Testimony of

Michelle Jump
Chief Executive Officer

of

MedSec LLC

on

Aging Technology, Emerging Threats:
Examining Cybersecurity Vulnerabilities in Legacy Medical Devices

Before the

United States House of Representatives

Committee on Energy and Commerce

Oversight and Investigations Subcommittee

April 1, 2025

Introduction

Chairman Palmer, Ranking Member Clarke, and members of the Committee, my name is Michelle Jump. I am the Chief Executive Officer of MedSec, a consulting and technical services firm focused on medical device and healthcare cybersecurity.

I appear before you today to share my perspective as someone who has spent the past 15 years helping organizations understand and navigate the introduction of emerging technologies in the medical device industry. Over that time, I have witnessed the industry move from initial recognition to full embrace of the promise that connected technologies bring—not only in making healthcare delivery faster, more efficient, and more accurate, but also in recognizing the new risks these innovations introduce.

As we connect more medical devices across hospitals, homes, and care centers, we also expose those systems to new threats. One such unexpected and significant threat is to the cybersecurity of our critical healthcare infrastructure.

As a regulatory and quality expert—not a technical one—my focus has not been on how to integrate or defend these technologies, but on understanding how innovation can unintentionally introduce risk even as it aims to provide solutions. This is the tradeoff we must manage in exchange for the benefits of connected technology.

Throughout my career, I have served as an active member and leader in numerous industry working groups, standards committees (both domestic and international), and trade associations. My life's work has been dedicated to ensuring that these critical technologies can be safely and securely integrated into the healthcare system—delivering on their promise to support clinicians in providing the highest quality patient care.

We appreciate the Committee convening this timely hearing to examine cybersecurity in the health sector, particularly as it relates to medical technology. Today, my testimony will focus on how cybersecurity in the medical device industry is currently regulated, and how we—as a collective of stakeholders—can work together to make the adoption of emerging technologies safer and more secure for the patients and healthcare providers who rely on them.

Today, I will cover seven areas of consideration on this topic:

First, a brief overview of how the increased utilization of connected technology in the health sector increases cyber risk;

Second, a review of the regulatory expectations for cybersecurity in medical devices and how the industry has responded to increasing cybersecurity expectations;

Third, a discussion of the cybersecurity challenges of the healthcare delivery organizations (e.g. hospitals);

Fourth, an explanation of the risk transfer process where the risk management of legacy medical devices moves from the medical device manufacturer (MDM) to the healthcare delivery organization (HDO);

Fifth, a review of how the health sector is targeted for cyber attacks;

Sixth, a description of the need to address the gap in qualified and trained cybersecurity professionals to support the health sector; and

Seventh, a summary of recommended actions to aid in the reduction of risk to the health sector from cybersecurity threats, subdivided into categories of Industry-wide, MDM, HDO, Suppliers, and Regulators.

About MedSec

As a global leader in medical device product security, MedSec drives industry wide improvements to the practice of medical device and healthcare security by providing a comprehensive range of cybersecurity services—including regulatory consulting, program and process development, workforce training, and technical services such as penetration testing and threat modeling. While MedSec is a smaller, boutique firm, when considering the combined revenue of our clients, we represent over 70% of the global medical device industry, by serving the full spectrum of medical device manufacturers from global corporations to start-ups.

In addition to its work with medical device manufacturers, MedSec is also deeply engaged in strengthening cybersecurity across the broader healthcare ecosystem through the participation in working groups, standards, and conferences. We partner closely with clients to help address their most pressing cybersecurity challenges, improve organizational resilience, and build long-term capacity for managing risk in an increasingly connected healthcare environment.

How Digital Integration Has Increased Cyber Risk in Healthcare

Over the past few decades, the healthcare environment has transformed significantly. What was once a largely paper-based system with standalone medical devices has evolved into a highly interconnected ecosystem. Today’s healthcare relies heavily on modern, networked medical device systems that share and depend on digitally stored data. Paper charts have been replaced by electronic health records (EHRs), and medical devices are increasingly softwaredriven. The once-clear boundaries between devices, systems, and data flows are rapidly disappearing.

As a result, healthcare delivery has adapted to embrace this new level of integration. EHRs are now the standard, and medical devices routinely transmit information across the care environment. These components work together in real time to support clinical workflows. For example:

- Medical devices located in patient rooms or at the bedside now communicate directly with central nursing stations. This allows fewer staff to safely monitor more patients.
- Devices are increasingly designed to transmit data directly into EHR systems, reducing staff workload. Some are even beginning to receive data from EHRs to preconfigure settings and improve workflow efficiency.
- Diagnostic imaging devices send images to radiologists for faster review, eliminating the need for on-site interpretation. Both images and results can be uploaded directly to the EHR.
- Implanted and wearable devices now connect to patients' smartphones to monitor performance and treatment. These devices also transmit data to clinicians, enabling timely follow-ups or urgent interventions when needed.

These are just a few examples of how healthcare technology has evolved—and how deeply dependent it has become on connectivity. A cybersecurity incident can significantly disrupt this interconnected environment. For example, a ransomware attack that disables hospital networks—or leads to systems being shut down as a precaution—can force immediate, resource-intensive changes to clinical workflows and staffing.

Hospitals may need to:

- Increase the number of nurses to manually monitor patients at the bedside
- Manually enter data into EHRs or revert to paper-based documentation, a time-consuming process
- Require radiologists to interpret images on-site or manually transfer imaging files
- Conduct in-person follow-ups for patients with implanted or wearable devices due to lost remote monitoring capabilities

In addition, if one facility is compromised and must divert patients, surrounding hospitals must be prepared to accommodate unexpected surges in patient volume.

Medical Devices

Medical devices have undergone significant transformation over the past several decades, incorporating new technologies to better serve both patients and healthcare providers. Historically, these devices were primarily hardware-based. Over time, however, they evolved to include software, connectivity to networked infrastructure and electronic health records (EHRs), and integration with commercial technologies such as Bluetooth and cloud service providers. This shift has significantly expanded the risk landscape for medical devices, particularly in terms of cybersecurity.

For over a decade, the FDA has been steadily raising the bar on cybersecurity expectations as part of its regulatory oversight. The agency released its first final premarket cybersecurity guidance in 2014[1], followed by postmarket cybersecurity guidance in 2016[2]. These documents emphasized that cybersecurity is a shared responsibility across the healthcare sector and urged manufacturers to consider security early in the design process as well as throughout postmarket device management.

While progress was being made under this framework, the rising frequency of ransomware attacks on hospitals, and increasing instances of medical devices being affected, led the FDA to call for explicit cybersecurity authority in its 2018 Medical Device Safety Action Plan[3].

A significant advancement came with the enactment of the Food and Drug Omnibus Reform Act (FDORA)[4], which granted the FDA new authority through the addition of Section 524B to the Food, Drug, and Cosmetic Act and went into effect on March 29, 2023. This provision establishes explicit cybersecurity requirements for medical devices undergoing marketing authorization. In parallel, the FDA issued updated premarket cybersecurity guidance

[1] U.S. Food and Drug Administration (FDA). (2014). *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* (Guidance for Industry and Food and Drug Administration Staff). Center for Devices and Radiological Health. October 2, 2014

[2] U.S. Food and Drug Administration (FDA). (2016). *Postmarket Management of Cybersecurity in Medical Devices* (Guidance for Industry and Food and Drug Administration Staff). Center for Devices and Radiological Health. December 28, 2016

[3] U.S. Food and Drug Administration (FDA). (2018). *Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health*. Center for Devices and Radiological Health. April 2018

[4] U.S. Congress. (2022). *Food and Drug Omnibus Reform Act of 2022*, Division F of the *Consolidated Appropriations Act, 2023*, Pub. L. No. 117-328, 136 Stat. 4459, 5689–5740 (Dec. 29, 2022)

entitled Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions[5].

FDA's implementation of these new legislative authorities and FDA Guidance has balanced the needs of patients by continuing to authorize innovative technologies while also holding manufacturers accountable for devices that simply carry too many cybersecurity risks.

These strengthened authorities and clearer expectations have already begun to drive meaningful changes across the medical device industry. Although often prompted by regulatory pressure during the submission process, manufacturers are increasingly shifting their mindset. Where once there was a willingness to "take their chances" with minimal cybersecurity integration, many now proactively ask, "What do we need to do?"

Some manufacturers have already been adapting, making substantial internal changes to embed cybersecurity into their organizational culture and business practices. However, lasting impact depends on continued leadership support, as such changes take time to fully mature and become part of the lasting culture within the organization.

Importantly, these cybersecurity expectations apply not only to new devices but also to existing devices undergoing modifications that require resubmission to the FDA.

The FDA has started to implement and, in some instances, require submissions to be provided to the Agency with their electronic submission template (eSTAR). This template is

[5] U.S. Food and Drug Administration (FDA). (2023). *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions* (Final Guidance). Center for Devices and Radiological Health. September 27, 2023

dynamic and based on how information is entered, can enforce sections to be completed and that documentation is attached and/or certain questions are answered to allow the submission to proceed. If a manufacturer is missing information, the manufacturer cannot submit their application. The eSTAR barrier to submission entry is an important deterrent to "throw documents at the wall and see what FDA reacts to." It raises the general incentive to provide solid documentation from the start so that they do not delay the start of their submission process. All products going through submission due to modification, regardless of whether that modification is related to cyber, must meet the current cybersecurity "bar" set by the FDA. Companies respond to this.

As medical device manufacturers continue to mature their cybersecurity programs and strengthen the protections within their products, market pressure is also playing a growing role. Hospitals and healthcare systems are placing greater importance on cybersecurity when making purchasing decisions. Increasingly, strong security features are seen as a market differentiator, while poor or absent security can be a dealbreaker. Hospitals can further drive this trend by establishing and consistently enforcing robust cybersecurity requirements in their procurement processes.

Healthcare Delivery Organizations

Cybersecurity practices at the hospital, including a commitment to maintaining secure devices, and the environment medical devices operate in are equally important. Maintaining a secure environment for hospital networks is a shared responsibility between healthcare delivery organizations (hospitals), health IT companies/EHR vendors, makers of operating systems and other software infrastructure, end users, and medical device manufacturers.

Healthcare Delivery Organizations (HDOs) have faced similar technological evolutions as medical devices have depended on more connectivity and advanced technology. The healthcare environment has become increasingly interconnected between medical devices, electronic health records, their networks, billing systems, pharmaceutical order systems, Laboratory Information Systems, imaging systems, and cloud environments. As discussed earlier, cybersecurity incidents in this connected environment can significantly impact delivery and timeliness of clinical care unless additional, qualified personnel are available to staff the disconnected workflow. They also have general operational environment cybersecurity risks from connected elevators, HVAC systems, hosting Wi-Fi networks, etc.

The rapid adoption of connectivity within HDOs has, in many cases, outpaced comprehensive cybersecurity planning. As a result, many healthcare facilities have not yet fully assessed or addressed all vulnerabilities in their connected environments. In recent years, however, there has been an increased focus on strategies such as network segmentation, which can help limit the impact of cyber incidents and improve the overall security posture of healthcare systems.

Risk Transfer: The Path to Legacy

As medical devices age and can no longer be effectively secured against modern cybersecurity threats, they enter a lifecycle stage known as End of Support (EOS). At this point, the device's manufacturer or software providers cease offering updates, security patches, and technical assistance. This typically occurs when key components—such as the operating system—are no longer supported, or when the underlying technology becomes obsolete and cannot be reasonably upgraded or maintained.

If a Healthcare Delivery Organization (HDO) chooses to continue using the device beyond this point, there are no current regulations that prohibit doing so. However, the responsibility for managing the cybersecurity risk associated with continued use of that device is transferred from the manufacturer to the HDO. This transition of responsibility is known as risk transfer.

Risk transfer is not a passive event, it is a formal process that requires deliberate actions and informed decision-making. Continued safe use of legacy medical devices depends on the HDO's ability to assess, document, and manage the security risks introduced by the device. This includes implementing compensating controls, conducting regular risk assessments, monitoring device behavior, and isolating the device from other networked systems where necessary.

This process has been well-documented in industry guidance, including the *Health Sector Coordinating Council's (HSCC) Health Industry Cybersecurity - Managing Legacy Technology Security (HIC-MaLTS*) and the International Medical Device Regulators Forum (IMDRF) guidance *Principles and Practices for the Cybersecurity of Legacy Medical Devices*[6]. These documents offer frameworks for risk management when legacy systems remain in use, outlining the actions HDOs should take to minimize potential harm to patients and disruption to clinical workflows.

However, the effectiveness of risk transfer relies heavily on the maturity of the HDO's internal processes and the availability of appropriately trained personnel. Not all healthcare organizations are equally equipped to take on this added responsibility. In particular, small, rural, or resource-constrained hospitals may lack the cybersecurity staff, asset inventory systems, or governance structures needed to safely manage legacy device risks.

This growing challenge highlights the need for:

- Standardized processes for managing EOS medical devices across HDOs;
- Investment in workforce development, including training for clinical engineering and cybersecurity personnel responsible for legacy device oversight; and
- Improved collaboration between manufacturers and HDOs to ensure transparency around device support lifecycles and to enable proactive planning for EOS transitions.

As healthcare technology continues to evolve rapidly, the accumulation of unsupported legacy devices within hospital environments presents a serious long-term risk. Without adequate processes in place to manage risk transfer, patient safety and operational continuity may be compromised. There is an opportunity for regulatory bodies, industry stakeholders, and healthcare providers to work together to develop more robust mechanisms for handling legacy device risk, ensuring that continued use of older technology does not come at the cost of cybersecurity or clinical effectiveness.

Who's the Target?

Medical device cybersecurity is frequently covered in the media and is often a focal point in discussions about the broader cybersecurity posture of the healthcare sector. A history of notable gaps in cybersecurity controls, along with high-profile reports highlighting serious vulnerabilities, has drawn scrutiny to medical devices in general as potential threats to critical healthcare infrastructure.

However, while medical devices attract significant attention, the most common and impactful cybersecurity threat facing hospitals—**ransomware**—rarely originates from the devices themselves. Typically, ransomware is designed to be introduced into hospital networks through human error, such as an employee clicking on a malicious link in a phishing email. Once inside the network, the malware can spread laterally. If medical devices are not adequately secured or segmented, they too can become infected or disrupted, compounding the impact of the attack.

This raises an important question: Does this mean that medical device security is less important? The answer is unequivocally no. Instead, it highlights the complexity of the issue and the extent to which cybersecurity must be treated as a shared responsibility. The security of a medical device when it leaves the manufacturer, right out of the box, is just one piece of a much larger puzzle. The cybersecurity practices of the Healthcare Delivery Organization (HDO), including how they maintain, configure, and manage medical devices within their operating environment, are equally critical to overall system security. Additionally, insecure medical devices can serve as entry points into the hospital, particularly those connectable to external systems.

Manufacturers can and should continue to be held to high standards for building secure devices, standards reinforced by recent legislative and regulatory changes such as Section 524B of the Food, Drug, and Cosmetic Act. However, even the most secure device can be exploited if it is placed into an unprotected or under-resourced environment. Hospitals, especially those with limited funding, often lack the financial and personnel resources to replace aging equipment or maintain sophisticated cybersecurity programs. As a result, legacy devices—known to have vulnerabilities—remain in active use not because of negligence, but due to a lack of alternatives.

Thus, ensuring that hospitals have access to secure technologies and that manufacturers maintain and update device security throughout the product lifecycle is essential but not sufficient on its own. Medical Device Manufacturers (MDMs) play a crucial role, but systemic underinvestment in cybersecurity at certain hospitals, particularly smaller or rural hospitals, remains a significant barrier to meaningful risk reduction.

Addressing this challenge requires a coordinated approach that includes:

- Supporting HDOs in building secure digital environments,
- Providing technical and financial assistance to enable device upgrades and secure network architectures,
- Ensuring manufacturers maintain security support throughout a product's lifecycle, and
- Continuing to reinforce the shared nature of responsibility between manufacturers, hospitals, and the broader healthcare system.

Ultimately, medical device cybersecurity cannot be effectively addressed in isolation. It must be part of a holistic strategy that recognizes the interdependence between devices, healthcare infrastructure, and the broader threat landscape. Regulatory guidance, targeted funding, and strong cross-sector collaboration will all be essential in helping hospitals keep pace with evolving cyber threats and protecting patient safety.

Missing Voice

Medical devices increasingly rely on commercial technologies such as Windows operating systems, Bluetooth connectivity, commercial and open-source software, and off-the-shelf chipsets. The integration of these components helps drive down development and production costs, ultimately contributing to efforts to contain rising healthcare expenses.

However, the security of these commercial components is directly tied to the security of the medical devices that incorporate them. Despite this critical connection, there remains insufficient focus on securing these foundational technologies. Compounding the issue, medical devices often rely on commercial software and hardware well beyond the lifecycle originally intended by the developers or vendors of these general use components.

This is where Software Bills of Materials (SBOMs) play a critical role. SBOMs provide visibility into the third-party and open-source components used in a medical device, helping manufacturers, regulators, and healthcare providers understand what software is present and what associated vulnerabilities may exist. Without SBOMs, it becomes significantly more difficult to assess risk, manage vulnerabilities, or respond quickly to newly discovered threats within a device's software supply chain.

Without involving these upstream technology providers in ongoing discussions—and without encouraging longer support lifecycles—we will continue to face systemic vulnerabilities in medical devices. Ensuring that these foundational technologies are developed and maintained with security and longevity in mind is essential to improving the overall resilience of healthcare technology.

This is also a People and Process Issue

The healthcare industry faces a critical shortage of trained cybersecurity professionals with the expertise required to manage security in a dedicated and strategic way. This is fundamentally a **people and process issue**. Without skilled personnel on the ground to guide secure practices, manage risk effectively, and accurately assess and monitor what is connected to hospital networks, we are at a severe disadvantage.

This is not something that can be addressed through regulation alone. The FDA, while instrumental in setting important standards and expectations, cannot regulate its way into better on-the-ground cybersecurity management. What's needed is a workforce that understands the unique complexities of healthcare environments and is capable of making informed, real-time decisions to protect patients and systems.

At present, we simply do not have enough qualified cybersecurity professionals to meet the growing demands of the sector. In my view, this talent shortage is a core issue. Without experienced cybersecurity staff embedded in healthcare settings—individuals who can identify vulnerable legacy devices, advocate for more secure infrastructure, and drive change from within—unsafe practices will persist and hospitals will remain vulnerable.

What makes this issue even more urgent is the **imbalance between supply and demand**. When skilled cybersecurity professionals are scarce and the competition for talent is high, many hospitals—particularly small or rural facilities—are priced out. They often cannot afford to hire or retain qualified staff, and as a result, go without. This workforce gap leaves many organizations unprepared and under-defended.

It is essential that this issue receives more focused attention. Workforce development, training incentives, and targeted funding to build internal cybersecurity capacity must be prioritized if we are to meaningfully improve the security posture of the healthcare sector.

Solutions – How Can We Address This

Meaningful progress in securing legacy medical devices requires a coordinated and sustained effort from both medical device manufacturers (MDMs) and Healthcare Delivery Organizations (HDOs). This is not solely a technological challenge—it is fundamentally a people and process issue. Even the most secure medical device, if deployed without proper ongoing support and oversight, can become vulnerable over time. Many connected medical devices are used far beyond their intended useful life, even for 20 years or more, making long-term security a critical concern. Security is not a “one-and-done” feature, it requires continuous attention, including staff training, well-defined processes, and routine maintenance. Without trained personnel at both MDMs and HDOs who understand and follow established cybersecurity practices, the legacy device problem will persist. Likewise, without a shared commitment from both parties to develop and apply updates, manage device configurations, and maintain the overall cybersecurity posture of devices and hospital networks, the risk associated with legacy technologies will continue to grow.

Currently, one of the most comprehensive resources available for addressing this issue is the Health Sector Coordinating Council (HSCC) *Health Industry Cybersecurity - Managing Legacy Technology Security*, (HIC-MaLTS). This document outlines best practices for managing legacy medical devices and provides practical, actionable guidance. However, it is important to note that this report is voluntary. It is a best practice guide, not a regulatory or enforceable policy document from agencies such as the FDA, CMS, or The Joint Commission.

To drive meaningful change, there must be greater alignment between voluntary best practices and enforceable expectations, as well as increased investment in training, process development, and long-term cybersecurity planning by both MDMs and HDOs.

Recommendations

Industry-Wide

1. More trained security people with the experience to manage security in a dedicated way. This can come in the form of focused development of staff already in place by supplemental training and development or in the investment of regional and virtual training programs to develop an expanded security-savvy workforce.
2. Focus on effective communication programs to help HDOs and MDMs better communicate and coordinate their shared responsibilities in maintaining health sector security.

Medical Device Manufacturers

1. Develop more security engineers who can help design more secure devices from the outset, aiding in the delay of entering a legacy state.
2. Mature communication with stakeholders regarding the support status of marketed devices. Customers should be notified in advance of a product going EOS and this should typically occur when necessary due to the MDM's inability to support the product.
3. Practice good supply chain management. Review the software components chosen to be added to a medical device and select those more effective at maintaining the device for a reasonable time once launched into the market.
4. Develop, commit to, and execute regular software maintenance activities to patch vulnerabilities as they occur, as is now required by Section 524B for devices going through premarket submissions reviews. Do not allow vulnerabilities to build up over time and increase the "defect density" simply because that vulnerability is lower risk on its own. Vulnerabilities can be chained together to create a larger impact attack. Default activities should be to patch newly identified vulnerabilities rather than leave them in place.
5. For current legacy medical devices, MDMs can evaluate how much cybersecurity risk they can manage while preserving safety and effectiveness for these devices and assess whether the costs justify the investment. For devices where updates do not make sense, we need to explore device withdrawal from market and replacement mechanisms.

Healthcare Delivery Organizations

1. It should be a best practice that hospitals maintain Cybersecurity Performance Goals (CPGs) or some type of bar at hospital level to help secure the networks on which these medical devices operate (see Regulator Recommendation #2 – this is a shared recommendation).
2. HDOs must maintain a culture of security throughout their processes, including installing patches issued by device manufacturers and maintaining devices in a manner consistent with the manufacturer's quality systems.
3. HDOs need a comparable regulatory oversight mechanism from an entity like the Joint Commission or CMS. This mechanism can ensure that training, process, and maintenance is performed on practices like the Healthcare Cybersecurity Performance Goals (CPGs). Focus will need to be applied on how hospital networks are secured and how medical devices are segmented on those networks.
4. Many hospitals also have cybersecurity standards for procurement. If these exist, they should be consistently applied.
5. More trained security professionals who can manage legacy devices appropriately, segment networks, understand and manage security risks, and protect the network.
6. Options for funding these efforts include additional reimbursement from CMS for going towards cybersecurity maintenance activities and/or dedicated funding to ensure under-resourced HDOs (the majority of HDO facilities) can be brought up to current best practices.

Suppliers

1. Commit to longer support timeframes so that newly identified vulnerabilities can be patched throughout the lifecycle of the medical device.

Regulators

1. FDA could leverage inspections to ensure medical device manufacturers are following their Postmarket Cybersecurity Guidance recommendations, their associated Quality Systems for addressing postmarket risks with devices currently in use, and their plans for making available updates and patches to medical devices.
2. Congress and/or CMS could provide funding to HDOs to improve their network security, create a better trained workforce, and comply with the Healthcare CPGs to better protect their environment and ensure medical devices are on isolated/segmented networks
3. Update the 2016 FDA Guidance: *Postmarket Management of Cybersecurity in Medical Devices* (Guidance for Industry and Food and Drug Administration Staff) to reflect current best practices on legacy and align with new statutory obligations.

Conclusion

Medical devices and the broader healthcare environment are now more dependent on connectivity than ever before. While this connectivity enables more efficient care, it also introduces a substantial range of cybersecurity risks. If any component of this interconnected system is not properly maintained or managed, the entire environment becomes vulnerable, putting patients, the continuity of care, and healthcare institutions at risk.

Effectively addressing the challenge of legacy medical devices will require sustained attention and resources, particularly in building cybersecurity awareness, training, and technical expertise across all stakeholders. This includes development and maintenance personnel at medical device manufacturers, IT and clinical engineering staff at Healthcare Delivery Organizations (HDOs), and developers and leadership at component and software suppliers whose technologies are integrated into medical devices and healthcare IT systems.

In addition, resolving these issues will require targeted investments across the ecosystem:

- **Medical device manufacturers** should assess existing legacy devices and determine where cybersecurity risks can be reduced and ensure they communicate with customers and follow appropriate risk transfer processes.
- **HDOs** should implement and maintain cybersecurity practices—such as network segmentation, asset management, and alignment with frameworks like the *Healthcare and Public Health Cybersecurity Performance Goals*.
- **Component and software suppliers** should be encouraged to build technologies that are secure by design and can be supported for longer lifecycles, reducing downstream risk to the healthcare sector.

Ultimately, strengthening the cybersecurity of connected medical technologies will require coordinated action across the entire healthcare ecosystem. Addressing the legacy device challenge is not a single-entity task, it is a shared responsibility that will demand strategic investment, collaboration, and accountability at every level.