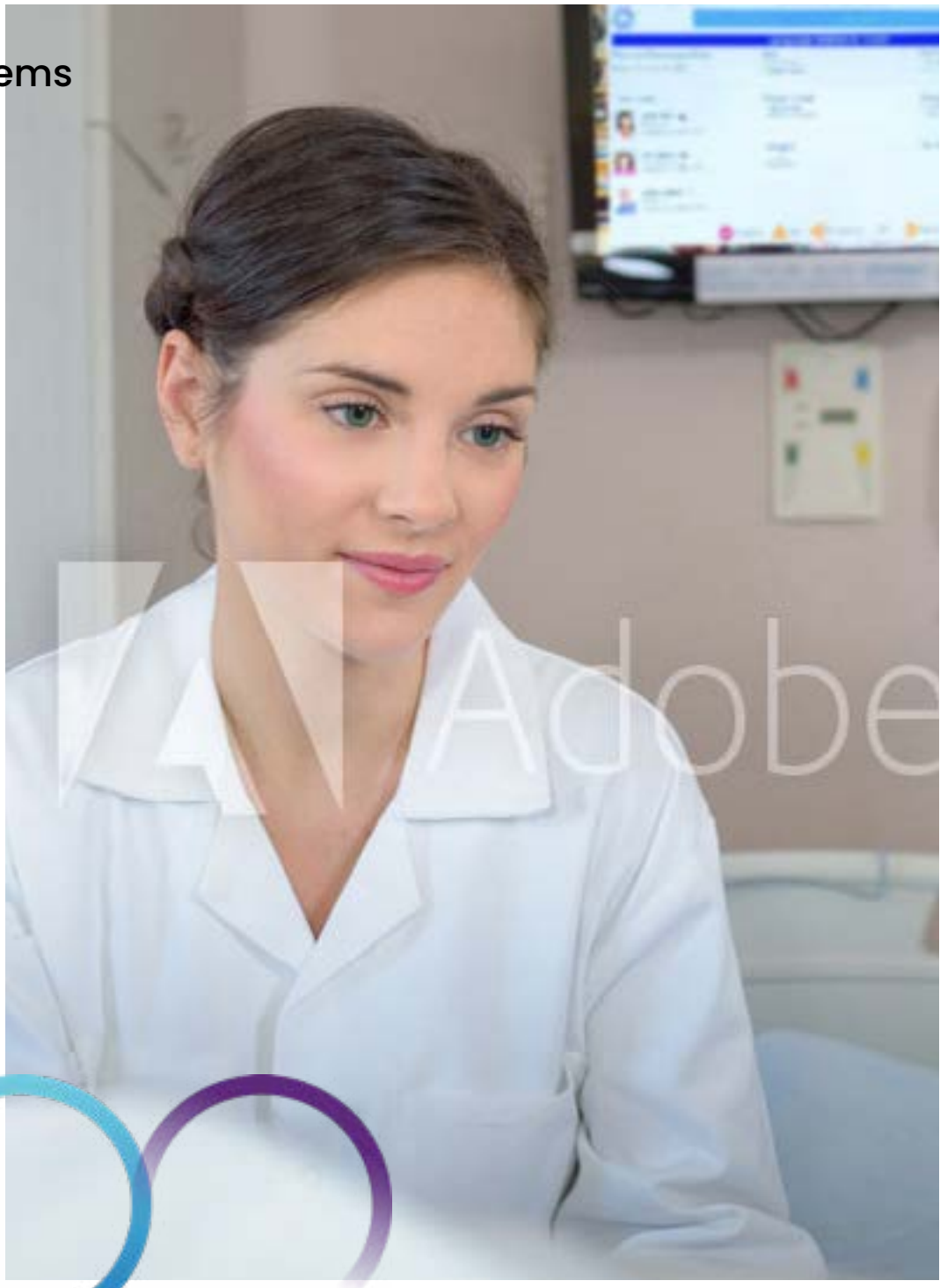
How Secure is Your Digital Front Door?

Balancing Access with Security in Patient Engagement Systems



Health care has a patient engagement conundrum: how to roll out the digital welcome mat and still keep the front door secure.

Information security depends on the foundational principles of confidentiality, integrity, and availability of data. All three are critical, but there are instances when one should be prioritized over the other. Theoretically, the most "secure" device is offline and probably largely unavailable. Thus, it's also fairly useless, especially as a tool for patient care, let alone patient engagement.

The key is finding the right balance in that three-legged stool—and the exact makeup of that balance will vary with the situation. For classified military information, confidentiality is paramount. In the financial arena, integrity wins out. In healthcare, availability of data can be a matter of life and death.

Access to data helps clinicians deliver the right care to the right person at the right time—improving quality of care and outcomes. Patients, too, are increasingly looking to connect with their providers and their health data via technology both in the hospital and from home. The rise of telehealth during the COVID-19 pandemic has only accentuated that trend.

The Internet of Medical Things (IoMT) expands each year. In 2018, Deloitte put the number of connected medical technologies at more than 500,000, including everything from ventilators, IV pumps and monitors to the SmartTVs in patient rooms. The connected medical market is predicted to increase by about one third by 2027.

While connected devices are an important part of the health care system and the data flow that makes health care work, "they create a much larger attack surface from the threat landscape perspective," says Russell Teague, Vice President, Advisory Services for Fortified Health Security, a managed security service provider that specializes in cybersecurity in the healthcare sector. "Each of those integrations creates an additional attack vector and increases the risk of security weaknesses being used as an entry point."

The challenge for health care organizations is to protect data while still making it readily accessible to the patients and providers who need it.

Health Care in the Cross Hairs

"Approaching security from an availability-first mindset is challenging," says Preston Duren, Director, Cybersecurity Operations for Fortified. "You can implement a million security protocols or completely lock down a connected device. However, if taking that device offline makes it harder for the end user, then you've essentially created a bigger problem than the one you set out to solve," says Duren.

Those problems become even larger when the end user is the patient, and the goal is patient engagement. "For anyone admitted to a hospital, receiving proper treatment and care is what they should be focused on," he says. "Which is why the goal of every hospital provide should be to offer a frictionless patient experience rather than add additional stress to an already taxing situation with products and solutions that are unfamiliar or complicated to access."

Meanwhile, health care is in the crosshairs. According to Forgerock, breaches involving usernames and passwords increased by 450 percent in 2020. More than one third of breaches occurred in health care, more than any other sector. Ransomware attacks were up across the board in 2020, but health care took the biggest hit as the pandemic made that sector both more vulnerable to attack and more likely to pay a ransom to avoid disrupting service.

Patients were concerned about data security even before this latest surge in cyberattacks. A 2018 survey by Aetna revealed that 76 percent of consumers had concerns about the security of medical data. Providers, too, take seriously the legal obligation to protect patient data as part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), but also their moral and ethical responsibility to patients.

> "I consider myself and [the security team] to be a part of the care team," says Arthur Ream, Chief Information Security Officer at Cambridge Health. "We're there to technically safeguard patients' data and make them feel safe, just like the providers are here to help them feel safe."

A data breach can greatly impact a patient or their family, he says. "It can cause credit problems; it can cause anxiety because their data is out there."

But security in a health care setting presents different challenges from other sectors, he says: "You don't want to be too restrictive that you slow the forward progress in the practice of medicine. But you don't want to be too loose. You've got to have that balance."

"Security is there to help protect the provider organization as well as the patients they serve," Duren adds. Patient engagement is an integral part of the business of delivering of quality health care and improved health outcomes.

It's also becoming increasingly obvious that cyber insurance is only a part of the solution. In the past, Teague says, hospitals leaned heavily on cyber insurance to recover from a major security incident. With cyber insurance coverage shrinking, premiums growing and some insurance companies pulling out of the healthcare market all together, providers are left with fewer options. Besides, Teague points out,

> "Insurance doesn't protect or help recover the impact to the provider brand, it doesn't protect patients' confidence or loyalty to the organization."

So, what's a health care organization to do?

Multi-Factored Solution

"It starts with investing in a robust cybersecurity program that goes beyond the basics by deploying advanced endpoint protection and adding multi-factor authentication to reduce threat surface areas. With these protocols in place, healthcare organizations know they have the proper capabilities to monitor, detect, respond and contain a major attack," says Teague.

"You have to use the best practices, a multi-factored, multi-layered approach to preventing and mitigating threats," adds Mitze Amoroso, Chief Information Officer of ArchCare, which provides a continuum of health care services to the elderly in New York City. You also have to be realistic and adapt your approach to the constantly changing health care security landscape. Amoroso admits that a few years ago, she had a goal of preventing any breach to the system, now she's more focused on mitigation and having systems in place to prevent, identify, and respond quickly and appropriately.

At ArchCare, that means strength in several critical areas, including security awareness education for all staff, cyberinsurance, constant monitoring of logs and tools, aggressive patching and updating cadence, and third-party vendor oversight. Her staff of 23 cover 30 locations 24/7—no mean feat. They can't do it alone—it takes the combined effort of all staff in the organization to protect against any attacks.

A large percent of malware attacks is delivered via email phishing. This attack strategy opens the door for malware, which in turn, pulls in the ransomware, Teague says. "This attack strategy doesn't happen in minutes; it often occurs over time and without the victim knowing." Being aware and having visibility is step one, being prepared and having the capability to respond quickly is step two. The faster an attack is detected and proactive response is taken, the less damage it causes.

> "At the end of the day, I'm only as good as my users, and my users in any location or environment are only as good as the weakest link," says Amoroso.

ArchCare conducts regular phishing simulations so that staff know what red flags to look for. They also send out videos on cybersecurity staff to watch each month. They created a whiteboard video series that explains security policies. During the pandemic, they also developed videos about cybersecurity at home that covered password and virus protection for both work-from-home and home entertainment. "We hope that education for the home will transcend to better cybersecurity for the business too," she says.

"We really take security very seriously," she adds, pointing to one academic medical center that estimates they lost $40-50 million because someone took a laptop on vacation. "If that happens to us, that's going to be really hard to sustain."

Third-Party Vendor Oversight

A multi-faceted security plan must extend beyond the health care organization itself. Careful evaluation of products and third-party vendors is another important piece of the puzzle.

Spending time assessing and reducing third-party vendor risk, paying particular attention to software for connected medical devices, Duren says. Understanding the function of the device or software and the other devices it needs to communicate with is a big part of understanding the risk involved. Devices should only access the information they need to function properly. Health care organizations typically have at least two separate networks, he explains: an operational network for medical devices overseen by the biomed or facilities department and a corporate IT network for financial data. A guest network for patients only gives access to the internet. However, it's important for biomed and IT to communicate about possible security concerns, such as a medical device that doesn't accommodate antivirus. A security team should oversee the overall strategy for securing the entire environment.

As part of the evaluation process, Arthur Ream recommends looking at how patients are using technology: their expectations and concerns. He suggests establishing a patient technology committee to allow actual patients to try out new technology and make recommendations to ensure safe and effective use by a variety of patients on a variety of platforms. The make-up of the committee should reflect the patient population served by the institution, he adds.

Third-party vendor oversight is also critical. Amoroso is a big believer in this. As part of the Request for Proposals process at ArchCare, she looks carefully at a prospective vendor's approach to security.

She admits that she has occasionally been accused of stifling innovation, although that is not her intent.

> "Sometimes security is not at the forefront of innovative technology, it's more an afterthought. I want to see security built into innovation," she says.

At ArchCare, any vendor that comes in contact with protected health information must submit a SOC 2 report both in the initial evaluation process and, if chosen, again every year. She also requires vendors fill out a security questionnaire. "It's not just a one-pager. It's 12," she says, with questions about security practices, safeguards and any breach that has occurred. "If you don't ask, how are you going to know?"

ArchCare also subscribes to a service that scores vendors in 10 security categories based on available public-facing information. This includes application security, patching cadence, and DNS controls. She matches that up with the questionnaire as a sort of double check. She'll consider a company with a score of A or B, but lower than that, she will opt for another vendor. If an existing vendor's score falls, she'll check with them to get more information.

Emphasizing third-party security is critical to ensuring the risk of a cyberattack is properly mitigated, says Teague, from several perspectives. Vendors serving health care organizations are more attractive targets than health care organizations themselves. Why attack one health care system when you can attack a vendor and potentially access several health care systems? Implementing a robust third-party security program to confirm security practices are being maintained is part of an organization's multilayered defense in addition to their own protections.

In addition, companies that offer cyber insurance are increasingly looking for their insureds to build their own security programs. Amoroso reports that a few years ago, renewing ArchCare's cyber insurance involved little more than signing on the dotted line and paying the bill. Now the renewal process involves a "mini security assessment."

Going Above and Beyond

All this is leading some large health care organizations to require HITRUST certification on top of SOC 2 and other audits. HITRUST is a security framework that combines requirements from some of the most commonly sought out security audits, including HIPAA, NIST, ISO, SOC 2, and more. The process—which can take 9 months to a year to complete—involves first completing a gap analysis to identify areas where HITRUST control requirements are not being met, a remediation process in which gaps are fixed, and a validated assessment that assures the vendor has implemented security protocols across 19 domains. "The average HITRUST assessment has about 280 controls requirements and you have to have a policy and procedure for all 280," says Justin Graham, HITRUST CCSFP Assessor for Tevora Health, a consulting firm that helps shepherd companies through the process.

Gaining this certification can be expensive, and when health care organizations require the certification that may drastically narrow the field of contenders in a given product line. But that extra assurance—and independent verification— can give an organization peace of mind.

Duren says that seeking the certification bodes well for a vendor's product. "It boils down to, does the vendor have a security program in place? If so, have they approached this with a security mindset that both provides a trusted environment as well as adds stakeholder confidence?" he says, adding HITRUST certification can really demonstrate that commitment.

Although Amoroso doesn't require HITRUST Certification from vendors, she certainly likes seeing it. "I look for all the certifications I can get," says Amoroso.

This is especially good news for patients, who simultaneously want more access to data and more protection for their data.

> "A company that is assessing and addressing risk is protecting their partners—the hospitals—and also protecting their partners' clients—the patients," Duren says.

When patients feel their data is protected, they feel more comfortable using the technology and engaging fully in their care. By blending innovation, usability, and security in their patient engagement systems, health care organizations can weave an ideal welcome mat that helps ensure patients keep returning for quality care.