BECKER'S HEALTHCARE

verizon business

Managing cybersecurity risk in an expanding healthcare ecosystem

The rise of telehealth, healthcare-at home and other remote care options is bringing greater flexibility to health systems and patients, who often prefer to receive more care at home. However, home-based care that relies on various connected devices introduces increased cybersecurity threats.

Becker's Healthcare recently spoke with three network and security experts about how healthcare leaders can identify and address cybersecurity risks as the device and delivery ecosystem grows. These experts discussed strategies for countering cyber threats, notably a layered security approach, and described issues associated with common bring-your-own-device (BYOD) policies. They also summarized advantages of company-owned or "company-liable" device programs.

How and where healthcare is being delivered is shifting

Health systems are increasingly focused on how to deliver care to patients outside of traditional healthcare settings. For example, in 2023, over 400 hospitals and health systems offered hospital-at-home programs and the number of programs is expected to grow by 50% in the next few years.[1]

When care is delivered outside of a hospital, connected devices and remote patient monitoring enable continuous monitoring and data collection. This helps clinicians track the patient's healthcare journey and intervene in real time when necessary.

"Healthcare providers no longer just have a snapshot of patients in the physician's office," Robin Goldsmith, Global Lead, Healthcare Innovation and Strategy at Verizon Business, said. "They can get an 'always on' understanding of their condition and adjust care plans accordingly. The overall goal is to keep patients healthier and out of emergency rooms."

Healthcare-at-home programs enable patients to engage in preventative, post-op and chronic care check-ins from the comfort of their home, minimizing the chances of missing an appointment due to transportation challenges and eliminating the risk of acquiring an illness from other patients in a busy office. Payers also see the benefits of these programs as a way to deliver high-quality care at a lower cost with positive outcomes.

More devices, however, mean more windows of opportunity for threat actors to attack. As a result, healthcare organizations must increasingly concern themselves with the security of more and more endpoints – including connected laptops, tablets, phones and wearable medical devices.

Home-based care is a potential weak link in the cybersecurity chain

In a traditional healthcare setting, IT security teams often have a proven security playbook: they conduct third-party due diligence to confirm that vendors have effective security controls in place; they ensure only secure devices and authorized users are allowed to connect to their network; and they conduct awareness training to help staff defend against ransom or other malware.

But when care moves outside the four walls of a traditional healthcare setting, the security challenges expand.

"CISOs and healthcare IT security teams now have to think about how to expand their efforts to the home," David Grady, CISM, Senior Manager, Network and Security Marketing at Verizon Business, said. "How do you make sure the devices patients are using are secure? That's a big challenge when patients use their own laptops or smartphones to communicate and share data with healthcare providers. All of these new endpoint devices contribute to what security experts call 'the ever-expanding attack surface.' Poorly secured remote users – from patients and staff to vendors – can become the weak link in the security chain."

[1] What hospital-at-home programs mean for healthcare, Advisory Board, July 20, 2023.

In addition to patients' devices, many healthcare systems also rely on clinicians to use their own devices. These BYOD policies introduce added security concerns. Twenty-five percent of mobile device users admitted to tapping on a phishing link at least once per quarter in 2023, according to the 2024 Verizon Mobile Security Index.

"That means that four times a year, mobile users are falling for phishing emails," Mr. Grady said. "They click on those links and have their credentials stolen or their systems compromised. There's so much work to be done in terms of implementing more security controls and raising awareness. And that work is on both the patient side and the provider side. Security has to be a partnership with shared responsibilities."

The 2024 Verizon Data Breach Investigations Report found that 28% of data breaches result from human mistakes and process errors, not from malicious acts. This brings into greater scrutiny the procedures and processes that healthcare organizations use to share information and move data. For example, important questions to be answered include:

- Are e-mails that contain personal health information encrypted?
- Does access to an online patient portal require strong passwords or two-factor authentication?
- Is a provider office still relying on faxes, which often can easily be compromised in a unattended fax machine?
- Are patients connecting remotely with secure Wi-fi connections?

Taking a layered approach – benefits and limits

To enhance security, a best practice adopted by many organizations is a "layered" security approach. Layered security means deploying a wide variety of security controls to meet a wide variety of threats.

A layered security program might include mobile device management solutions to control what is installed on company-issued devices, unified endpoint management, zero-trust access, data loss prevention tools, malicious website blocking and end-user education.

However, Derek Peabody, Senior Director, Mobile UC & Solutions Product Management at Verizon Business, cautions that a provider's layered security efforts can only extend so far beyond the four walls of an office or a hospital. When patients and employees bring their own devices, validating the security of those devices can be very difficult. That difficulty increases cyber risk while also potentially negatively impacting the patient experience.

"When you look at the layers of security that restrict what can and can't be done on the device, it becomes almost untenable in a BYOD scenario," says Mr. Peabody. "Nobody wants their personal device to be that locked down."

An alternative to BYOD: Company-owned and company-liable devices

A promising alternative to BYOD policies is for hospitals and health systems to invest in company-owned or "company-liable" device programs that provide patients and other users with devices that have been built with consistent and proven security controls.

"From the healthcare system's perspective, there's often concern about the upfront cost of acquiring, configuring and supplying these [company-owned or company-liable] devices," Mr. Peabody said. "What we're seeing, however, is that it is often costlier – and riskier – to invest in the long-term, ongoing maintenance of a BYOD environment. The administrative aspects of configuring and shipping devices can be outsourced to third-party solutions, so healthcare providers aren't stuck with the administrative burden."

While some end users may initially be reluctant to carry two devices – their own phone and a company-issued one – it is important that both employees and patients understand the importance of maintaining the security of critical healthcare information.

Educating users about the potential risk that poorly secured personally owned devices pose to their privacy often convinces them that carrying two devices makes sense. Adding to the case for company-owned or company-liable devices is the realization that this option often better protects the business.

"There's also the separation of work and personal lives," Mr. Peabody said. "It's harder for employees to separate those if they are working on their personal devices. With a corporate device, at the end of the day, you put your phone or tablet away and just use your personal device. That becomes much more difficult with BYOD, where the personal and the professional meet in a single device."

In addition to providing security benefits, a company-owned device strategy can strengthen a healthcare organization's business identity. "If employees are using BYOD devices to make outbound calls to a patient at home, they are using their personal phone number, which the business doesn't control," Mr. Peabody said. "Patients are often reluctant to answer a call from a number they don't recognize, and that can have an impact on clinical outcomes. It's best when healthcare providers have clear ownership of phone numbers, so their patients can have

confidence about who they are talking to. Having the organization's well-known toll-free number display when a patient gets a phone call goes a long way to building trust and can minimize the need for making repeated calls out."

Practice makes perfect

Despite their efforts to maintain a strong, layered security program, some health care organizations inevitably find themselves under attack from cyber criminals. And the worst time to develop a critical incident response plan is in the middle of an attack.

Proactive critical incident response planning brings together key stakeholders – from IT teams to public relations, regulatory teams, clinical leadership and more – to develop and agree on a plan. Representatives from these groups should then meet regularly to practice how they will respond to a ransomware attack or the theft of patient data.

Mr. Grady points out that it's important to have a well-documented plan that's regularly updated; everyone's contact information should be correct, and staff should understand their roles and responsibilities if a breach or an attack occurs. "Without trust and governance, there will be more finger pointing than collaboration during a crisis," Mr. Grady said. "Better to have a plan that everyone agrees to in advance."

Given the prevalence of ransomware in the healthcare sector, this particular risk is an essential consideration during critical incident response planning before any ransomware attack occurs. "Organizations must do a deep dive on their ransomware policy so they don't have to sort that out in real time," Mr. Grady said. "'Will we pay? Should we pay? How do we pay? These are the questions that need to be answered in advance. Providers and health systems can always consult with local law enforcement or the FBI to get advice about what to do in those situations."

Once critical incident response plans have been developed, a best practice is for teams to practice on a quarterly basis using desktop exercises that simulate a cyberattack. This approach can mean the difference between a rapid recovery from a cyberattack or a long-term disruption to services, impacting patient care and the organization's reputation. "As you introduce more technologies for care, security has to be first and foremost, given the potential impact that breaches and ransomware attacks can have on the healthcare sector," Mr. Goldsmith said. "It can be a life-or-death scenario where you have to shut down sites and turn patients away because you can't deliver the care that's needed."