Adopting Medical Cyber Physical Systems

to Keep Up with an Increasing IoT World

leidos

Cyber-attacks directed toward health care agencies can cause significant harm to institutions and the patients they serve. Combating these threats requires a renewed focus on moving beyond compliance and building resilient cyber physical systems.

As the health care industry adopts modern medical devices to better care for and diagnose patients, hospitals must still ensure legacy systems are secured and maintained — as replacing them is not always an option financially. This is critical to the correlation of Medical Cyber Physical Systems (MCPS), and overall, to providing secure patient care efficiently.

The Internet of Things (IoT), and Internet of Medical Things (IoMT), are the foundation of MCPS. These systems integrate the computation and networking often found in digital systems into physical objects and infrastructure, allowing connection to the internet and other medical devices. It's all about incorporating digital defenses for physical hardware.

Securing both digital and physical systems in health care is challenging as devices must adhere to stringent certifications and policies, while functioning in a medical capacity. Patient care relies heavily on medical professionals having cross platform access to real-time data from wearables to medical devices for diagnosis.

A strong cyber infrastructure is necessary to help ensure that surgery automation to data aggregation will continue to revolutionize patient care; however, the current health care infrastructure faces critical issues and concerns from patient privacy to security.

"Addressing these critical infrastructure issues in the near future will be critical to providing secure patient care more efficiently," said Anna L. Ehrhardt, Cyber Manager for Leidos' Health Group and Leidos' Cyber Accelerator Health Group Lead.

The health industry historically has faced unique threats against its cyber physical systems, considering the delicacy of patient information. Now with the increase of IoMT devices, a patient's sensitive data streams across a network of digital devices, which strays from the norm of legacy medical security adding an additional level of complexity to avoid exploitation without impacting patient care.

"The amount of data points contained now on these devices increases the risk of exposing patient sensitive data exponentially," Ehrhardt said. "Think of a scenario where a hacker could infiltrate the network and overwrite software on a medical device performing automated surgery resulting in a potential loss of life. We truly are in a very technological transformative era within health care."

> "The amount of data points contained on these devices increases the risk of exposing patient sensitive data exponentially. Think of a scenario where a hacker could infiltrate the network and overwrite software on a medical device performing automated surgery resulting in a potential loss of life. We truly are in a very technological transformative era within health care."
>
> —
>
> Anna L. Ehrhardt
>
> Cyber Manager for Leidos' Health Group and Leidos' Cyber Accelerator Health Group Lead

Leidos' Health Group is getting ahead of these vulnerabilities with its medical Cyber Physical Systems (CPS) for harvesting Real-World Evidence (RWE) and Real-World Data (RDE) from hospitals, clinics and medical facilities. By applying to analytics to improve time from signal of concern to resolution, it's possible to reduce the time required to approve existing drugs for new indications.

"Essentially, the solution secures all health care system data, applications, analytics, and results that are at rest, in motion and/or are in use from an IoT and IoMT perspective," Ehrhardt explained.

"One of our goals at Leidos is to ensure that we eliminate as many potential attack vectors as possible to reduce the ramifications from exposure to these threats," Ehrhardt said.

And considering health facilities are still using a mix of modern and legacy systems, a MCPS is critical to ensuring all systems are secure, regardless of their sophistication.

Yet regulation and compliance challenges remain. "New technologies are being released months before the regulations and policies that govern them. At the same time hospitals have legacy devices lacking security from the initial build and to replace these devices could cost millions of dollars," Ehrhardt explained.

While the National Institute of Standards and Technology's publication 1500-201 provides a solid framework for cyber physical systems, the medical community must also consider how implementing that framework impacts the Food and Drug Administration's certification processes.

"The goal is, in my opinion, to find a comprehensive cybersecurity framework that uses security as its foundation that includes all the different agency policies, regulations and any interdependencies allowing for technological modernization to occur without risking patient safety."

Ehrhardt also recommends policymakers tailor these frameworks to the specific industry because securing IoT devices will differ from health care to manufacturing. "Currently there are multiple different policies out there, but all are tailored to a one size fits

> "The goal is, in my opinion, to find a comprehensive cybersecurity framework that uses security as its foundation that includes all the different agency policies, regulations and any interdependencies allowing for technological modernization to occur without risking patient safety."
>
> —
>
> Anna L. Ehrhardt
>
> Cyber Manager for Leidos' Health Group and Leidos' Cyber Accelerator Health Group Lead

all approach. Meeting the specifications in one policy could violate the requirements of another policy. These conflicts need to be addressed to ensure emerging capabilities are properly secured to allow for these amazing advancements in patient care to operate as intended," Ehrhardt said.

Leidos focuses on supporting health care customers by providing a secure digital infrastructure. Currently the company is working on protecting and expanding its infrastructure base, providing data-first multi-cloud security and software-as-a-service solutions.

"Leidos has been helping health care organizations secure sensitive patient and medical data while ensuring privacy and compliance to regulations like HIPAA are maintained, through the use of the [Real-World Evidence Solution]," Ehrhardt said. "RWE helps protect the connections, access keys and data between medical devices and hospital networks, regardless of their location, creating a secure MCPS."

Hospitals and integrators such as Leidos will face increasing pressure to demonstrate how they are mitigating risk, and how they are working with vendors to identify and remediate new issues without violating FDA certification. As once a medical device is FDA certified, adding extra security on top of it may impact the safety or performance of the device.

Considering compliance challenges, Leidos is working with customers to have a more complete, auditable system. Using Real-World Evidence detects real-time threats in the environment, along with a centralized application to push real-time group policy, access control and security updates.

In other words, by using Real-World Evidence, Leidos can go beyond compliance on any type of device to ensure constant and consistent security postures are maintained.

With the influx of emerging technologies in the health care industry, legacy systems can't be left behind. They must be secured and capable of being updated to meet new standards, while adapting to new technologies.

"Until we can get a comprehensive view, it's going to be a constant ebb and flow of what is the best way to secure the environment during this modernization era," Ehrhardt said.

Discover more about how Leidos is supporting health care agencies

leidos