Capgemini

SAFEGUARDING THE CONNECTED HEALTH REVOLUTION: MEDICAL DEVICE SECURITY

The convergence of cutting-edge technology and patient-centric care is catalyzing a revolution in healthcare. Connected health devices are at the forefront of this digital transformation, poised to reshape patient experiences and healthcare outcomes. In this era of innovation, one vital aspect should command our attention: the imperative to secure medical devices

THE PROMISE OF CONNECTED HEALTH

By 2032, the global connected healthcare market is ***projected to grow*** to $520bn. Considering that the estimated market size was $58.2bn in 2022, this anticipated growth is remarkable and connected devices have already begun to reshape the healthcare landscape, offering unprecedented opportunities to monitor, diagnose, and treat patients remotely.

From wearable fitness trackers to implantable medical devices, the possibilities are vast. Imagine a scenario where doctors can remotely adjust a patient's pacemaker settings, or individuals with chronic conditions can have their vitals tracked and analyzed in real time, alerting healthcare providers to any concerning trends. This integration between technology and healthcare has the potential to revolutionize patient experiences and outcomes.

THE SECURITY IMPERATIVE

As we embark on this transformative journey, ensuring the security of these connected medical devices - which open new gateways for cyberattacks and data breaches - is crucial. Safeguarding sensitive patient information is only the beginning; the nucleus of the issue lies in preserving patient well-being itself.

The healthcare industry must embrace this new paradigm, where security is an integral part of a device's very DNA. Taking a proactive approach will ensure that security isn't merely a feature, but an inherent attribute that safeguards both patient data and device functionality right from the outset.

Presently, healthcare providers find themselves navigating two distinct paths. On the one hand, there's the endeavor to retrofit existing legacy devices with connected technology, aiming to enhance overall functionality within the integrated healthcare ecosystem. On the other hand, a new class of purpose-built medical devices is emerging, designed to seamlessly thrive within the dynamic digital landscape. Either way, device security cannot be an afterthought and every step must align within the security framework set by relevant regulatory standards.

HARMONIZING INNOVATION AND REGULATION

In the transition to intelligent industries, similar security concerns span across sectors. For instance, a healthcare provider faces similar concerns to those of an automotive manufacturer. From data privacy and customer safety to public trust, ransomware, the financial implications of attacks, and regulatory compliance—all loom large. But due to the stringent regulations governing the industry, the latter, regulatory compliance, is especially important to understand.

The world of connected medical devices must exist within a comprehensive regulatory framework. Regulatory bodies such as the FDA set rigorous benchmarks, demanding that medical devices meet the highest security standards before entering the market. Spearheading this drive is the ***FDA's Pre-Market Approval*** (PMA) process, a pivotal stage where medical device manufacturers must meet stringent security criteria before introducing their products to the US market. This initial phase sets the tone for ongoing vigilance as devices continue to be monitored post-release for updates, compliance, and potential recalls.

On an international level, collaborations on international medical device regulators like the ***IMDRF*** are uniting economic communities like Brazil, Australia, Japan, China, and the European Union, which showcases a collective commitment to addressing cybersecurity challenges. Such global frameworks are necessary because connected devices aren't solitary entities - they engage within diverse ecosystems.

This also means that devices interfacing with hospital environments must align with IT security standards like ISO 27001 and similarly, align to operational technology (OT) standards such as IEC 62443, essential for devices manufactured within OT environments. Supply chain compliance also gains prominence, with each component needing to meet specific regulations.

As regions introduce their own mandates, the emergence of the ***US Cybertrust Mark*** sets the standard for an industry that needs to convey confidence and trust to consumers that the device they are purchasing are secure. President Biden's executive order underscores comprehensive software transparency, and the EU's impending ***Cyber Resilience Act*** highlights the industry's shift towards robust risk assessments and security diligence for connected devices.

ELEVATING EXPERTISE AND COLLABORATION

It's clear that medical device security extends a unique challenge that requires specialized expertise. And yet, the cybersecurity industry is grappling with a scarcity of professionals equipped with the diverse skill sets required to engineer secure devices. Meeting this challenge head-on calls for strategic talent acquisition, continuous skill development, and the cultivation of a workforce poised to address the multifaceted security concerns of medical devices.

At Capgemini, collaboration is our guiding light. By forging alliances across industries, we are bridging the expertise gap to craft bespoke security solutions for medical devices. With our extensive cyber portfolio and engineering expertise spanning sectors such as healthcare, automotive, and energy, Capgemini is uniquely poised to offer holistic security measures that resonate with distinct requirements. Already, eight in ten health tech providers are using Capgemini innovations to connect and share data, and over 95% of the industry works with us to ensure they deliver the highest quality products and value to the market.

From assessing existing security controls, to threat modeling, to risk assessment, to software bill of materials (SBOM), to defining security requirements, to supporting FDA submissions, Capgemini's support is end-to-end. And in a complex market, collaboration can be the difference between doing business and not doing business.

For example, Capgemini recently worked with a global medical device company to develop a security architecture for a connected, wearable, handheld insulin pump. To deliver all the key artifacts needed for compliance and 510(k) submission, our experts applied security across the product lifecycle, firmware/hardware, mobile application, cloud, PKI setup, and communicated with partners every step of the way. From ECG machines to state-of-the-art colposcopy devices, we are helping our customers move more quickly into the next generation of medical care.

SHAPING A RESILIENT HEALTHCARE LANDSCAPE

The trajectory of connected health devices charts an inspiring course for the future of healthcare. Ensuring the integrity of this transformation is our collective responsibility. By weaving security into the fabric of connected health innovation, we can pave the way for a resilient healthcare landscape that nurtures patient well-being and inspires the pursuit of excellence.

In this journey towards pioneering the future of medical device security, Capgemini remains unwaveringly dedicated to making the Connected Health Revolution a safe and transformative reality.

AUTHORS

Geert van der Linden

Global Head of Cybersecurity Service Line

Cloud Infrastructure Services

geert.vander.linden@capgemini.com

Aarthi Krishna

Global Head of Intelligent Industry Security

Cloud Infrastructure Services

aarthi.krishna@capgemini.com

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided every day by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of nearly 350,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering, and platforms. The Group reported in 2022 global revenues of €22 billion.

Get the Future You Want | **www.capgemini.com**

For further information please contact:

infra.global@capgemini.com