drug Administration (FDA) promotes a prescriptive framework with comprehensive technical requirements, primarily the 2023 guidance that established the Secure Product Development Framework (SPDF) and imposed measures like encryption, authentication and regular patching. Although both frameworks align on fundamental principles, divergence still exists in scope, enforcement and technical detail, posing compliance issues to global manufacturers. Observed gaps highlight the pressing requirement for aligned global strategies that combine regulatory alignment, sharing of threat intelligence, and adaptive innovation to enhance device resilience and protect patient safety from expanding cyber threats.

Keywords: Cybersecurity, Data protection, Digital health, FDA guidelines, Medical devices, Post-market surveillance.

Correspondence:
Venkateswara Raju Kalidindi
Associate Professor, Department of Regulatory Affairs, Shri Vishnu College of Pharmacy, Vishnupur, Bhimavaram, West Godavari-534202, Andhra Pradesh, INDIA.
Email: Venkateswararaju.k@svcp.edu.in
ORCID: 0000-0002-6279-4710

Received: 02-04-2026;
Revised: 29-05-2026;
Accepted: 13-07-2026.

INTRODUCTION

Today's healthcare has been totally revolutionized with the integration of digital technology into medical devices. Whereas devices were once isolated to perform single tasks, today they are increasingly networked, able to communicate wirelessly, remote monitor, share data in the cloud, and even perform real-time analytics powered by artificial intelligence (USFDA, 2019). Improved clinical outcomes, more personalized care, and greater patient engagement are all promised through these developments. But the same interdependence that drives innovation also introduces vulnerabilities that malicious forces might exploit. Medical devices, unlike typical IT systems, have direct physiologic interfaces with patients; therefore, a cyber-attack might jeopardize not only data integrity but also human life (Sivaraman *et al*., 2019). Due to the high worth of health information and the potentially catastrophic consequences of disrupted services, the healthcare sector has been one of the most tempting points for cybercriminals. Medical equipment was frequently at the heart of ransomware assaults, which rose by more than 70% against hospitals between 2020 and 2021 based on reports (Zhang *et al*., 2022). Incidents such as the 2019 Medtronic insulin pump recall and the 2017 Abbott pacemaker recall, whose defects allowed illegal reprogramming, illustrate the real-world risks of poor cybersecurity protocols (Freyer *et al*., 2024). These instances reveal that cybersecurity in healthcare is a concrete threat that needs systematic and governmental response rather than just a hypothetical concern. Over recent years, several significant real-time cyber incidents affecting medical devices have been graphically summarised in Figure 1.

METHODOLOGY

In this review, a systematic narrative method was used to review the regulatory, technical, and academic evidence on medical device cybersecurity in the European Union and the United States. PubMed, Scopus, IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar were searched systematically in terms of literature, as well as the official documents of

OPEN ACCESS
Manuscript TECHNOMEDIA

DOI: 10.5530/ijpi.20260296

Publishing Partner : Manuscript Technomedia. [www.mstechnomedia.com]

the European Union Agency for Cybersecurity, the MDCG repository that belongs to the European Commission, IMDRF publications, and the Food and Drug Administration database. Search terms were a combination of keywords containing medical devices cybersecurity, MDR 2017/745, GDPR, NIS/NIS2, FDA guidance, SPDF, IoMT security, ransomware in healthcare and risk management and secure by design. The publications between 2013 and 2025 were taken into consideration with the preference on the peer-reviewed articles, regulatory recommendations, and reports on cybersecurity risks, compliance requirements, and lifecycle management of connected devices. Articles on non-English, opinion articles, which are not technical in nature and studies that are not related to healthcare situations were excluded. The information extracted was grouped into themes on threat landscapes, benefits of cybersecurity practices, EU and US regulatory framework, and cross-jurisdictional comparison. Thematic synthesis was thereafter undertaken to determine instances of regulatory convergence, divergence and their implications to global manufacturers.

Medical devices are distinct from typical IT infrastructure since they face specific challenges. The life cycle of many devices is quite long, often spanning 10 to 20 years, during which hardware and software can become obsolete and unsupported. The potential effect of a single compromise is heightened by the fact that devices utilized in clinical environments are often linked together in hospital networks (Shnawa and Ss, 2022). Also, capability, size, and power constraints might render it impractical to include advanced security measures, rendering devices inherently more vulnerable than traditional IT systems. Cybersecurity for medical devices is an important area for control through regulation due to these considerations (Bracciale *et al.*, 2023). The Parkerian Hexad model describes the basic security principles underpinning the whole medical device protection by referencing the traditional CIA (Confidentiality, Integrity and Availability) concept in an expanded manner to encompass eight key elements, as shown in Figure 2.

Regulators around the globe have been cracking the whip on their regulations based on these threats. EU Medical Device Regulation (MDR 2017/745) have cybersecurity responsibilities, which are also supplemented by broader legislation like NIS Directive and GDPR (Al-Haidari *et al.*, 2021). ENISA plays a key role in supporting implementation through providing sector-specific guidance, risk management methods, and technical advice (Kostkova *et al.*, 2022). FDA has issued guidance documents since 2014. The 2023 premarket guidance update provided the concept of a SPDF (Anwar *et al.*, 2023). The manufacturers need to demonstrate security features such as encryption, authentication, timely patching, and vulnerability management as part of regulatory submissions, and they need to integrate cybersecurity considerations across the device lifecycle (Garg *et al.*, 2020). Figure 3 is a summary of the key security control categories needed for medical device cybersecurity.

Even though cybersecurity is recognized to be pivotal to the functionality and safety of medical devices within both nations, the technical emphasis and scope of their approaches vary. While the FDA has more specific, device-specific technical requirements, EU is more holistic in its approach, encompassing cybersecurity in legislation that applies to a range of industries (Almousa *et al.*, 2022). The difference causes challenges for multi-national manufacturers, for example, redundant compliance processes and uncertainty regarding bringing goods into compliance with multiple standards. Without standardized global standards, innovation may be impeded, and patients may face inconsistent levels of protection (Hussain *et al.*, 2022). As the US and the EU possess two of the most influential regulation frameworks globally, others often replicate their approach. A comparison of different frameworks is thus necessary to determine international standards as well as for compliance within the regions (Khera *et al.*, 2023). Stakeholders can get a better idea of how to develop strong, secure medical device ecosystems by examining overlaps, gaps, and points of convergence. This paper discusses the pros and cons of the USA and EU cybersecurity regulations for medical devices and examines the means to harmonize them. Through this, it illustrates how, in the era of digital health, cybersecurity has evolved from being an afterthought in technology to being a vital component of patient safety and regulatory compliance (Perez *et al.*, 2023). This study was based on real-life occurrences and recent regulatory debates. From a technological aspect as well as from manufacturers' and clinicians' real-life experiences, this review focuses on the pragmatic implications of these policies.

Cybersecurity Threat in Medical Devices

The attack surface of the healthcare sector has expanded because of increasing medical device interconnectivity, laying patients and health systems open to a variety of cyberthreats. These threats, from highly sophisticated state-sponsored attacks to malicious software infections, are testament and not hypothetical. Cyber-attacks on medical devices have the potential to disrupt critical care, delay treatment, or even put patients in danger, in contrast to bank or retail sector breaches. The devices vulnerable to cyber-attacks are listed in Table 1.

Malware and Ransomware

Ransomware is one of the largest threats to health care, which denies user's access to vital services until a ransom is paid. The WannaCry attack in 2017 had a devastating effect on the National Health Service (NHS) in the United Kingdom (DHSC, 2018), causing procedures and appointments to be cancelled. The attack did not directly target medical devices but impacted connected systems, illustrating how weaknesses in a hospital can cause devices to become unavailable. This weakness has been illustrated further by subsequent ransomware attacks that directly made

use of vulnerabilities in infusion pumps and diagnostic imaging devices.

Unauthorized Access and Device Manipulation

In case security is not adequate, medical devices such as insulin pumps, pacemakers, and implanted neurostimulators can be accessed remotely by unauthorized users. Malicious wireless instructions can be transmitted to these devices, something ethical hackers have consistently demonstrated. FDA recalled 465,000 Abbott pacemakers in 2017 due to defects that would allow for illegal reprogramming (USFDA, 2018). This incident proved how hackers could alter pacing configurations or drain device batteries, compromising patient lives.

Data Breaches and Privacy Infringements

Cyberattacks compromise patient privacy alongside interfering with functionality. Sensitive health data is often transmitted and stored by medical devices, leaving it susceptible to theft or interception. In a Ponemon Institute report, the average cost of a healthcare sector data breach in 2022 was more than USD 10 million, the highest of any sector (Mehta *et al.*, 2023). Since they contain financial and medical information that may be used in fraud, stolen health data are particularly valuable on the illegal market.

Denial of Service (DoS) and Availability Risks

To function correctly, medical devices, particularly in critical care and remote monitoring applications, must be continuously connected. Through the exploitation of DoS or distributed DoS (DDoS) attacks, perpetrators could exploit this dependency and overwhelm Device communication interfaces and render systems useless during a crisis (Krittanawong *et al.*, 2023). For example, networked infusion pump vulnerabilities have been exploited for example, to traffic-crash systems, delaying legitimate medical requests.

Software and Supply Chain Vulnerabilities

Exploitation of vulnerabilities realized during the supply chain is becoming prevalent. Third-party software libraries or modules that may contain unseen flaws are often integrated into medical devices (Magrabi *et al.*, 2019). Many digital systems, such as some healthcare applications, were affected by the Log4j vulnerability that was unveiled in 2021. Devices were compromised by manufacturers who failed to upgrade or patch them in a timely way, illustrating how difficult it is to maintain a device safe throughout its lifespan.

Legacy Devices and Patch Management

Long after the manufacturers cease to offer updates or support, many of these devices are still being used in hospitals. These old devices often do not have the ability of modern encryption or authentication techniques and are running outdated operating systems (Farahani *et al.*, 2022). Although they are very vulnerable, they continue to be used because it is costly to replace them. Over 70% of medical imaging equipment used unsupported versions of Windows, as stated in a 2020 survey, making them the best target for hackers.

Internet of Medical Things (IoMT) and Network Vulnerabilities

Emerging threats are introduced by the expansion of the IoMT, including networkable wearable devices, monitor sensors, and

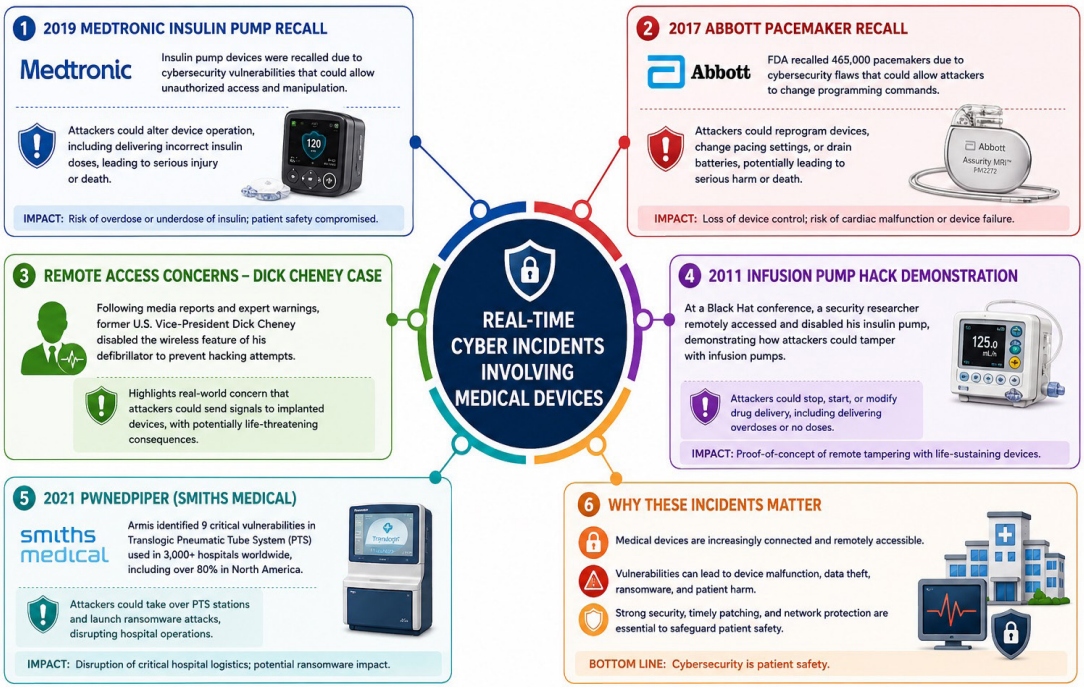

Figure 1: Recent Cyber Incidents of Medical Devices.

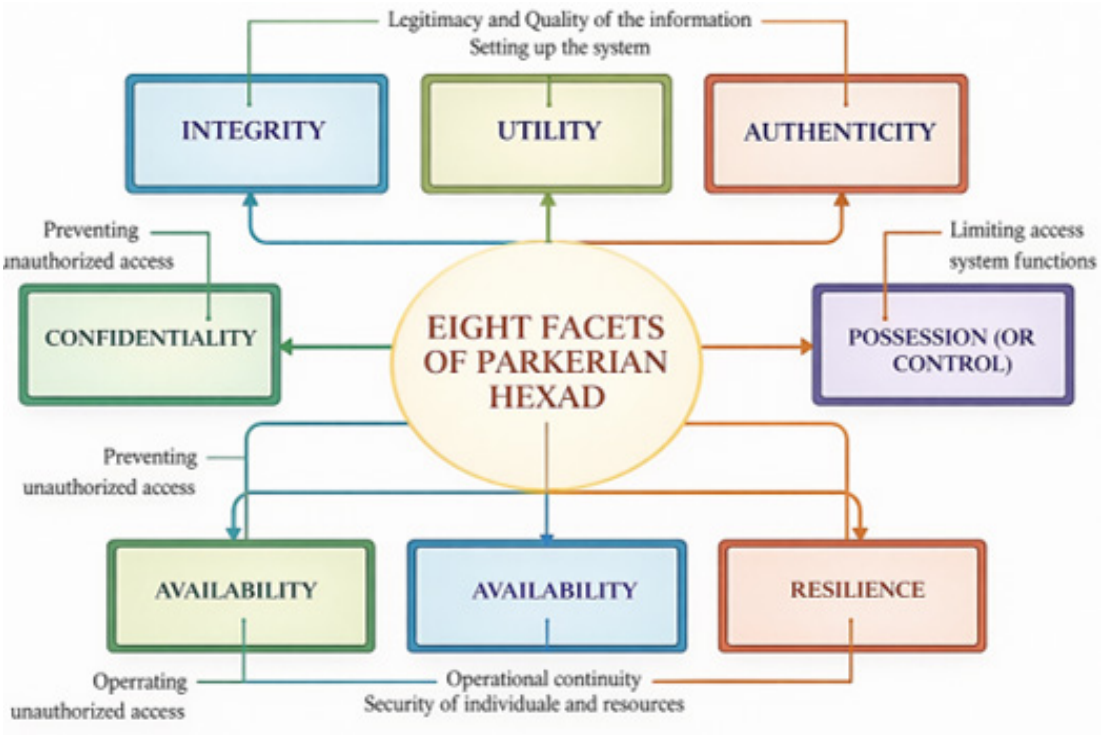

Figure 2: Eight Facets of Parkerian Hexad.

medical devices. Attackers can be able to transition from a compromised device to the broader clinical network because of poor authentication practices, poorly segmented hospital networks, and unencrypted data streams (Fernandes *et al.*, 2023). IoMT ecosystem complexity increases the difficulty of robust monitoring and crisis response. Apart from minimizing risks, strengthening security measures has tangible benefits for patients, authorities, and healthcare systems.

Benefits of Cybersecurity in Healthcare

Active cybersecurity measures have vast benefits for manufacturers, healthcare providers, patients, and regulators, despite the extreme vulnerability of medical devices to cyberattacks. Facilitating safe innovation, improving trust, and ensuring digital health system sustainability are all motivations to improve cybersecurity beyond compliance. The principal benefits of implementing robust cybersecurity practices within healthcare and medical devices are depicted in Figure 4.

Improved Patient Safety

The safeguarding of patient life is the primary benefit of robust cybersecurity. Developers can minimize the risk of unauthorized tampering by implementing encryption, authentication, and constant surveillance in the device design (Jha *et al.*, 2024). Secure firmware updates, for example, ensure that implanted devices, like insulin pumps or pacemakers, cannot be nefariously altered, reducing the risk of potentially lethal scenarios.

Preservation of Sensitive Healthcare Information

Cybersecurity ensures patient information's integrity, confidentiality, and availability. Robust access controls and encryption prevent data leaks and unauthorized releases as the volume of interconnected devices capturing individual health data increases (Kotz *et al.*, 2022). Not only is preserving privacy ethical, it is also legally mandated according to policies such as the GDPR in the EU and HIPAA in the USA.

Regulatory Compliance and Market Access

Companies that integrate cybersecurity into their products have faster market access and simpler regulatory clearances. US and EU regulators alike now demand submissions with supported security features (Kruse *et al.*, 2017). Insufficient protection raises the risk of delay, recall, or even rejection of a product. Conversely, demonstrating compliance with standards such as ENISA's guidelines or the FDA's SPDF enhances confidence in the reliability of the device.

Financial and Reputation Benefits

Financial damages may occur due to cyber-attacks. If reputational damage is not factored in, the typical healthcare breach costs over USD 10 million (Moustafa *et al.*, 2019). Healthcare providers and manufacturers reduce their exposure to litigation, fines, and lost consumer confidence by investing in security that prevents loss. A good reputation for cybersecurity can also assist companies in distinguishing themselves from congested sectors, providing them with a competitive advantage.

Increased Clinical Efficiency and Trustworthiness

Malware and denial-of-service attacks are less able to create downtime on properly protected systems. Since seconds count in emergency care, trustworthy performance is highly critical. Cybersecurity features such as reliable communication protocols and real-time intrusion detection ensure that devices operate correctly so that physicians can focus on patient care instead of technology problems (Wu *et al.*, 2023).

Foundation for Future Innovation

Security of digital infrastructure is critical for new technologies such as blockchain-based health records, telebotic surgery, and artificial intelligence (Ali *et al.*, 2022). Without cybersecurity, these advances can't be deployed safely. Stakeholders lay the foundation for safe deployment of next-generation medical technologies that can potentially lead to further patient benefit by incorporating robust protections now.

The structural design of regulatory rules affects significantly the real-world effectiveness of technical controls, as evidenced by the challenges of the second section. The next section looks at how the US and EU regulatory regimes attempt to structure device security in the real world while taking such threats into consideration.

Regulatory Framework for Medical Device Cybersecurity in EU

The EU has created an extensive, multi-layered regulatory framework interweaving cybersecurity needs into more extensive data protection and digital infrastructure legislation. Of central significance to this framework is the MDR 2017/745, completed in May 2021, which explicitly identifies cybersecurity as a primary determiner of device performance and patient safety (ECMDCG, 2019). Annex I to the MDR requires manufacturers to make devices that can avoid unauthorized access, data manipulation, and functional modification along the product lifecycle. The regulation imposes ongoing risk assessment and requires manufacturers to deploy controls aimed at confidentiality, integrity, and availability of information. Two principal cross-sectoral tools, the GDPR and NIS Directive (ENISA, 2023), support the EU cybersecurity ecosystem. The GDPR applies tough controls on personal health information by ensuring encryption, data minimization, and legal processing, whereas the NIS Directive mandates healthcare operators and digital service providers to put in place sufficient cybersecurity measures and report incidents to national authorities on a timely basis. These instruments collectively express the EU's comprehensive vision, seeing cybersecurity as a foundation for patient safety, data governance, and systemic resilience, not merely a technical aspect. Central institutional backing is through the ENISA and the MDCG. ENISA technical reports and sectoral advice foster security-by-design, coordinated vulnerability disclosure, and good risk management throughout the healthcare field (Mahomed *et al.*, 2023). ENISA's work is supported by MDCG's 2019-16 Guidance in translating MDR commitments into implementable requirements for manufacturers, covering post-market surveillance, patch management, secure software development, and documentation practices. While not binding,

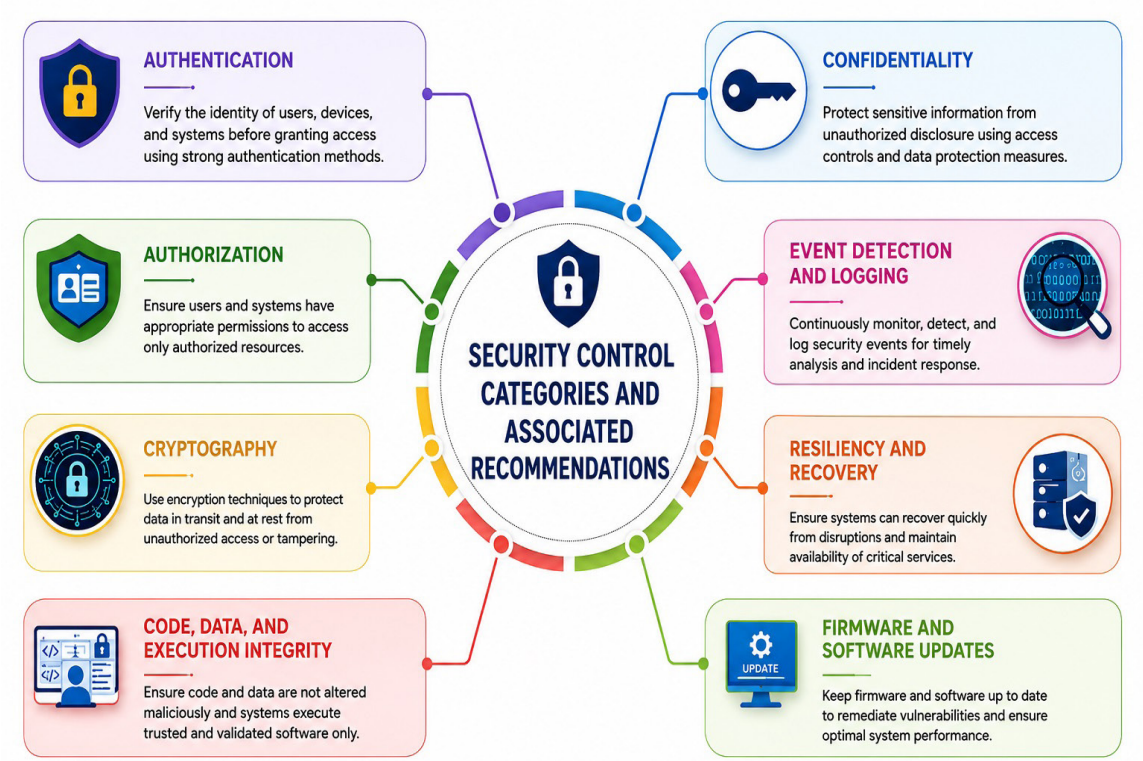

Figure 3: Categories of Security Controls and Suggestions.

Table 1: List of medical devices prone to cyberattacks.

Medical Device	Cyber Attack	Result of the Attack
Pacemakers	Unauthorized firmware access; battery drain; MITM attack.	Altered pacing, device shutdown, wrong diagnostics.
Insulin Pumps	Remote dose manipulation; DoS; OTA exploit.	Hypoglycemia, ketoacidosis, missed alerts.
MRI Scanner	Magnetic field alteration; alarm disable; patient data mix.	Burns, missed warnings, wrong diagnosis.
X-ray Generator	Increase current; modify display; forced restart.	Radiation overdose, loss of configuration.
Infusion Pump	Spoof alerts; disable purge; pendant manipulation.	Over/under medication, air embolism risk.
PET Scanner	Disable alarms; encrypt data; modify procedures.	Ransom demand, wrong diagnostic protocol.
CT Scanner	Increase KVP; modify display; alter density threshold.	Radiation excess, segmentation failure.
Ventilator	False alarms; restart attack.	Treatment disruption, unnoticed failure.
Anesthesia Device	Disable oxygen guard; alter dosage.	Hypoxia, overdose, fatal outcomes.
Lung-Heart Machine	Heparin pump manipulation; alarm disable.	Clotting or bleeding, unnoticed danger.
Dialysis Machine	Pressure monitor Disconnect; dialysate ratio change.	Acute poisoning, pump shutdown.
Medical Lasers	Remove standby; change power.	Tissue burns, surgical interruption.
Robotic Surgery	Video feed off; false warnings.	Procedure halt, patient risk.
MD Data Systems	Refuse data transfer; false incidents.	Wrong treatment decisions.
Monitoring Equipment	Alter vitals; deny transfer.	Misdiagnosis, delayed response.
EHR Systems	Modify/delete records; change timings.	Wrong treatment, loss of history.

MDCG guidance finds extensive usage in conformity assessments, offering uniform interpretation across Member States. Strong focus by the EU is put on the principle of cybersecurity-by-design, where security controls are imposed upon manufacturers to embed in product development from initial stages (Gopalakrishnan *et al.*, 2022). This encompasses context-specific risk modelling, encryption and authentication controls, resilience and penetration testing, and access control policies. Suppliers need to hold an up-to-date risk management file recording identified threats, mitigation measures, and residual risks, which is part of the technical dossier that is assessed in conformity assessment. In addition, defense-in-depth is integrated within EU guidance, where there are numerous layers of protective measures across the device's lifecycle. Post-market surveillance responsibilities under MDR include cybersecurity vigilance, with Periodic Safety Update Reports (PSURs), Corrective and Preventive Actions (CAPA), and obligatory incident reporting to national authorities and CSIRTs under the NIS Directive (Boulos *et al.*, 2022). Dual reporting might add administrative burden but improves accountability and traceability of cyber incidents. The regulatory frame work is depicted in Figure 5.

The EU regulatory framework is further reinforced through harmonization with overarching digital policies. The GDPR ensures legal processing of health information, and the Cybersecurity Act (2019) creates an EU-wide certification system that may ultimately be extended to medical devices (Thamilarasu and Poovendran, 2022). The upcoming NIS2 Directive, which Member States are scheduled to transpose in 2024, will make more stringent cybersecurity obligations on healthcare organizations and suppliers (Fernández-Alemán *et al.*, 2013). Together, these tools demonstrate an organized regulative environment that closely interlinks patient safety, data protection, and cyber resilience, highlighting the EU's determination to promote cybersecurity across the healthcare industry (Hasselgren *et al.*, 2020).

Regulatory framework in USA

FDA, has become a world leader in driving medical device cybersecurity policy. In contrast to the legislative model of the European Union, the U.S. system is guidance-based, with the majority depending on non-binding but very influential regulatory guides that hold significant matter during device submissions. The FDA initially published premarket cybersecurity guidance in 2014, stipulating what manufacturers should do to show evidence of protection from cyber threats through formal risk analysis, asset identification, threat modelling, and mitigation planning (Agbo *et al.*, 2019). This was followed by post-market guidance in 2016, which presented concepts of Coordinated Vulnerability Disclosure (CVD), risk-based patching, and continuous monitoring. With growing complexity in cyberattacks and interconnected healthcare systems, the FDA's 2023 premarket guidance markedly raised expectations by requiring manufacturers to submit extensive cybersecurity documentation, design controls, and lifecycle risk management approaches. Cybersecurity is now officially codified under the

Federal Food, Drug, and Cosmetic Act (FD&C Act) as a factor in both the safety and effectiveness of devices, thereby integrating it into statutory compliance requirements.

SPDF

FDA's cybersecurity approach is founded on the SPDF (Rajput *et al.*, 2022). It turns cybersecurity into an active design component instead of a passive one by mandating the incorporation of security principles from the device lifecycle. The SPDF encompasses the threat modelling, security architecture, validation and verification, documentation patch management. The SPDF integrates cybersecurity into existing quality management processes by adhering to Quality System Regulation (21 CFR Part 820), ensuring traceability and accountability along the device life cycle.

Cybersecurity Bill of Materials (CBOM) and Patch Management

One of the key characteristics of the U.S. approach is that a CBOM, a thorough listing of a device's software components, libraries, and operating systems, is mandatory (Singh *et al.*, 2023). The CBOM increases transparency and enables regulators and healthcare organizations to evaluate vulnerabilities and prioritize the deployment of patches. Manufacturers are required to deploy validated patch management systems that allow secure updates without interfering with device operation. They are also expected to offer implementation support to users and provide unambiguous timelines for the availability of patches, thus increasing user awareness and system reliability.

Post-Market Management and Vulnerability Disclosure

FDA post-market cybersecurity guidance puts high value on ongoing monitoring, anticipatory vulnerability discovery, and open disclosure procedures (Abbas *et al.*, 2023). Manufacturers are tasked with working with ethical hackers, researchers, and health care providers through CVD programs and evaluating discovered risks through a tiered control framework that differentiates controlled from uncontrolled risk states. The 2016 guidance also promoted cooperation with Information Sharing and Analysis Organizations (ISAOs) to support situational awareness throughout the healthcare environment.

Legislative Trends and Enforcement

Prior to 2022, the FDA depended mostly on general device safety provisions to implement cybersecurity requirements. Nonetheless, the Consolidated Appropriations Act of 2022 provided the FDA with direct authority to mandate cybersecurity data in all device filings (Patel *et al.*, 2024). The Act requires inclusion of precise description of cybersecurity controls, coordinated vulnerability disclosure strategy and post-market monitoring and patch management plan. This legislative development revolutionized cybersecurity from being a "best practice" to a legal requirement, solidifying the FDA's enforcement authority and holding everyone in the medical device industry accountable.

Strengths and Challenges of US Approach

US regulatory framework is exceptional for its technical specificity, lifecycle incorporation, and prescriptive definition, providing a

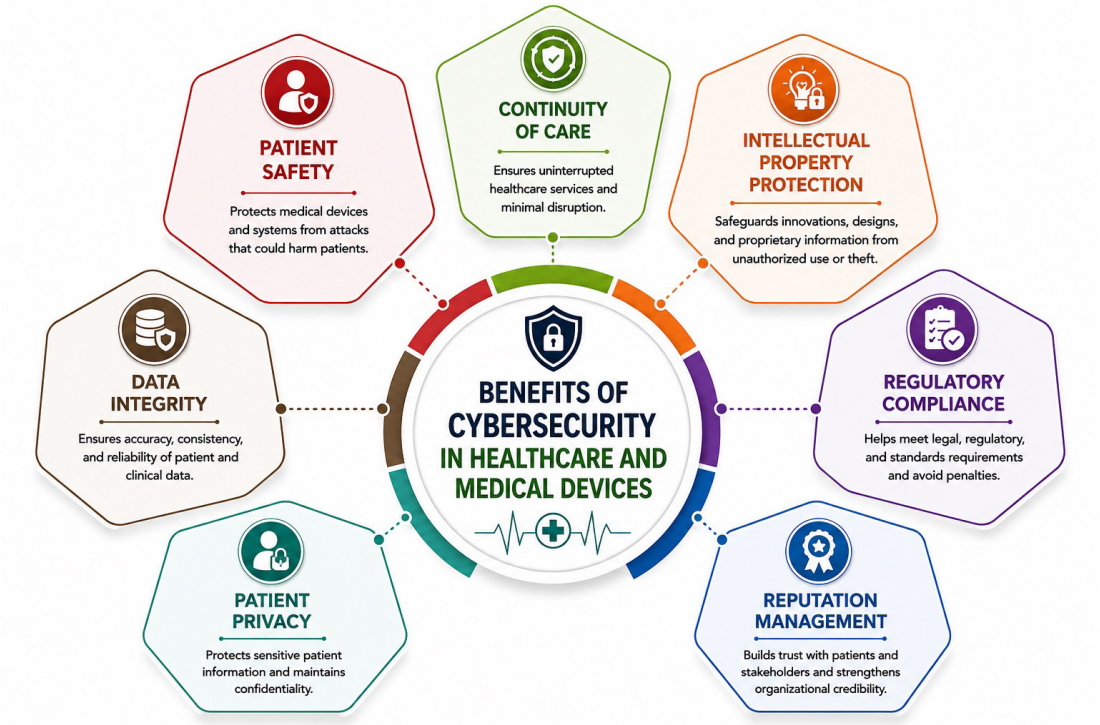

Figure 4: Benefits of Cybersecurity for Medical Devices.

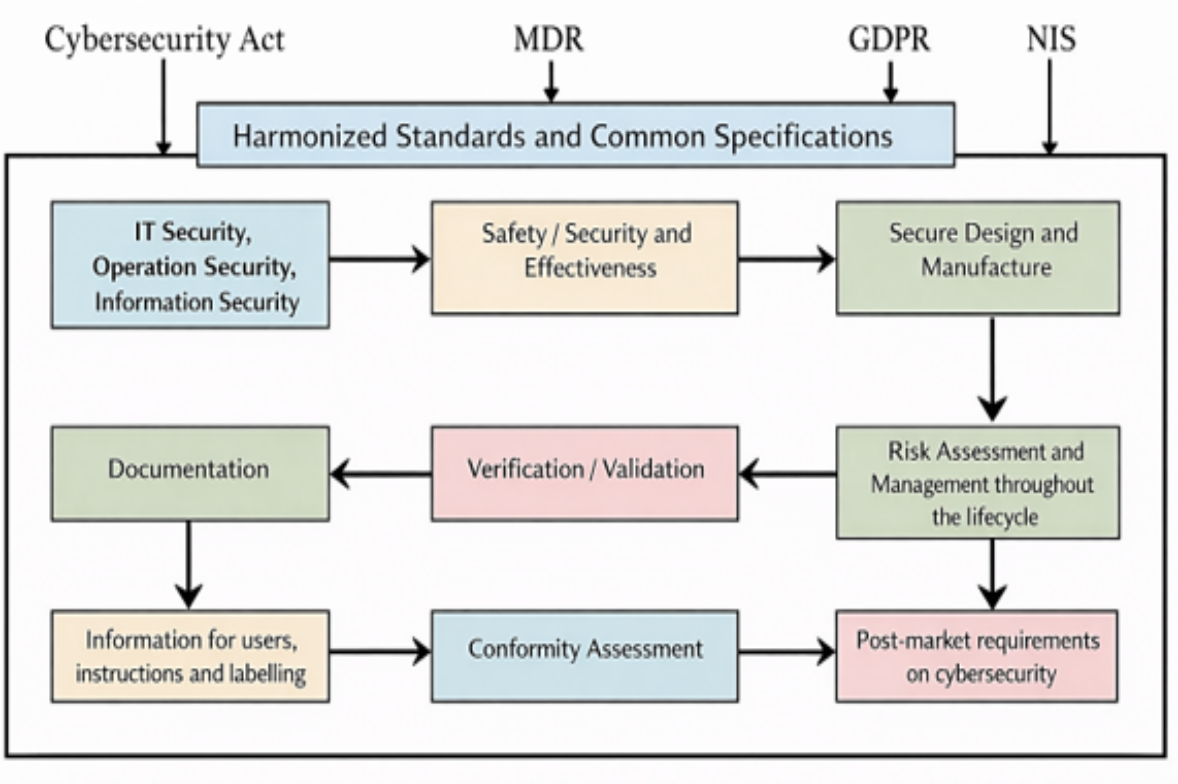

Figure 5: Medical device regulations as per EU.

worldwide example of organized compliance. SPDF and CBOM together provide visibility, traceability, and risk-based assurance across all stages of device development and deployment. Complexity of the model is a challenge, though. Implementation requires significant financial and technical investment, with high costs to small and medium-sized enterprises. Moreover, the prescriptive character of the framework can stifle innovation in favour of adherence. Fragmentation of oversight by the FDA and other federal agencies of cybersecurity sometimes creates policy misalignment, whereas the speed at which cyber threats evolve can exceed the FDA's cycle times, creating temporary regulatory loopholes (Yaqoob *et al.*, 2021).

Comparison of Cybersecurity of Medical Devices in EU and USA

A comparative analysis of the EU and US cybersecurity environments shows convergence in the underlying principles and divergence in regulatory implementation and scope as given in Table 2 (Alsubaei *et al.*, 2019). The two continents identify cybersecurity as a core element of patient safety but differ significantly in their legislative and operational priorities. EU uses an all-encompassing and integrative model of regulation, integrating cybersecurity as part of its larger digital health and data protection framework. Core devices like MDR 2017/745, MDCG 2019-16 guidance, ENISA advice, GDPR, and the NIS/NIS2 Directives all require security-by-design elements across the lifespan of the device (Naeem *et al.*, 2021). Compliance is checked by notified body testing during conformity assessments, keeping attention focused on data integrity, breach handling, and interoperability always. The EU model hence focuses on systemic embedding, relating cybersecurity directly with data protection and network resilience. By contrast, the US system, directed by the FDA, is technically prescriptive. It relies on the QSR and is supported by the 2023 premarket guidance, which requires risk management plans, Software Bills of Materials (SBOMs), and formalized threat models to be included in premarket submissions. Requirements for post-market are aimed at vulnerability disclosure, patching, and coordinated response mechanisms. The US strategy emphasizes technical thoroughness, supplemented by guidelines like NIST and AAMI SW96:2023. The divergence is also seen in standards adoption, where the EU adopts ISO/IEC 81001-5-1 and ENISA guidelines, whereas the US favours NIST and AAMI guidelines. The lack of congruence normally forces global manufacturer companies to retain dual compliance records, which adds both cost and time to market (Biasin *et al.*, 2024). For instance, a manufacturer of an implantable cardiac device needs to create separate cybersecurity documents specific to every region. While IMDRF and WHO have made a start on harmonization with specific reference to post-market surveillance and coordinated vulnerability disclosure implementation being uneven across regions (Al-Turjman *et al.*, 2022). An aligned global regulatory system may eliminate redundancy, promote interoperability, and provide balanced patient protection across borders. Eventually, convergence between the EU's privacy-led scope and the US's technical precision will be critical in balancing innovation with world patient safety.

Table 2: Cybersecurity requirements as per EU and USA.

Parameter	European Union (EU)	United States (USA)
Regulatory Basis	GDPR, MDCG 2019-16, MDR 2017/745, and the NIS/NIS2 Directive.	Quality System Regulation (21 CFR Part 820), FDA Cybersecurity Guidance (2023), and the FD&C Act.
Cybersecurity in Premarket	mandates that manufacturers incorporate security into risk management and file according to MDR.	The FDA mandates that submissions include SPDF integration, threat modelling, and cybersecurity risk management.
Post market Expectations	Reporting incidents under the MDR. vigilance system; NIS2 adds obligations for reporting breaches.	Post-market recommendations: patching, vulnerability management, and coordinated disclosure (suggested by CBOM).
Key Documents	EU NIS2 Directive (2023), ENISA Guidelines (2023), and MDCG 2019-16.	FDA Post-market Cybersecurity Guidance (2016, revised 2023 draft), FDA 2023 Guidance.
Focus Areas	Holistic: patient safety combined with data protection and privacy (GDPR alignment).	Technical safeguards, risk-reduction strategies, and label transparency.
Enforcement	Compliance is assessed by Notified Bodies and Competent Authorities.	FDA analyses applications and has the power to compel recalls and non-compliance.
International Influence	Consistent with EU data protection and digital policy.	Impacts international cybersecurity frameworks through IMDRF participation and FDA recognition.

Challenges and Future Directions of Medical Device Cybersecurity

Despite strong advances in cybersecurity legislation in the USA and EU, medical devices are susceptible to new threats. Technological evolution happens too fast to be followed by regulatory changes, resulting in temporary exposure of devices to new attack vectors. Legacy equipment, which is still common in hospitals, adds additional threats with old operating systems and poor upgrade opportunities. Regulatory complexity further weighs on smaller producers, especially under duplicative structures like the EU's MDR, GDPR, and NIS, and the FDA's prescriptive but non-harmonized regulations (Khan *et al.*, 2023). This absence of international standardization adds cost and restricts market entry for multinational manufacturers. Economic and resource requirements also hinder compliance. Conceiving threat models, keeping up with CBOM, performing penetration testing, and publishing timely patches are expensive endeavours that most SMEs and healthcare organizations cannot afford to maintain. Such financial limitations can constrain innovation and slow down balanced deployment of safe medical technologies. Progress in the future will need technology and regulation flexibility. Artificial intelligence and machine learning can augment threat detection, while zero-trust architectures and blockchain can strengthen device security and data integrity. Establishing regulatory sandboxes can accelerate safe innovation, and standardized global norms can minimize duplication, enhance interoperability, and safeguard patients. Education and legacy device management remain just as important. Integrating cybersecurity into organizational culture and healthcare delivery systems is essential to protect patient safety, maintain innovation, and ensure public trust in the face of a more digitalized health field (IMDRF, 2022; Abie and Balasingham, 2012).

CONCLUSION

Cybersecurity has become a core driver of medical device safety, effectiveness, and long-term dependability, rather than simply being a peripheral regulatory requirement as previously. The comparison of US and European frameworks presents divergent but complementary strategies the United States taking a prescriptive, technically oriented model rooted in FDA guidance and regime risk management, whereas the European Union harmonizes cybersecurity more comprehensively as part of digital health regulation and data protection law. Yet, both models reinforce the enduring necessity of international harmonization, specifically in the treatment of legacy device vulnerabilities, scattered regulatory channels, and the unequal burden on small and medium-sized producers. In the future, responsive regulatory paradigms need to be accompanied by ongoing threat intelligence sharing, compliance mechanisms that are viable, and the adoption of emerging technologies like blockchain to guarantee data integrity and artificial intelligence to anticipate risk monitoring. Notably, cybersecurity must be incorporated as an integral part of the healthcare ecosystem along the continuum, from device manufacturing and development to clinical rollout and physician participation. This shift will take place by reconciling the U.S. emphasis on technological fervour with the EU's focus on patient privacy and rights. It is only through collaborative global standards and across-industry collaboration that medical devices can stay resilient, reliable, and innovation-led in the changing threat environment. The coming decade offers the prospect of creating globally harmonized standards which marry U.S. technical excellence with EU's rights-based regulation. Policymakers, business leaders, and healthcare professionals should place greater emphasis on cross-sector cooperation, investment in security-by-design concepts, and

smaller manufacturer capacity-building to keep medical device ecosystems secure, interoperable, and innovation-led.

ACKNOWLEDGEMENT

The authors are thankful to Shri Vishnu College of Pharmacy for providing the necessary facilities.

ABBREVIATIONS

AAMI: Association for the Advancement of Medical Instrumentation; **CAPA:** Corrective and Preventive Actions; **CBOM:** Cybersecurity Bill of Materials; **CIA:** Confidentiality, Integrity, and Availability; **CSIRTs:** Computer Security Incident Response Teams; **CT:** Computed Tomography; **CVD:** Coordinated Vulnerability Disclosure; **DoS:** Denial-of-Service; **DDoS:** Distributed Denial-of-Service; **EHR:** Electronic Health Records; **ENISA:** European Union Agency for Cybersecurity; **EU:** European Union; **FDA:** Food and Drug Administration; **FD&C Act:** Federal Food, Drug, and Cosmetic Act; **GDPR:** General Data Protection Regulation; **HIPAA:** Health Insurance Portability and Accountability Act; **IMDRF:** International Medical Device Regulators Forum; **IoMT:** Internet of Medical Things; **ISAO:** Information Sharing and Analysis Organization; **MDCG:** Medical Device Coordination Group; **MD:** Medical Device; **MDDS:** Medical Device Data Systems; **MDR:** Medical Device Regulation; **MITM:** Man-in-the-Middle; **MRI:** Magnetic Resonance Imaging; **NHS:** National Health Service; **NIS:** Network and Information Systems Directive; **NIST:** National Institute of Standards and Technology; **OTA:** Over-the-Air; **PET:** Positron Emission Tomography; **PSUR:** Periodic Safety Update Report; **QSR:** Quality System Regulation; **SBOM:** Software Bill of Materials; **SME:** Small and Medium-sized Enterprises; **SPDF:** Secure Product Development Framework; **US/USA:** United States of America; **WHO:** World Health Organization.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHOR CONTRIBUTIONS

Lakshmi Prasanthi Nori designed the study, over-saw the research process, supervised the process, and prepared the main draft of the manuscript. The literature review, data collection and revisions were assisted by Cherukuri Harsha Vardhan. Brahmaiah Bonthagarala advocated the regulatory analysis and technical review. K. Lalitha Sri was working with figures and tables. N. V. Sai Lakshmi assisted in pooling data and references. Sarapenta Sravani helped in the compilation of cybersecurity data and tables. Gumpati Supriya has helped in comparison, proofreading and formatting. Venkateswara Raju Kalidindi went through the work and submission process.

REFERENCES

Abbas, Z., Shaikh, F. K., Khan, S. U., and Chowdhury, M. (2023). Privacy-preserving frameworks for healthcare IoT: A systematic review. Journal of Network and Computer Applications, 212, 103576. https://doi.org/10.1016/j.jnca.2023.103576

Abie, H., and Balasingham, I. (2012). Risk analysis of medical device security with remote delivery of healthcare. International Journal of Telemedicine and Applications, 2012, 902173. https://doi.org/10.1155/2012/902173

Agbo, C. C., Mahmoud, Q. H., and Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. Healthcare, 7(2), 56. https://doi.org/10.3390/healthcare7020056

Al-Haidari, F., Alenezi, A., and Hossain, M. S. (2021). Threat modeling and security assessment of smart medical devices. IEEE Access, 9, 134892-134904. https://doi.org/10.1109/ACCESS.2021.3115476

Ali, A., Hassan, R., Li, J., Khan, M. M., and Alsaqer, M. (2022). Security and privacy challenges in the internet of medical things: A comprehensive survey. Sensors, 22(3). https://doi.org/10.3390/s22030885

Almousa, M., Al-Issa, Y., Ottom, M. A., and Tamrawi, A. (2022). A comprehensive survey on cybersecurity for medical devices: Taxonomy, challenges, and future directions. Computers and Security, 115, 102604. https://doi.org/10.1016/j.cose.2022.102604

Alsubaei, F., Abuhussein, A., and Shiva, S. (2019). Security and privacy in the internet of medical things: Taxonomy and risk assessment. Future Generation Computer Systems, 93, 541-559. https://doi.org/10.1016/j.future.2018.10.009

Al-Turjman, F., Zahmatkesh, H., and Shahroze, R. (2022). Cybersecurity of smart healthcare: A survey of trends, architectures, and emerging challenges. Future Generation Computer Systems, 125, 580-599. https://doi.org/10.1016/j.future.2021.07.010

Anwar, S., Singh, R., Kumar, A., and Chandrasekaran, K. (2023). Artificial intelligence for anomaly detection in connected medical devices: Opportunities and risks. Journal of Biomedical Informatics, 139, 104259. https://doi.org/10.1016/j.jbi.2023.104259

Biasin, E., Kamenjašević, E., and Ludvigsen, K. R. (2024). Cybersecurity of AI medical devices: Risks, legislation, and challenges. In Research handbook on health, AI and the law (pp. 57-74). Edward Elgar.

Boulos, M., Peng, G., and Vopham, T. (2022). An overview of GeoAI applications in health and healthcare. International Journal of Health Geographics, 21(1). https://doi.org/10.1186/s12942-022-00297-4

Bracciale, L., Loreti, P., and Bianchi, G. (2023). Cybersecurity vulnerability analysis of medical devices purchased by national health services. Scientific Reports, 13, 19509. https://doi.org/10.1038/s41598-023-45927-1

Department of Health and Social Care. (2018). Lessons learned from the WannaCry ransomware cyber-attack. London, UK.

European Commission Medical Device Coordination Group. (2019). MDCG guidance documents. Brussels, Belgium.

European Union Agency for Cybersecurity. (2023). ENISA cybersecurity guidance. Athens, Greece.

Farahani, B., Firouzi, F., and Chang, V. (2022). Healthcare internet of things: Architecture and system design challenges. Future Generation Computer Systems, 124, 320-343. https://doi.org/10.1016/j.future.2021.05.038

Fernandes, S. L., Pradhan, N., Naik, N., Chatterjee, J., and Choudhury, P. (2023). Medical device security: A cybersecurity risk management framework. Biomedical Engineering Letters, 13(3), 379-390. https://doi.org/10.1007/s13534-023-00267-7

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., and Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics, 46(3), 541-562. https://doi.org/10.1016/j.jbi.2012.12.003

Freyer, O., Jahed, F., Ostermann, M., Rosenzweig, C., Werner, P., and Gilbert, S. (2024). Consideration of cybersecurity risks in the benefit-risk analysis of medical devices: Scoping review. Journal of Medical Internet Research, 26, e65528. https://doi.org/10.2196/65528

Garg, S., Singh, A., Kaur, K., Aujla, G. S., Batra, S., and Chen, J. (2020). Edge computing-based security framework for big data in healthcare. Future Generation Computer Systems, 108, 1328-1341. https://doi.org/10.1016/j.future.2018.04.046

Gopalakrishnan, V., Xu, R., Zhang, L., and Shankar, K. (2022). Cybersecurity in implantable medical devices: Emerging threats and countermeasures. Sensors, 22. https://doi.org/10.3390/s22155607

Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., and Faxvaag, A. (2020). Blockchain in healthcare and health sciences: A scoping review. International Journal of Medical Informatics, 134, 104040. https://doi.org/10.1016/j.ijmedinf.2019.104040

Hussain, F., Hassan, S. A., Hussain, R., and Hossain, E. (2022). Cybersecurity for healthcare IoT: A survey of existing threats and solutions. IEEE Internet of Things Journal, 9(12), 9203-9225. https://doi.org/10.1109/JIOT.2021.3139793

International Medical Device Regulators Forum. (2022). Principles and practices for medical device cybersecurity (IMDRF/SEC WG/N60FINAL). Geneva, Switzerland.

Jha, S., Gupta, R., Verma, R., and Sharma, A. (2024). A resilience framework for securing AI-enabled medical devices. Journal of Biomedical Informatics, 150, 104603. https://doi.org/10.1016/j.jbi.2024.104603

Khan, R. A., Arora, A., and Gupta, M. (2023). Risk assessment model for medical device cybersecurity in smart hospitals. Computer Methods and Programs in Biomedicine, 234, 107568. https://doi.org/10.1016/j.cmpb.2023.107568

Khera, R., Jain, S., Lodha, R., and Arora, A. (2023). Cybersecurity of medical devices: Current status and future directions. Indian Journal of Medical Research, 158(4), 280-287. https://doi.org/10.4103/ijmr.ijmr_2057_22

Kostkova, P., Brewer, H., De Lusignan, S., Fottrell, E., Goldacre, B., and Hart, G. (2022). Who owns the data? Open data for healthcare. Frontiers in Public Health, 10. https://doi.org/10.3389/fpubh.2022.870563

Kotz, D., Gunter, C. A., Kumar, S., and Weiner, J. P. (2022). Privacy and security in mobile health: A research agenda. Computers and Security, 120, 102806. https://doi.org/10.1016/j.cose.2022.102806

Krittanawong, C., Rogers, A. J., Aydar, M., Choi, E., Johnson, K. W., and Wang, Z. (2023). Integration of artificial intelligence in healthcare cybersecurity: State-of-the-art and future challenges. NPJ Digital Medicine, 6(1). https://doi.org/10.1038/s41746-023-00884-0

Kruse, C. S., Frederick, B., Jacobson, T., and Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1-10. https://doi.org/10.3233/THC-161263

Magrabi, F., Ammenwerth, E., McNair, J. B., De Keizer, N., Hyppönen, H., and Nykänen, P. (2019). Artificial intelligence in clinical decision support: Challenges for evaluation. International Journal of Medical Informatics, 129, 285-294. https://doi.org/10.1016/j.ijmedinf.2019.06.017

Mahomed, A., Ndamase, A. S., Chigome, R., and Crowther, N. J. (2023). Cybersecurity challenges of electronic health records in developing countries: A review. Health Information Management Journal, 52(2), 71-79. https://doi.org/10.1177/18333583221137313

Mehta, N., Pandit, A., and Shukla, A. (2023). Privacy-preserving machine learning for medical device data: Methods and challenges. Journal of Biomedical Informatics, 140, 104269. https://doi.org/10.1016/j.jbi.2023.104269

Moustafa, N., Turnbull, B., and Choo, K.-K. R. (2019). An ensemble intrusion detection technique based on proposed statistical flow features for protecting IoT network traffic. IEEE Internet of Things Journal, 6(3), 4815-4830. https://doi.org/10.1109/JIOT.2018.2871719

Naeem, M., Malik, A. W., Kiran, M., Akhunzada, A., and Islam, S. U. (2021). Cybersecurity risk management framework for medical IoT. IEEE Access, 9, 113430-113445. https://doi.org/10.1109/ACCESS.2021.3104276

Patel, V., Rajan, D., and Kumar, A. (2024). Cyber resilience strategies for cloud-based medical device ecosystems. Future Generation Computer Systems, 149, 14-27. https://doi.org/10.1016/j.future.2023.10.045

Perez, T., Sharma, K., and Venkatesh, J. (2023). Post-market surveillance of cybersecurity vulnerabilities in medical devices: A global review. Frontiers in Digital Health, 5, 113245. https://doi.org/10.3389/fdgth.2023.113245

Rajput, D. S., Thakur, A., Kumar, R., Maddikunta, P., Gadekallu, T. R., and Liyanage, M. (2022). Secure and sustainable healthcare data transmission using artificial intelligence and blockchain. Sustainable Energy Technologies and Assessments, 52, 102271. https://doi.org/10.1016/j.seta.2022.102271

Shnawa, H. A., and Ss, A.-D. (2022). Cybersecurity threats and protection of IoT medical devices. Health Technology, 12(6), 1287-1296. https://doi.org/10.1007/s12553-022-00704-1

Singh, A., Sharma, P., and Verma, R. (2023). Security challenges in healthcare IoT: A systematic review. Computers and Security, 129, 103204. https://doi.org/10.1016/j.cose.2023.103204

Sivaraman, V., Chan, K., Earl, J., Gallego, B., Dedrick, J., and Ahmad, I. (2019). Security and privacy risks of internet-connected medical devices. JAMA Internal Medicine, 179(9), 1225-1226. https://doi.org/10.1001/jamainternmed.2019.2111

Thamilarasu, G., and Poovendran, R. (2022). Machine learning-based intrusion detection for smart healthcare systems. Computers and Security, 118, 102732. https://doi.org/10.1016/j.cose.2022.102732

U.S. Food and Drug Administration. (2018). Cybersecurity vulnerabilities identified in Medtronic implantable cardiac devices: FDA safety communication. Silver Spring, MD.

U.S. Food and Drug Administration. (2019). Medtronic recalls insulin pumps due to cybersecurity vulnerabilities: FDA safety communication. Silver Spring, MD.

U.S. Food and Drug Administration. (2023). Cybersecurity in medical devices: Quality system considerations and content of premarket submissions. Silver Spring, MD.

Wu, Y., Jiang, X., Tang, J., and Liu, J. (2023). Blockchain-enabled security for medical device communication networks. IEEE Transactions on Industrial Informatics, 19(4), 5132-5143. https://doi.org/10.1109/TII.2022.3222345

Yaqoob, I., Salah, K., Jayaraman, R., and Al-Hammadi, Y. (2021). Blockchain for healthcare data management: Opportunities, challenges, and future directions. Future Generation Computer Systems, 119, 79-95. https://doi.org/10.1016/j.future.2020.09.058

Zhang, Y., Wang, L., Li, X., and Chen, H. (2022). Secure communication protocols for wearable and implantable medical devices: A review. IEEE Access, 10, 54487-54501. https://doi.org/10.1109/ACCESS.2022.3176512

Cite this article: Nori LP, Bonthagarala B, Vardhan CH, Lakshmi KLSNVS, Sravani S, *et al*. Digital Defence in Healthcare: Medical Device Cyber Security in the EU and USA. Int. J. Pharm. Investigation. 2026;16(4):1312-22.