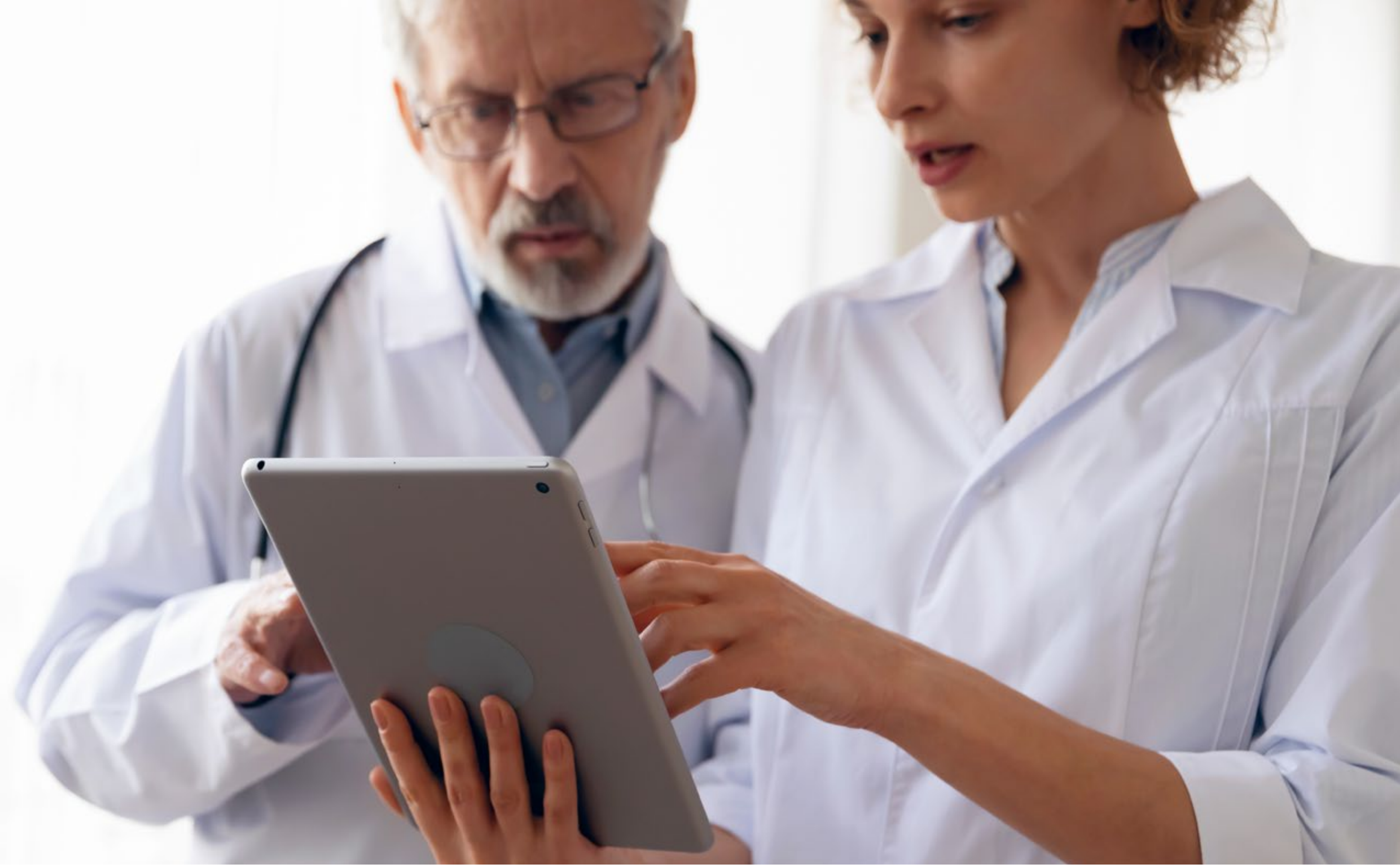
Protect your healthcare organization from cyber criminals



Beware the lurking security threat

Cyber threats take many forms, from sophisticated ransomware attacks carried out with the help of linguistics teams to clumsy intrusions by low-level recreational hackers. They can happen within your organization or sneak in through third-party vendors. Electronic threats are constantly evolving, and healthcare organizations need to be vigilant and nimble to respond effectively.

Intrusions can sneak in through third-party vendors

During a February 16, 2022 HealthLeaders webinar, *Securing the Healthcare Enterprise in 'The New Normal'*, presenters Christine Wheaton, Chief Privacy and Security Officer at Henry Ford Health in Detroit, MI and Jacqueline Sullivan, VP of Security Operations Coordination for Minneapolis-based U.S. Bank, discussed some of the most pressing cybersecurity threats facing health systems and some strategies that organizations can use to protect against them.

Identifying the threat

Ransomware attacks are currently the number one threat to healthcare organizations, according to Wheaton and Sullivan. Hackers break into a system and steal patient health records, financial data, or other sensitive information, and demand money to release it. While there are exceptions, most of this nefarious cyber activity is financially driven, says Wheaton.

“Years ago, when we first started hearing about ransomware it was targeting individuals,” says Sullivan. Hackers now are often targeting organizations using some of the same methods – most often phishing emails. Once they’re in, they linger in the system.

“It’s not just about navigating a network, but it’s actually a human looking around to locate the crown jewels of the organization,” says Sullivan. When the intruder identifies that information, they may encrypt it or even move the data out the network and demand money for its return.

Cyberattacks are also hitting new targets, says Wheaton. “We’re seeing more concern with potential threats to medical devices, as well as medical record and imaging-type, or laboratory data integrity-type attacks.”

Security intrusions often occur through third-party vendors. For example, if your organization uses an outsourced call center that’s connected to your network, it opens up a lot of avenues for risk, says Sullivan.

During the pandemic there was an uptick in intrusions to third-party video calls

Cyber threats may also come from untraditional sources. During the pandemic there was an uptick in intrusions to third-party video calls and threats related to devices inside the home, because more staff members were working remotely. Household printers, Alexa enabled speakers and even Wi-Fi enabled home appliances, can pose risks. “We weren’t thinking that a washing machine could be an avenue for attack. But you have all these devices at home and they are constantly listening,” Sullivan says.

Addressing the threat

Because risk arises from many sources, an organization's cybersecurity program needs to be multifaceted. It should include the following:

1. COMPREHENSIVE TRAINING

Despite increasingly sophisticated cyberattacks, tried and true cybersecurity practices still hold up, says Sullivan. These include:

- making sure that your workforce is getting periodic cybersecurity safety training
- ensuring that staff members are aware of the risks around the data
- establishing and maintaining strong passwords
- enabling multi-factor authentication

People working for the healthcare organizations and patients need to know where threats lie, common methods used to compromise a system, and what they should do if a problem arises, or they see something unusual. "You need to make sure people know how to report when they see these things," says Wheaton.

Create barriers between devices used inside and outside the organization

2. PROACTIVE PRACTICES

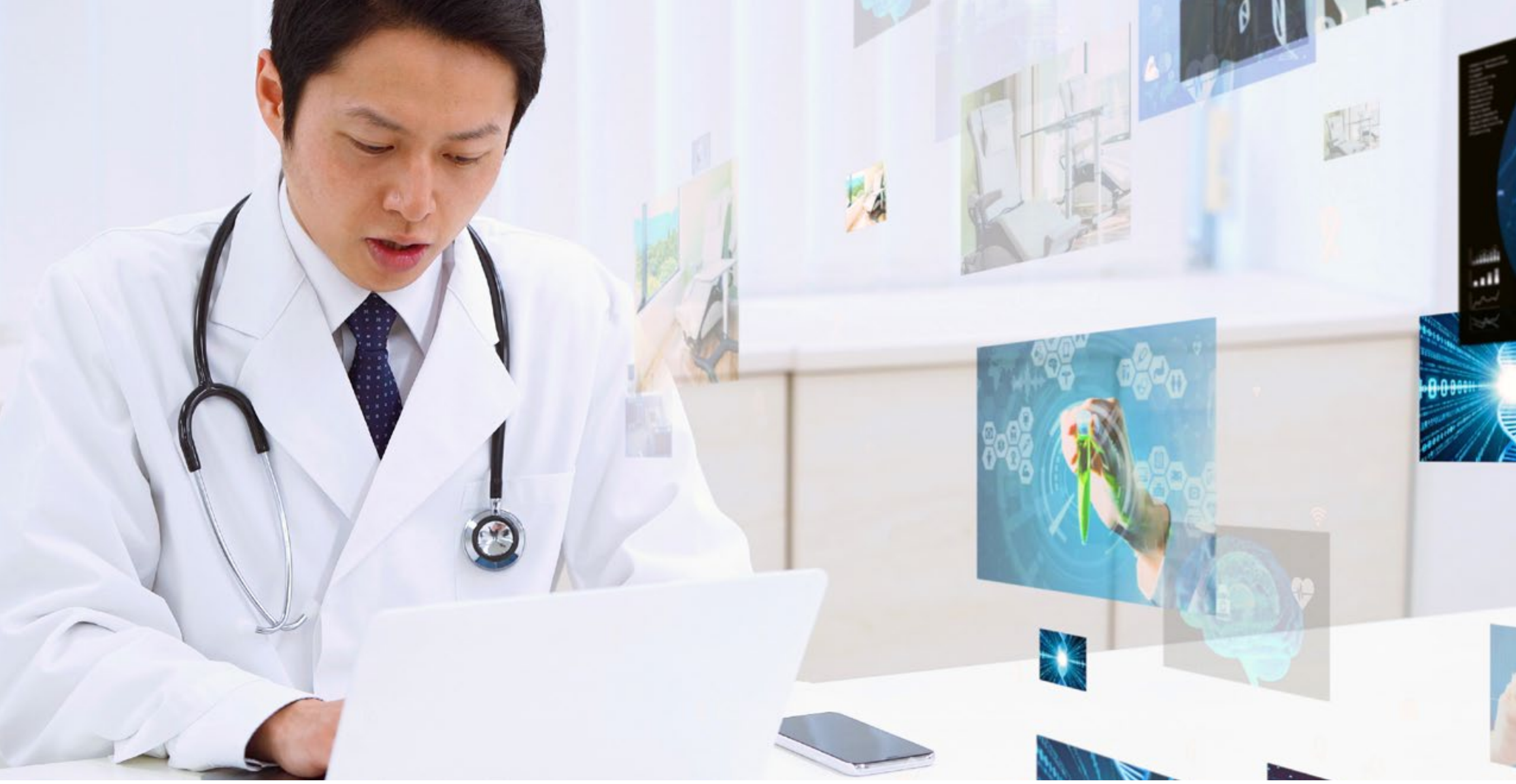
Security should not be an afterthought.

"When people are looking at a new solution, a new medical device, even a new web-application solution, we want to be there, we want to be involved," Wheaton says. The goal is to perform a third-party risk assessment and a solution-security assessment. The same is true of identity and access management. "Now, we're looking more broadly at what are the medical devices doing to become authenticated and authorized to share data and connect to our network," says Wheaton.

Don't overlook devices used at home or those that are not considered a traditional threat. Even simple programs and software, or seemingly innocuous devices, such as home printers, need to have up-to-date security features and comprehensive-use policies, says Sullivan. When possible, create barriers between devices used inside and outside the organization.

"In some cases, you can have an entirely separate network for these devices that aren't corporate managed and that's a really good practice to do that," says Wheaton.

Be on the alert for security gaps in seemingly secure technology. For example, texts sent using the Apple® voice feature are monitored for quality by Apple personnel. This means that someone using this feature on a hospital-issued phone might be exposing information to outside parties," Wheaton continued.



3. IDENTIFY YOUR WEAKNESSES

Each organization should identify its unique vulnerabilities.

“You need to have a good workflow defined between the folks on your team who are ingesting and understanding these vulnerabilities and establishing risk with the teams in IT who manage the assets and who can remediate,” says Wheaton.

Challenge your systems using independent third-party penetration testing. It can find weak spots before hackers do. “That will help make sure that your protections are evolving because the penetration testers evolve their tests,” says Wheaton.

Organizations also need to have a clear plan in place if problems arise. Establish a response team that includes crucial groups from throughout the organization so that your organization is ready to address threats quickly and comprehensively, says Wheaton.

4. VET YOUR VENDORS

Your organization needs ensure that third-party vendors have adequate cybersecurity measures in place.

Periodic quality checks can help spot potential threats or lapses. Also, establish breach protocols for these vendors. They should spell out a clear process for both reporting and follow-up, says Wheaton.

Detect vulnerabilities before hackers do

ABOUT U.S. BANK

Our healthcare industry team understands the nuances of your industry and provide personalized guidance to help keep your revenue cycle and financial operations running smoothly. We offer banking, payment and investment solutions to enable your organization to deliver a better patient financial experience and sustain healthy revenue.

For more information, please visit Healthcare Finance Services | U.S Bank.

ABOUT THE PANELISTS

Christine Wheaton, *Chief Privacy and Security Officer at Henry Ford Health*
Christine is a digital technology executive and strategic information security specialist with more than 25 years of experience building and leading large-scale global teams and information technology programs. Recognized as a leader with a strong technical foundation, she is an excellent driver of capability and organizational change.

Jacqueline Sullivan, *VP of Security Operations Coordination at U.S. Bank*
Jackie is the Vice President for Security Operations Coordination with U.S. Bank's information security organization and a former board member for the National Cyber Security Alliance. With more than 15 years of progressive experience, Jackie is the owner of the social engineering vertical within U.S. Bank.

Alexa is a trademark of Amazon.com, Inc. or its affliates. Apple is a trademark of Apple, Inc.

This document is prepared by U.S. Bank Payment Services as a service for its customers. The information discussed is general in nature and may not apply to your specific situation. 0522 CR-21208268