Keeping health systems safe is increasingly difficult, but not impossible

This is the second Insight in our 3-part series outlining challenges health systems must face when choosing smart devices, upgrading security and network reliability to support clinical communication and collaboration technologies. This Insight focuses on Security and the additional activities that need to be addressed once a new smart device is chosen.

Security

With the increase in cyberattacks and ransomware, health systems are doing everything they can to keep their systems safe. Security for devices is based on the type of device, operating system and version being run. There are known issues with all the operating systems out there, and manufacturers send out security patches all the time. But malicious hackers are always looking for a new way to break into systems and security and IT departments must stay ahead of the curve.

But it's not just the increase in cyberattacks and ransomware that health systems must manage. Due to the sensitive nature of patient health information, IT departments are responsible for various types of security on devices including multi-layer user authentication and authorization, and sometimes even biological authentication, to ensure PHI remains safe.

A separate challenge is that most providers are using their own devices for communications (usually smartphones). This requires that health systems set up a *separate* set of rules for BYOD situation than for hospital-owned devices. This could include educating those using their own devices on how to identify apps they can safely download, as well as making sure they download their device's specific system updates on a regular basis.

Dealing with the security challenges of BYOD ***and*** health system-owned devices adds another layer of complexity when upgrading technology

Health systems also must consider including an MDM (mobile device management) policy on both BYOD and health system-owned devices in case these devices are lost or stolen. Having an MDM solution can provide several safeguards to the devices deployed in your enterprise. They allow the health system to control updates from an OS level down to the applications used on the devices. Controlling these elements leads to less vulnerability in being exploited.

Health systems should subscribe to the security bulletins for their device manufacturer as well as the operating system specifically, so the security team is alerted when an exploit does come to the surface. Patches can be quickly downloaded, or the problem can be blocked before it infiltrates the health system.

Basic MDM can control sign-ons and wiping devices, but many health systems are looking for even more control from a security and compliance standpoint. This is where Enterprise Mobility Management (EMM) comes in. EMM provides the health system full control of devices, including pushing out software updates, controlling the security, wiping information if needed, and even managing the end-user experience like screen savers.

Security of devices is an integral part of insuring PHI stays safe on a clinical communication and collaboration platform – but you need to make sure teams can use devices anywhere inside and outside of the hospital. The third Insight in our Voice series will cover network connectivity and reliability.

Read about best practices in choosing a new device for your health system
Smart Devices in a 24/7/365 Work Enviroment

Author

MYRON WALLACE
VP of Commercial Enterprise Technologies, Halo Communications

As VP of Commercial Enterprise Technologies, Myron Wallace is responsible for the ongoing evolution of collaboration technologies at Halo Communications. He is an advocate for the utilization of emerging technologies leveraging cloud strategy, engineering, and architecture to drive revenue, cost control and network efficiencies.