Article

Measures for Protecting Patients and Providers:
The role of IT security in remote patient monitoring and recommendations for securing connected health programs

"Greater uptake of mobile digital technology in the work arena will confer immense clinical benefits within the NHS. Clarity about information governance processes, assurances over data security and dissemination of clear communication to frontline health professionals regarding both these aspects are the need of the hour."

– Séan Matheiken, Consultant Vascular Surgeon and Digital Health Innovator
London, UK
@bloodysurgeon

Given the wealth of sensitive personal data healthcare organizations process and store, it's no surprise that hospitals, medical offices, and other healthcare organizations are prime targets for cybercrime. As attacks get more sophisticated and the consequences of a breach more severe, security hardening across the operation becomes imperative.

Many organizations are counting on their firewalls to protect the data and devices within the network, but this isn't enough. It's becoming much easier for hackers to break into networks through under-secured endpoints like IoT devices, PCs, and printers. In a typical organization, the number of endpoints is much greater than the number of servers, sometimes as many as two devices per employee. Consider all the computers and printers healthcare workers use throughout the day—including portable devices used in patient rooms and laptops taken home for use after-hours. The sheer volume of endpoints increases the risk. Just one stolen or vulnerable device can provide entry to the network, expose sensitive data, and put the entire infrastructure at risk. That's why it's so important to deploy devices with built-in security protections that can detect and automatically recover from attacks.

This is also true for devices deployed to patients as part of population health management (PHM) programs designed to provide remote patient monitoring (RPM) and digitally connected coordination of care. Many overlook this potential threat, especially those who elect to implement a bring your own device (BYOD) model. BYOD models are PHM programs in which patients are asked to install apps on their personal smart phones, tablets, or notebooks for purposes of periodically collecting health-related data. Many organizations are trying to strike a balance between the equipment necessary to deliver RPM programs and the overall cost of operating such programs. However, among the plethora of reasons for why such models are not optimal is the lack of visibility and control over personal devices. The ability to reduce the exposure to risk that such a deployment model may introduce to your organization is limited.

Challenges and risk points

At the enterprise level. Healthcare organizations spend a lot of time and money making sure firewalls are strong and the server infrastructure is protected. But what about endpoints like mobile devices? If they become compromised, the entire network—and patient data connected to it—can be at risk.

At the user level. Users pose another security risk that is often neglected. Users can be hacked more easily than their devices through deception. For instance, PC users can be tricked into

"Four in ten US physicians want regulation and standards in the provision of connected health and technology."

– Reena Sangar, Head of Digital Health, Ipsos (Ipsos Digital Doctor report, 2017)

browsing a fraudulent website that can infect their machine with malware. Another common vector is opening an infected email attachment.

At the endpoint level. Unsecured endpoints like PCs and smartphones can open the entire network to attack. But managing the security of PCs and smartphones can take a lot of time and expertise. Many IT administrators still use laborious, manual processes which can drive up costs. Across a large fleet of devices, this inevitably leaves individual devices out of compliance and at higher risk.

Recommendations

HP has devised a comprehensive suite of security measures that keep your organization and your patients secure. Here are a few of our recommendations. For more details visit HP Security.

Secure devices at the BIOS level. All devices—PCs, printers, and mobile devices, including smartphones and tablets—start using firmware called BIOS (Basic Input Output System). The BIOS is responsible for controlling the basic functions of a computing device. It's the critical layer between the underlying hardware and the operating system. This is core to how the PCs, printers, and smartphones operate, so an unsecured BIOS can offer a dangerous amount of access to a hacker.

Protect against user-initiated malware. The average user receives 16 malevolent emails per month. Isolating a web browser in a hardware-enforced virtual container can help prevent watering hole and browser drive-by attacks from clicking on malicious links. Similarly, isolating common documents, which are attached to emails, can also prevent embedded malware from harming the PC and data.*

Secure data. The first step to protecting data is to make sure that only authorized users can access devices and the networks to which they are connected. Even in a home-based monitoring program, this is important. Individuals other than the patient, such as personal caregivers, may need access to devices. Biometrics and multi-factor authentication can help protect PCs and identities. In some instances, for example in the case of home health workers, fleet-wide authentication solutions should be implemented that require users to enter more than just a password. Adding a fingerprint or scanning a badge is a more secure authentication solution. Also, data should be encrypted on the device, especially for mobile devices.

Manage and monitor devices. Unsecured endpoints like PCs and mobile devices can open the entire network to attack. But managing the security of these devices can take a lot of time and expertise. Many IT administrators still use laborious, manual processes, which can drive up costs. Across a large fleet of devices, this inevitably leaves individual devices out of compliance and at higher risk.

Protect patients. Safeguarding patient information is vital and, if not properly managed and secured, may even be life threatening. One way to protect against potential harm is to monitor peripheral devices. Monitor connections to extended endpoints such as Bluetooth® and USB-connected biometric devices. Monitoring, detecting, and alerting of irregular or weak signals can help keep patients safe and your network secure.

Reduce risk now

Build a better defense today. It's time to take proactive steps to reduce risk and help secure patient data. Security can be complicated, but HP offers hardware and solutions that make it easier for healthcare organizations to protect patients, secure data, address user vulnerabilities, streamline management, improve compliance, and reduce costs.

About

HP offers solutions that save time and help reduce costs and resources to maintain security across a fleet of devices and at every level. For more information, or to schedule a thorough risk assessment, contact your HP representative today.

* Symantec Internet Security Threat Report, March 2018

Sign up for updates
hp.com/go/getupdated

Share with colleagues

4AA7-4818ENW, March 2019