Executive Roundtable: Cybersecure Devices in MedTech

ISSUES PAPER

Overview

The ICA Executive Roundtable: Cybersecure Devices in MedTech, held in Adelaide in June 2025, brought together industry leaders, cybersecurity experts, academic researchers, health professionals, and policy stakeholders to examine the urgent and complex challenges facing the secure development, deployment, and regulation of medical technologies.

This issues paper reports on the discussion held at that roundtable. It highlights key issues in the progress of technologies in medical devices and platforms and how these intersect with the health services sector. It recommends development of cybersecurity skills in the workforce, clear governance mechanisms, and cybersecurity by design in medical devices. It outlines implications for practice, policy, and investment.

> "Ten years ago, attackers could focus on a single device. Now we have multiple devices, and you can launch one attack to another device to another device—finding the weakest device to get in."

Issue Definition

Medical devices increasingly use digital networks to transmit data, support diagnostics, or enable remote monitoring and control. The connectivity of these technologies surfaces new safety considerations and concerns for healthcare providers, governance, and users.

The roundtable defined these technologies as encompassing both hardware and software medical devices, those that interact directly with the body, as well as those that are used in analysis or for gathering and communicating information.

> "The way that we need to look at it in healthcare is to not talk about it just as a cyber security issue. It's actually a clinical, whole safety issue."

Key trends & challenges

The two most discussed challenges around the table on the cybersecurity of devices in MedTech were the maturity level of the digital medical technologies sector and the question of who owns the security risk inherent in these devices.

Contact: Kathryn Anderson Kathryn.anderson@flinders.edu.au
www.flinders.edu.au/innovation-central-adelaide

The medical technology sector was described as in its infancy, but with a rapid rise and expansion. There is a need for a greater level of skill in cyber security across the workforce, embedded into education and training for healthcare professionals and device developers. The cultural and structural divide between biomedical engineering teams and IT or cybersecurity professionals was identified as a major systemic issue, leading to digital medical devices being treated as isolated clinical tools, and limited understanding of their integration into broader digital health systems.

"Not only do we have new med technology, internet of medical things and all the new developments, we've got tech debt where, you know, some of these legacy medical systems are running still on Windows XP."

Legacy technologies emerged as a complex issue at the health system level, combining financial, technological, governance, and cultural aspects. From a financial perspective, capital constraints and long investment cycles lead to network-connected medical devices remaining in service far beyond their secure life expectancy. Technical challenges are encountered in the interoperability of devices run on variably aged and configured operating systems. The question of governance arises as purchasing decisions are often made by clinical staff, with security and interoperability responsibilities deferred to IT teams. This leads to significant gaps in accountability and response readiness. And a culture of disconnect between clinical and cybersecurity concerns and accountability needs to change to promote a stronger culture of risk ownership and visibility across departments and leadership levels.

Cybersecurity adoption barriers

A primary tension exists between the desired speed-to-market to move medical devices into practitioner use, and the time required to extensively test and secure their network communications.

"We're seeing a lot of MedTech manufacturers coming to the market, a lot of startups across Australia. It's one of our biggest industry growth sectors, MedTech."

It was noted that cybersecurity is rarely a competitive differentiator for purchasers, and cost, functionality, and vendor ecosystem compatibility deprioritise it for manufacturers.

There is a critical need to balance the design constraints of devices, that in many cases must be lightweight and compact, with the space needed to provide adequate compute power to enable cybersecurity. It was noted that rather than designers and manufacturers taking a cybersecurity-by-design approach, priority is often given to the usability of devices in the health setting and for end users. However, it was stressed that the (lack of) cybersecurity of medical devices has a potential for high impact on health outcomes.

Concerns were raised around the weight of regulatory processes, and complexity of the regulatory environment. The multiple intersecting categories, standards, classifications, and bodies, impact time-to-market and cost of product for vendors and manufacturers. A practise of prioritising compliance over rigorous security sees regulation driving organisations to focus on "tick-box" compliance rather than meaningful risk reduction.

> "A small device manufacturer will want to get product in the field as quickly as they can, through approvals, so that they can get something on the market and hopefully get some revenue coming through."

Workforce & policy recommendations

Embed security throughout the device lifecycle

This includes secure development practices, real-time vulnerability patching, secure data handling, and mechanisms for safe disposal. Cybersecurity-by-design approaches and continuous lifecycle support should be a baseline, not a bonus.

Implement system-level architecture and zero-trust models

Adopt zero-trust architectures and advanced network segmentation to manage risk from inherently insecure devices. Recognise that security cannot always be embedded in the device itself and must instead be enforced at the system or network level, particularly in large-scale hospital environments.

Reframe cybersecurity as clinical safety

Shift the narrative: cybersecurity should be seen as integral to patient safety, not merely a technical issue. This framing may be more persuasive to clinicians and decision-makers and could support greater alignment between cybersecurity practice and clinical governance.

Harmonise standards and procurement frameworks

Currently, digital medical device vendors must respond to disparate security requirements from different jurisdictions, departments, and hospitals—even within the same state. There is a strong case for a harmonised national procurement standard for MedTech cybersecurity to improve both vendor efficiency and patient safety.

> "If Australia wanted to support innovative MedTech businesses to access the Australian market, there'd be, I think, a lot of potential for top-down government policy to drive harmonisation in terms of data management."

Invest in education and workforce capability

Universities and training providers must embed cybersecurity fundamentals into biomedical engineering, health informatics, and clinical training programmes. A lack of understanding at the intersection of clinical science and IT remains a significant barrier to secure design and operational integration.

Contact: Kathryn Anderson Kathryn.anderson@flinders.edu.au
www.flinders.edu.au/innovation-central-adelaide

Top priorities for action

For governance

- Implement system-level architecture and zero-trust models
- Call for data harmonisation and national procurement standards by federal government
- Define 'who owns the risk' in the cybersecurity of medical devices

For designers, manufacturers, investors and vendors

- Embed security throughout the device lifecycle, from design to decommission
- Include cybersecurity as a basis for investment decisions
- Build cybersecurity cost and time considerations into development cycles

For workforce

- Upskill clinical staff in the fundamentals of cybersecurity
- Educate for cybersecurity as a whole-of-care clinical safety consideration
- Cultivate a culture of risk ownership and visibility across departments and leadership levels

For university

- Embed cybersecurity training across the health disciplines
- Research the connectives in cybersecurity from allied areas, for example, fintech
- Engage multiple stakeholders in medical technology to advance knowledge and practice

Conclusion

The Cybersecure Devices in MedTech discussion revealed deep structural, cultural, and commercial challenges in the secure development and deployment of medical technologies. While the need for secure medical devices is clear, realising that goal requires more than technical solutions—it demands system-level thinking, cultural change, harmonised standards, and sustained investment in capability. Cybersecurity in MedTech is not simply a matter of compliance—it is fundamentally a matter of clinical safety and public trust. If Australia is to position itself as a leader in health innovation, ensuring that devices are both functional and secure must be a priority.

About ICA

Innovation Central Adelaide (ICA) at Flinders University is a collaboration with Cisco, and one of six innovation centrals across Australia. These anchor the National Industry Innovation Network, an initiative that engages with higher education institutions. ICA's purpose is to collaborate with industry, business, and government to advance digital enablement and uptake. It does this via defined research and innovation work packages, including contract research, concept-to-proof programs, student projects, higher degree engagement, and by generating and fostering issues-based communities.

Contact: Kathryn Anderson Kathryn.anderson@flinders.edu.au
www.flinders.edu.au/innovation-central-adelaide