FTI JOURNAL

ARTICLE

Are Connected Medical Devices Leaving Your Hospital's Doors Wide Open?

November 2020

Internet-connected healthcare devices, ubiquitous in hospitals, are often rife with vulnerabilities. Here's how hospitals can keep their networks secure and patients safe.

Hospitals are often synonymous with treatment and care, but cyber actors view them as prime targets for their attacks.

On the rise is a serious new risk that centers on hospitals' internal networks and healthcare devices that connect to them. Vulnerabilities in these devices can serve as an entry point to hospital networks for nefarious, over 41 million patient records were breached, with a single incident affecting close to 21 million records.

The threat is grave. On September 9, 2020, a female patient died as a result of a ransomware attack on Dusseldorf University Hospital in Germany. As the patient was in transit to the hospital, attackers locked up the facility's system by encrypting 30 of its internal servers. The patient had to be transferred to another hospital roughly 19 miles away and did not survive.

As healthcare embraces benefits from technology, this is a reminder of the inherent perils of getting healthcare technology wrong. It is estimated that larger hospitals networks have upwards of 350,000+ medical devices running simultaneously — and that's excluding the millions of connected devices that patients bring into these hospital networks. In the next 10 years, the number of connected medical devices is expected to surge to roughly 50 billion thanks to advances in 5G technology, edge computing and more.

With so many new devices entering these hospital networks, the surface area for potential attacks only widens due to inherent vulnerabilities in these devices. This not only threatens standalone connected medical devices because of their reliance on networks to function, but entire networks themselves. Think back to May 2017, when a WannaCry outbreak shut down computers across more than 80 NHS organizations in England alone. The attack resulted in almost 200,000 cancelled appointments, 600 general practitioner surgeries having to resort to pen and paper and five hospitals needing to divert ambulances because they couldn't handle any emergency cases.

How can these devices — which are paving the way for tomorrow's healthcare system — be so susceptible to attack? Because they were not designed with privacy or security in mind.

An Inherent Fallacy

Establishing cybersecurity protocol with today's connected healthcare devices is a challenge for a number of reasons.

In May 2019, a cybersecurity report predicted that 70 percent of medical devices would be running on an unsupported operating system that's vulnerable to attack by January of 2020.

Consider that the purpose of these devices is to quickly and efficiently transmit information. These devices are designed for low latency — not security. Security incurs a technical overhead, which negates the desired benefits of the device. For example, implementing encryption and authentication methods slows down response time and requires additional bandwidth allocations, putting security and the purpose of the device at odds.

Another issue is that these devices are typically designed to work "straight out the box" with little to no setup. That means they're operating on default, easy-to-use settings that may not offer robust security protocols. Original equipment manufacturers' (OEMs) instructions will often refer to FDA regulations, which state that the function of a device cannot be changed unless it's proven that the systems can't be patched. In other words — if it isn't broken, don't fix it.

This "plug and play" issue extends beyond just the hospital and their own devices. Connected third parties who take the same approach with their devices are adding additional vulnerabilities to the hospital, as cyber actors can leverage this connection as an entry point.

Then there's the issue of funding these security measures. Many hospitals simply don't have the budget to uproot their entire technological infrastructure, update all of their systems and invest bolstering the security of their networks. This puts administrators in a tricky position where they might have to choose between bolstering their networks or investing in a new diagnostic tool.

Finally, there are concerns around timeworn networks and outdated systems. Many organizations, including hospitals, are built atop a technology infrastructure consisting of outdated operating systems. These systems grow old to the point that they cannot be updated or patched yet remain the building blocks to the foundation of the network. In May 2019, a cybersecurity report predicted that 70 percent of medical devices would be running on an unsupported operating system that's vulnerable to attack by January of 2020. As more connected devices are integrated into these networks, more opportunities arise for hackers to breach these walls made of sand.

It's difficult because cybersecurity, much like medicine, can be an inexact science. But both evolve and progress. Anyone who interacts with hospital networks — from administrators to IT teams to third-party vendors — needs to think proactively to align the two sciences and to ensure they're not creating an opening for others to do harm.

Securing these networks is not an impossible task — just a challenging one. However, given the immense patient benefits that connected healthcare devices provide, its only become increasingly important that hospitals take necessary steps to ensure the security of these life-saving technologies.

Four Steps to Securing Connected Medical Devices

1. Assess your risk appetite.

Hospital administrators know the opportunities — as well as the risk — that connected devices introduce into a hospital. The questions they need ask themselves are:

- Have I done everything to protect my patients?

- Have I coordinated with my third-party vendors to ensure my patient's safety in case of an emergency?

The truth is that headline-grabbing cyber attacks are now transparent to patients and the media alike. People can see whether a hospital has done its due diligence and maintained its responsibility to protect its network. Thus, hospitals need to make sure they've taken a comprehensive approach to ensuring the safety of patients and their data. If not, they risk a diminishing patient base.

2. Stress-test your devices

Many OEMs will state that they've followed proper safety protocols and buttoned up every serial and communication port. However, an unprotected network can allow for even a secure device to be compromised. A Bluetooth-enabled intravenous system, for instance, may work great in a warehouse, but what happens when it's introduced to a saturated network with inadequate bandwidth? What happens when it shuts off?

The responsibility falls on hospitals and OEMs alike to put these devices to the test within their own environments. Networks themselves should be tested before larger devices are introduced, while smaller devices should be tested on-site.

3. Update your system

For any legacy organization, staying current is essential. Unfortunately, it can be costly to upend an entire organization's technological infrastructure. While it may be a hard sell, the reality is that an entire hospital network could go down if the risk is not properly mitigated.

One option to consider is performing this task in piecemeal. Start with the systems that are most integral to your organization and work outward from there. Understandably, it can be difficult to convince the head of finance to invest in fixing an outdated system that serves no current purpose. However, one needs only remember the recent NHS error where an outdated spreadsheet format left contact tracers scrambling to find an estimated 50,000 people who had been in close contact with someone who had the coronavirus. The incident was reported as a "catastrophic data error" that put people's lives at risk.

4. Follow the guidelines

In the EU and the UK, guidelines have been published by the European Union for Cybersecurity (ENISA). They speak specifically to hospitals and offer cybersecurity guidance around procurement, products and infrastructure.

The United States could afford to take a page from ENISA's playbook. The National Institute of Standards and Technology (NIST) has put forth broader guidelines for private U.S. organizations, which includes hospitals. In 2013, it was predicted that 50 percent of U.S. organizations would adopt the NIST Cybersecurity Framework by 2020. However, in the midst of a tumultuous year, it's uncertain whether NIST has reached that goal.

Indeed, hospital administrators have a long road ahead of them when it comes to securing their connected medical devices. However, until a change is made, cyber actors will continue to prey on hospitals and use connected devices as easy access points to exploit. Therefore, the best time to invest is today, if not yesterday.

© Copyright 2020. The views expressed herein are those of the authors and do not necessarily represent the views of FTI Consulting, Inc. or its other professionals.

JORDAN RAE KELLY
Senior Managing Director
+1 202 312 9140
jordan.kelly@fticonsulting.com

PATRICK MACGLOIN
Senior Managing Director, Cybersecurity
+44 207 6325017
patrick.macgloin@fticonsulting.com