1

Why Medical Device Cybersecurity Cannot Be Ignored

More than 90% of hospitals worldwide rely on networked medical devices to deliver critical care, yet nearly half of these devices have known security vulnerabilities that remain unaddressed. The integration of advanced technology into healthcare systems has created vast attack surfaces, exposing patients and providers to risks beyond data breaches—risks that can directly threaten human life. This chapter examines why ignoring the cybersecurity of medical devices is no longer an option and underscores the urgent need for robust, transparent defenses in the evolving landscape of connected healthcare.

Lives on the Line: The Human Cost of Device Exploits

The stakes in medical device cybersecurity are as urgent and concrete as the risk to human life. Failures in securing healthcare technology can result in immediate harm, such as incorrect therapy administration or sudden loss of critical function. Attackers who exploit medical devices move beyond data theft and directly threaten patients' safety, sometimes with irreversible consequences. In one well-documented case, insulin pumps with unsecured wireless communication protocols proved vulnerable to remote exploitation. Hackers demonstrated that, using rudimentary radio equipment and software flaws in the device firmware, it was possible to transmit unauthorized commands and trigger the pump to deliver dangerously excessive or insufficient doses of insulin. These attacks bypassed authentication due to the absence of strong encryption and session management, exposing patients to life-threatening hypoglycemia or hyperglycemia. Had such methods been used maliciously in a real clinical environment, the result could have been coma, organ failure, or fatality, especially for patients relying on these pumps for daily glycemic control (Aldosari, 2025).

Pacemakers have also been targeted. In a high-profile security demonstration, researchers exploited outdated, unpatched firmware in a commonly deployed brand of implantable cardiac defibrillator. The researchers reverse-engineered communication protocols, exploiting the lack of cryptographic verification between the programming device and implant. By sending malicious radio frequency transmissions, they triggered the device to deliver unnecessary, potentially fatal electrical shocks or, conversely, disabled lifesaving therapy during cardiac events. Clinical compromise was possible because the wireless protocol enabled over-the-air updates without verifying origin or integrity, creating an open channel for attackers within range. While no deaths resulted from this demonstration, the technical route to harm was clear and has sparked widespread concern about similar vulnerabilities in thousands of deployed units worldwide (Elendu et al., 2024).

Large-scale hospital breaches illuminate how attacks on medical device infrastructure affect not just individuals but also entire critical care workflows. The WannaCry ransomware incident

remains a prominent example. This attack infiltrated hospital networks using a widely known exploit targeting unpatched Windows systems, quickly spreading laterally to networked infusion pumps, diagnostic imaging devices, and life-support systems. Devices frozen by the ransomware could not be operated, monitored, or programed, resulting in the suspension of surgeries and the transfer of vulnerable patients to unaffected centers. Mechanisms involved included a combination of exploit chaining, lateral privilege escalation, and poor network segmentation, amplifying a local device compromise to affect hospital-wide operations and increasing the risk of death for critical inpatients (Aldosari, 2025; Elendu et al., 2024).

Vulnerabilities often begin with minor oversights that scale into catastrophic failures. A single device left with outdated firmware or a default password may function as an entry point. Attackers scan for such weaknesses, breach the device, and then use it as a foothold to probe the network for further vulnerabilities or launch denial-of-service attacks against interconnected systems. For example, a compromised infusion pump could be commanded to alter drug dosages, but it could also serve as a jump host, letting attackers map the internal hospital landscape and disable monitoring devices in intensive care units (ICUs). This chain reaction threatens not only single patients but entire wards, especially as device interconnectivity increases. The technical progression—from software bug to network compromise—means a minor misconfiguration can rapidly escalate to a critical care incident (Aldosari, 2025).

Legal consequences for neglecting medical device security are substantial. Healthcare organizations and device manufacturers found liable for preventable breaches face regulatory penalties from agencies such as the U.S. Food and Drug Administration (FDA) and the Department of Health and Human Services (HHS). Notable lawsuits have resulted in multi-million-dollar settlements, regulatory oversight, and mandatory product recalls. For instance, after vulnerabilities were discovered in a line of cardiac devices, the manufacturer was compelled to issue software updates and submit to ongoing FDA scrutiny. The obligations imposed in these settlements often require improved device monitoring, regular patching regimes, and more rigorous premarket security testing. Such legal precedents have influenced sector-wide policy, embedding cybersecurity by design as a regulatory requirement and establishing industry standards for device life cycle management (Elendu et al., 2024).

There is an equally pressing ethical dimension. Stakeholders in the development and deployment of medical devices hold a professional and moral obligation to ensure the safety and security of their products. Medical device manufacturers must integrate robust security measures from the earliest stages of product development, recognizing that any failing directly endangers patients. Technical professionals and clinicians share responsibility as advocates for implementing and updating secure technology in their institutions. Failure to address known vulnerabilities or allocate resources to security is not only a breach of patient trust but falls short of fundamental professional ethics, especially given the potentially fatal consequences of an exploited device (Aldosari, 2025).

Rapid technological evolution has transformed medical devices from standalone machines into components of complex, interconnected hospital networks. This shift has multiplied attack surfaces and amplified both the potential impact and obligation for strong device security. Cybersecurity must match this complexity, evolving as a core aspect of patient care and organizational accountability (Aldosari, 2025; Elendu et al., 2024).

The Evolution of Medical Devices: From Analog to Networked

Medical device security has rapidly evolved from an afterthought to a mission-critical concern due to the dramatic technological changes unfolding across the healthcare landscape. As frontline practitioners and technical stewards encounter persistent real-world cyber threats, it is vital to recognize that the challenges are not merely device-specific but rather a byproduct of a profound transformation in system design and connectivity, which has fundamentally altered risk profiles over time.

Initially, medical tools operated as standalone, electromechanical devices with minimal digital integration. These early machines—infusion pumps run by basic timers, manual defibrillators, or single-function monitors—provided essential care functions that were largely isolated from external influence. Cyber risk was almost nonexistent, as physical proximity and specialized technical access were necessary prerequisites for sabotage or malfunction.

The transformative turning point emerged with the embedding of microprocessors, memory, and software-based controls into medical hardware. Software-driven functionalities facilitated more advanced signal processing, improved diagnostics, and tailored therapy delivery. For instance, patient monitors evolved to provide real-time waveform analysis and customizable alarm parameters, while infusion pumps began supporting programmable dosing and interoperability with electronic medication orders. This new paradigm enabled clinical advancements

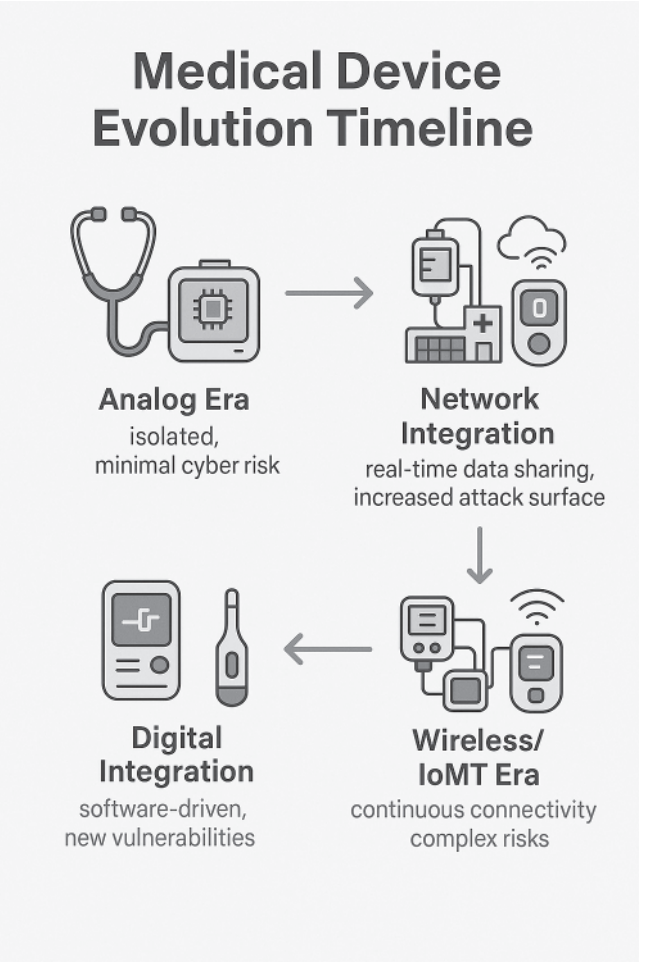
but simultaneously introduced layers of hidden complexity and interdependence—each module, driver, and software library now represented a potential vector for error or exploitation.

These new capabilities set the stage for the next era: comprehensive system integration across local networks and enterprise IT environments. Medical devices, formerly independent, now share data with centralized workstations and electronic health record systems, allowing clinicians to monitor multiple patients in real time, share diagnostics instantaneously, and synchronize care interventions between modalities. The sophistication of such integrations is seen in ICUs, where multiparameter monitors, networked ventilators, and infusion stations deliver harmonized care routines. This interconnectedness advances safety and efficiency, allowing collaborative intervention and seamless escalation of care, but at the expense of new and consequential cybersecurity dependencies (Ahmed et al., 2023).

The expansion of wireless networking—using protocols like Wi-Fi and Bluetooth—ushered in continuous, location-independent data flow. Hospital settings now support mobile carts, wearable telemetry units, and remote-controlled imaging systems, while ambulatory and home-based applications rely on Internet of Medical Things (IoMT) architectures to relay vital data between patient, provider, and caregiver. For example, wireless pacemakers transmit rhythm logs to cloud analytics platforms, and network-enabled infusion pumps receive remote programming and alerts from care teams. This heterogeneity in device make and network protocols enables distributed, proactive care but at the same time complicates risk modeling and incident response. With such pervasive connectivity, patient safety has become increasingly contingent on secure wireless communication, meticulous endpoint management, and system-wide visibility into network activity (Ahmed et al., 2023).

Each incremental network connection inherently increases the attack surface. Where once a device needed to be physically accessed to be compromised, now adversaries can potentially exploit any exposed communication channel. The multitude of interfaces—ranging from proprietary device protocols, standard service discovery mechanisms, and remote firmware update services—multiplies the opportunities for exploitation. Multimodal monitors that combine electrocardiogram (ECG), pulse oximetry, and blood pressure sensors rely on continuous network presence, creating multiple vectors for adversaries to disrupt or manipulate clinical data. Wireless-enabled imaging systems may expose authentication weaknesses or contain errors in third-party communication stacks, as seen in several high-profile vulnerability disclosures in recent years. Each new connectivity layer augments clinical capacity but also requires an equivalent increase in security diligence (*A Review on the Security Vulnerabilities of the IoMT against Malware Attacks and DDoS*, 2019).

The migration toward firmware and software-centric design not only is about flexibility but also forms the operational core of every contemporary medical device. The move away from fixed-function, hardware-driven controls allows remote update capability, the addition of new features, and rapid deployment of clinical improvements. However, this dynamic environment transforms risk management into an ongoing obligation; a single software bug or misconfiguration can render devices nonfunctional or, worse, dangerous to patients. In practice, an exploitable flaw in networked pacemaker firmware may require urgent patching across thousands of deployed units—highlighting the operational, clinical, and regulatory complexities tied to secure update mechanisms (*A Review on the Security Vulnerabilities of the IoMT against Malware Attacks and DDoS*, 2019).



All these technological advances have contributed to the increasing intricacy of medical device ecosystems. The result is not just a growth in technical sophistication but a fundamental transformation in attacker strategy and defender responsibility. Cyber adversaries now target chains of interconnected endpoints, seeking vulnerabilities in software, configurations, or overlooked protocol layers. The attack surface has multiplied, bringing with it a diversity of threat actors—from opportunistic malware campaigns to targeted ransomware and sophisticated state-sponsored attacks.

The convergence of complexity, interconnectivity, and dynamic software controls has indelibly changed the risk environment for medical devices. This ever-widening attack surface has not only heightened the need for specialized incident response but also opened the door to a more diverse array of adversaries and motives, which will further inform the evolving approaches to healthcare cybersecurity.

Hidden Threats: Attackers in the Shadows

Advances in digital technology have blurred the boundaries between clinical care and computational systems. Medical devices once isolated from the outside world are now deeply woven into hospital networks, managing everything from vital monitoring to automated drug delivery. However, with increased network integration comes an enlarged attack surface. Adversaries with varied motivations can exploit device vulnerabilities, making it critical to recognize the distinct groups and ideological forces that drive such attacks—and the practical risks they pose to patient safety and healthcare operations.

Malicious Hackers and Cybercriminal Groups

Malicious hackers—ranging from independent actors to highly organized collectives—are often drawn by the lure of financial profit, widespread notoriety, or a simple urge to disrupt. Their attacks frequently begin with identifying weak points in device integration: default passwords on infusion pumps, unpatched vulnerabilities in MRI machines, or unsecured wireless telemetry. These avenues allow unauthorized access, which can be weaponized for data theft, operational disruption, or extortion.

Financially motivated attacks frequently focus on ransomware, leveraging the urgent, life-critical nature of hospital services. For example, cybercriminals might deploy specialized ransomware to target a fleet of networked insulin pumps, rendering them inoperable and demanding payment for restoration. Other attacks employ sophisticated phishing schemes to steal credentials granting access to imaging or diagnostic devices, ultimately allowing attackers to exfiltrate protected health information to sell on dark web marketplaces (He et al., 2021; Riggi, 2020). There are also disruptive campaigns designed to demonstrate the hacker's technical prowess: disabling ventilators during a public health crisis or manipulating device firmware to call attention to security gaps. Even when such actions are not politically motivated, they carry profound consequences for patient health and trust in medical technology (He et al., 2021).

State-Sponsored Threats and Advanced Persistent Adversaries

State-sponsored malicious actors—often referred to as advanced persistent threats (APTs)—operate under government directives, seeking rewards beyond mere profit. Their objectives might include sabotaging rival nations' healthcare infrastructure, collecting sensitive health data for intelligence purposes, or undermining public confidence in national health systems during pandemics. State actors can invest significant resources into uncovering zero-day vulnerabilities or crafting custom malware designed to evade detection.

The infamous WannaCry outbreak, attributed to North Korean sponsorship, stands as a striking example of this class of adversary: hospitals across Europe and Asia endured widespread device outages, diagnostic delays, and forced patient diversions when ransomware disabled everything from imaging devices to basic patient records systems (Riggi, 2020). Russian-backed adversaries have unleashed ransomware with destructive payloads, lacking even the possibility of decryption, while Iranian groups have targeted research facilities to pilfer intellectual property for government

use (Riggi, 2020). In each case, the underlying motivations are geopolitical, whether to inflict harm, gain strategic advantage, or retaliate for sanctions. These actors often work methodically over long periods, embedding spyware or backdoors in devices, gathering intelligence over months or years with carefully staged operations.

The Insider Threat

Insider threats compound the risk landscape, as those with legitimate access—such as clinical staff, IT consultants, or contract technicians—can intentionally or inadvertently trigger catastrophic vulnerabilities. Insider actions may be rooted in grievances, a desire for financial gain, or simple carelessness. For example, an employee might download unauthorized software onto a hospital workstation, unintentionally introducing malware that propagates to dozens of connected medical devices. Inadequate security training and insufficient oversight allow such risks to persist (He et al., 2021).

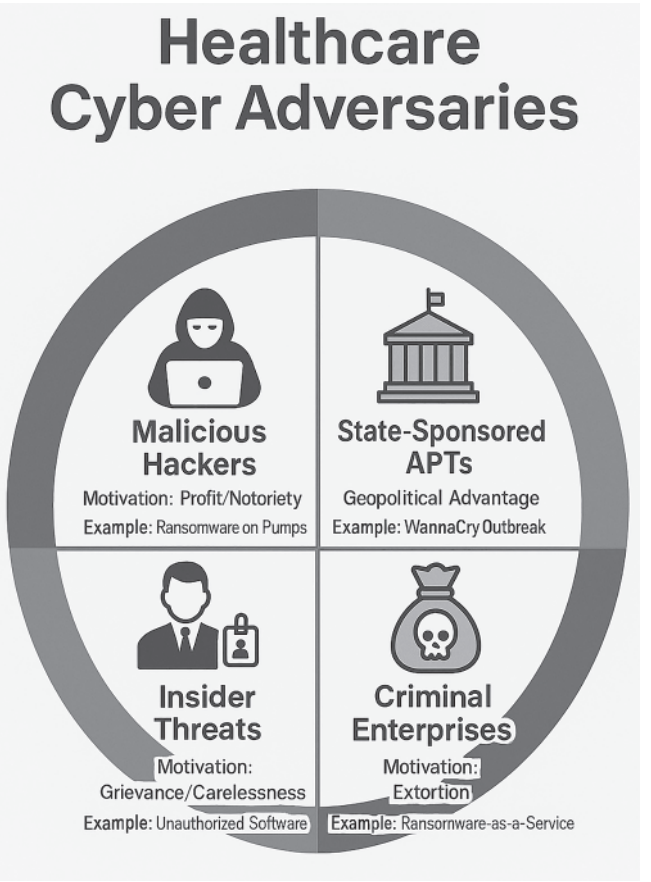
At a more grave extreme, disgruntled insiders with elevated privileges can intentionally sabotage device functionality. By exploiting poorly managed access controls or overlooked audit logs, they might disable alarm features in life-sustaining ventilators or alter medication delivery settings to dangerous levels. Mistakes can also have devastating outcomes: a contractor who accidentally deletes a critical firmware update from a shared server could prevent essential devices from receiving patches, leaving known vulnerabilities open to exploitation. As the medical cyber-physical environment grows more intricate, human error and negligence become increasingly consequential (He et al., 2021).

Criminal Enterprises and Extortion Specialists

Organized crime syndicates have discovered that hospitals represent high-value, vulnerable targets. Unlike traditional enterprises, healthcare organizations cannot easily pause operations. Criminal enterprises exploit this operational pressure by locking down critical assets, including medical devices, through ransomware and threatening to release or destroy sensitive data unless large ransoms are paid. These attackers operate with the knowledge that disruptions can jeopardize patient lives, using this leverage to maximize financial returns (He et al., 2021; Riggi, 2020).

Criminal groups may operate on a "ransomware-as-a-service" basis, offering sophisticated malware toolkits to lesser-skilled actors who wish to extort healthcare institutions. In some cases, ransomware campaigns are so thoroughly orchestrated that criminals systematically disable redundant systems, backup devices, and network segments to ensure compliance with their demands. The result is a systemic risk not just to individual hospitals but to the continuity of entire health systems, as witnessed during coordinated attacks that paralyzed emergency care and canceled thousands of appointments worldwide (He et al., 2021; Riggi, 2020).

The prevalence of these adversaries is not simply the product of growing connectivity but of misconceptions that system architecture or proprietary technology will deter sophisticated attackers. In reality, such assumptions foster complacency, leaving critical vulnerabilities exposed to all categories of motivated adversaries, setting the stage for deeper exploration into why secrecy alone offers little true protection.



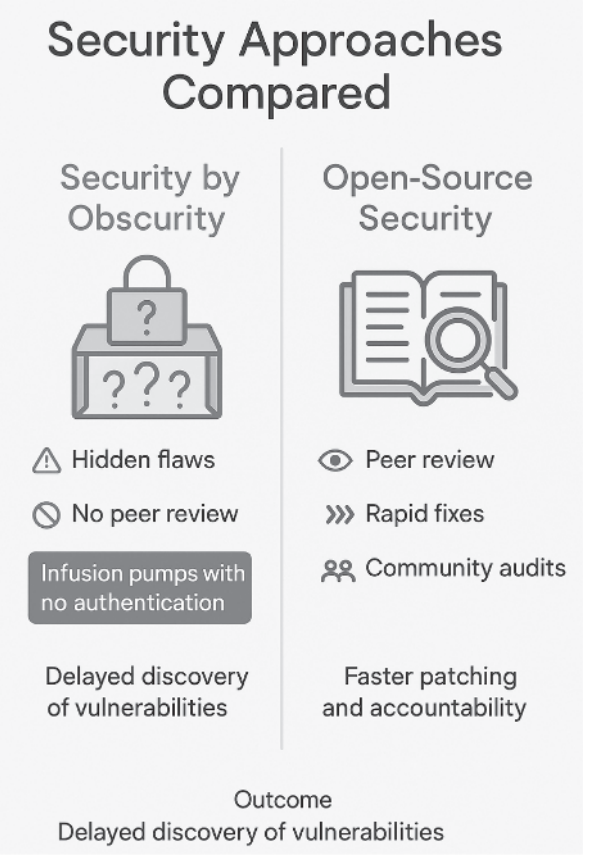
The Myth of Security by Obscurity in Medical Devices

For many years, manufacturers of medical devices relied on the belief that simply hiding the workings of their products or keeping software proprietary would provide sufficient security. This meant that as attacks grew more sophisticated, the industry continued to depend on secrecy and obscure code as its main line of defense, assuming that attackers would struggle to exploit what they could not see. However, this reliance on obscurity as a means to achieve security has created fertile ground for risky complacency. Advanced adversaries consistently exploit weaknesses that stem from overconfidence in proprietary systems rather than real, tested defense mechanisms.

The notion that security is guaranteed through an undisclosed or nonpublic design often leads engineers and developers to overlook rigorous testing or comprehensive protective strategies. Proprietary systems can mask unexamined vulnerabilities simply because they are hidden from public scrutiny. Companies sometimes view security more as a marketing claim than a design imperative, since the internal workings remain invisible to most users and regulators unless a serious incident occurs. This approach not only stifles meaningful evaluation and improvement but also enables dangerous gaps to persist. For example, device manuals and certification documents routinely divulge technical details about frequency use and transmission protocols, providing adversaries with enough data to mount informed attacks, even when the underlying source code remains closed (Williams & Woodward, 2015).

In practice, the myth of obscurity fails because attackers do not respect the artificial walls set up by proprietary designs. They deploy sophisticated techniques to reverse engineer devices, even without official access to design files. Extraction and analysis of firmware is one of the most common approaches. Attackers frequently use tools such as Joint Test Action Group (JTAG) debuggers and disassemblers to pull binary code directly from hardware or memory chips. Once extracted, this code can be decompiled and painstakingly teased apart to reveal how the device operates. Security vulnerabilities—such as hardcoded credentials, unencrypted data transfers, or weak authentication protocols—often become apparent after just a few hours or days of analysis by a skilled researcher or malicious hacker. Public reports of vulnerabilities routinely surface through independent discovery, not through voluntary disclosure by manufacturers. This makes clear that hiding technical details does little to delay or prevent determined adversaries from uncovering flaws.

Concrete examples of failed obscurity abound within the healthcare sector. Medical infusion pumps, which regulate lifesaving medications, have been found with embedded web services that completely lack authentication or encryption. Attackers have demonstrated how networked pumps can be manipulated remotely, even from outside hospital boundaries (Williams & Woodward, 2015). In another public case, researchers at the University of Michigan's Archimedes Center successfully compromised pacemakers and insulin pumps by exploiting radio interfaces intended for routine device management. In these scenarios, vulnerabilities such as default passwords, poorly protected wireless links, and undocumented maintenance functions were exposed through sheer determination and technical skill—none of which required original design documents.



Historically, manufacturers have sometimes discovered faults in their proprietary devices but failed to share them with clinicians or regulators. The tragic case of a 21-year-old man who died when his implantable defibrillator short-circuited highlights this problem. The manufacturer, Guidant, first noticed the flaw several years earlier and made undisclosed corrective changes in production but neglected to notify the public or medical professionals. This incident triggered the recall of 70,000 devices—only after fatal consequences brought the problem to light (*Killed by Code: Software Transparency in Implantable Medical Devices—Software Freedom Law Center*, 2010). Such secrecy delays both warnings and solutions, exposing patients to unacceptable risks.

Open-source security strategies present a sharp contrast. When code is visible and available for independent analysis, researchers, developers, and even concerned end users can collectively examine and test devices for vulnerabilities. Peer review provokes rapid detection and correction of flaws that might otherwise remain dormant in closed systems. Open standards create uniformity and allow different products to work together, improving safety and simplifying compliance. Community-driven security audits and independent bug reports foster a culture of accountability beyond what closed, proprietary design can achieve. Industry regulators and advocacy organizations have increasingly pointed to transparent models as offering defense-in-depth and more timely patching of discovered vulnerabilities. Large open-source projects have established quality controls to ensure that only trusted code is adopted, stopping malicious or untested changes before they can endanger end users (*Killed by Code: Software Transparency in Implantable Medical Devices—Software Freedom Law Center*, 2010).

As reliance on embedded medical technology deepens, the limitations of obscurity in ensuring patient safety become more obvious and dangerous. Lessons from the past—including preventable fatal incidents—demonstrate that the ethical and professional requirements of device security cannot be met by secrecy alone. The stakes are high: unreliable devices put lives at risk, and when patient safety depends on technology, every aspect of protection must be open to verification, challenge, and improvement. Accountability begins not with the promise of hidden defenses but with clear, responsible, and community-supported security principles. The ongoing evolution of medical devices compels those who design, test, and deploy them to prioritize transparency—the only enduring foundation for trust and safety in modern healthcare (*Killed by Code: Software Transparency in Implantable Medical Devices—Software Freedom Law Center*, 2010; Williams & Woodward, 2015).

Unethical Complacency: Why Excuses Won't Suffice

Failures in the security of medical technology create a silent but dangerous gap between what designers intend and what patients and clinicians truly experience. When engineers and organizations tacitly believe that obscurity is enough to protect network-connected medical devices, they risk more than technical vulnerabilities. They invite moral and legal consequences that stretch far beyond the boundaries of code. Trust in "hidden" systems, instead of verified protections, can mask deep flaws in design, exposing patients to harm and organizations to liability. A misplaced confidence in obscurity reflects a deeper breach—a lapse in professional duty to the people whose lives depend on these technologies.

As medical devices link to hospital networks or cloud platforms, threats multiply and new vulnerabilities emerge. Device manufacturers who dismiss the urgency of patch management, encryption,

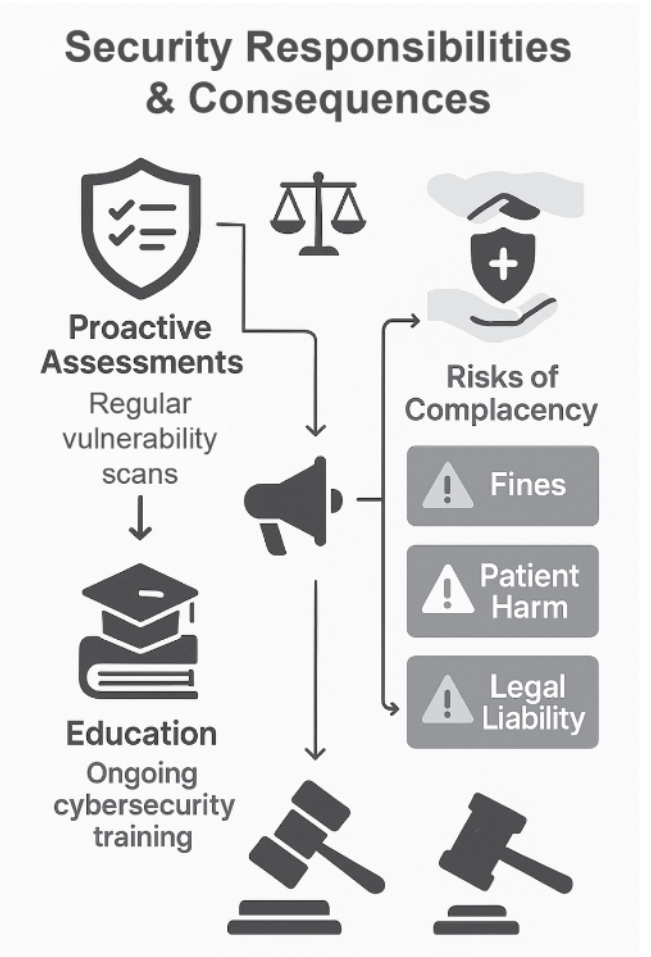
or routine risk assessment place patients at risk of harm to both privacy and property. The harm goes beyond technical failure: compromised devices can interrupt life-sustaining therapy, expose sensitive health records, or offer an entryway for ransomware threats. Neglecting available security updates violates not only industry best practices but also legal mandates like the General Data Protection Regulation's Article 32, which requires immediate action to mitigate known vulnerabilities (Dhirani et al., 2023). Inaction is not a victimless oversight—it can lead to massive regulatory fines and, more critically, patient endangerment.

The professional responsibility to secure medical devices is not theoretical; it is rooted in the lived reality of modern medicine. Every software update, configuration decision, and incident response plan can mean the difference between continuity of care and catastrophic failure. Engineers and developers hold a duty of care, accountable not solely to their employer or the letter of the law but to those relying on every breath, heartbeat, or dose a device controls. This ethical obligation cannot be contracted away or diminished by ignorance (Augusta University, 2024). Medical device security is a direct extension of the Hippocratic principle: do no harm. Skirting these responsibilities is not merely a lapse in technical judgment but a breach of a professional standard that prioritizes human life.

Healthcare organizations and device manufacturers are required to embrace a proactive stance that treats security as fundamental to patient care. Such a stance involves regular vulnerability assessments, robust firewalls, and continuous monitoring for signs of intrusion (Augusta University, 2024). It also demands swift and transparent disclosure of discovered breaches. The Consolidated Appropriations Act of 2022, for example, instructs companies to report known cyber incidents within 72 hours of identification, reinforcing the significance of rapid and open communication for mitigating harm (Augusta University, 2024). Transparency and disclosure—whether about vulnerabilities or successful attacks—are acts of moral leadership. They empower clinicians, patients, and technical teams to take informed, risk-reducing actions.

The idea that lack of expertise excuses poor security simply does not hold up under scrutiny. The professional duty to learn is as essential as the obligation to care. Ongoing education and systematic professional development in cybersecurity are basic requirements, not aspirational goals, for responsible participation in developing or operating life-critical medical devices (Dhirani et al., 2023). Real-world cases have shown that organizations often face severe penalties or lawsuits when they fail to patch known flaws in devices, especially when those lapses result in patient harm or widespread data exposure. For instance, when a manufacturer decided to defer installing a critical patch in hospital software to avoid immediate inconvenience, they violated both the spirit and the letter of safety regulations—a choice explicitly condemned under General Data Protection Regulation (GDPR) statutes (Dhirani et al., 2023).

Concrete accountability mechanisms are necessary to demand and ensure safe practices in medical device security. Manufacturers and healthcare providers face product liability claims, where courts have held that reasonably foreseeable vulnerabilities must be addressed or else be grounds for legal action. Regulatory authorities impose fines and can even revoke approvals when organizations conceal incidents or neglect mandated security controls (Augusta University, 2024; Dhirani et al., 2023). Strong incident reporting systems and clear internal channels for raising security concerns allow organizations to learn from mistakes instead of repeating them. A culture encouraging transparency and learning—rather than blame and silence—becomes the bedrock of trust and continual safety improvement.



Patients trust that every step has been taken to secure the technologies their lives depend on. Upholding this trust means medical device professionals must reject complacency. They must act promptly to address known risks and commit to lifelong learning about emerging threats (Augusta University, 2024; Dhirani et al., 2023). Promoting ethical practices in cybersecurity is not merely about compliance, it is about protecting dignity, privacy, and life itself. Each decision—action or indecision—contributes to a shared culture that defines whether medicine will remain a source of safety and hope in an increasingly digital world.

Final Insights

Recognizing the profound human risks posed by medical device vulnerabilities and the complex, interconnected nature of modern healthcare technology compels us to adopt a comprehensive, transparent approach to cybersecurity. Now that we understand the limitations of security through obscurity and the diversity of adversaries targeting these critical systems, it is clear that safeguarding patient safety demands more than reactive fixes—it requires embedding robust security practices throughout device design, deployment, and ongoing management.

Healthcare professionals, engineers, regulators, and researchers must collaborate closely to develop resilient architectures, prioritize timely vulnerability disclosure and patching, and foster a culture of continuous learning and ethical responsibility. By doing so, we can build medical device ecosystems that not only withstand evolving cyber threats but also uphold the highest standards of accountability, ensuring trust and protection for patients in an increasingly digital healthcare environment.

References

A Review on the Security Vulnerabilities of the IoMT Against Malware Attacks and DDoS. (2019). Arxiv.org. https://arxiv.org/html/2501.07703v1.

Ahmed, S. F., Alam, M. S. B., Afrin, S., Rafa, S. J., Rafa, N., Gandomi, A. H. (2023, September 29). *Insights into Internet of Medical Things (IoMT): Data Fusion, Security Issues and Potential Solutions*. Information Fusion. https://doi.org/10.1016/j.inffus.2023.102060.

Aldosari, B. (2025, May 6). *Cybersecurity in Healthcare: New Threat to Patient Safety*. Media LLC; Cureus; Springer Science and Business. https://doi.org/10.7759/cureus.83614.

Augusta University (2024). *Cybersecurity Ethics: What Cyber Professionals Need to Know*. Cybersecurity Ethics: What Cyber Professionals Need to Know. https://www.augusta.edu/online/blog/cybersecurity‐ethics.

Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., Newe, T. (2023, January 19). Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. Sensors. https://doi.org/10.3390/s23031151.

Elendu, C., Omeludike, E. K., Oloyede, P. O., Obidigbo, B. T., Omeludike, J. C. (2024, September 27). *Legal Implications for Clinicians in Cybersecurity Incidents: A Review*. Medicine; Wolters Kluwer. https://doi.org/10.1097/md.0000000000039887.

He, Y., Aliyu, A., Evans, M., Luo, C. (2021). Healthcare Cyber Security Challenges and Solutions Under the Climate of COVID19: A Scoping Review. Journal of Medical Internet Research; ncbi. https://doi.org/10.2196/21747.

Killed by Code: Software Transparency in Implantable Medical Devices—Software Freedom Law Center. (2010, July 22). Softwarefreedom.org. https://softwarefreedom.org/resources/2010/transparent-medical-devices.html.

Riggi, J. (2020). *Ransomware Attacks on Hospitals Have Changed | Cybersecurity | Center | AHA*. Www.aha.org. https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed.

Williams, P., Woodward, A. (2015, July). *Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem*. Medical Devices: Evidence and Research. https://doi.org/10.2147/mder.s50048.