You Can Implement the Right Endpoint Security Solutions to Solve Your Hospital BYOD Challenges

by Jenny Kanevsky | Dec 23, 2020 | Healthcare | 0 comments

According to Forbes, hospitals are facing new and evolving mobile security challenges, now more than ever. Telemedicine, remote data access, and Bring Your Own Device (BYOD) programs put Protected Health Information (PHI) at significant risk. Hospitals must adapt to keep up with growing virtual care trends.

Security teams must consider numerous variables when developing a mobile security plan, including healthcare regulatory requirements like HIPAA, patient and provider risk tolerance, and internal and external threats. Determining these baseline parameters is essential when establishing an organization's mobile security policies and procedures.

Consider Your Organization's Unique Factors

Mobile security needs vary based on several factors. Even within the same industry, organizations have different goals, IT infrastructures, ratios of remote to onsite workers, and security profiles.

Enterprises should consider all factors when deciding how to execute a mobile security strategy. These variables include workforce trends and employee preferences, cost considerations, and administrative management issues. Security leadership must evaluate, compare, and select one or more tools to implement.

Workforce Trends

The remote workforce model is here to stay. According to the Harvard Business Review, COVID-19 has changed talent acquisition and management indefinitely. Mobile security solutions must meet a healthcare organization's current remote workforce needs and accommodate future growth.

The trend towards BYOD shows no signs of reversing. Employers enjoy the cost-saving benefits since they don't need to supply or maintain devices. Employees appreciate the accessibility and convenience of using personal devices. But, depending on the chosen BYOD solution, employee privacy can be an issue. Hospitals that implement BYOD with Mobile Device Management (MDM) solutions risk employee dissatisfaction because MDM gives IT full control of end-user devices. However, BYOD can maintain employee privacy when a Virtual Mobility Solution (VMS) is implemented. Hospitals seeking increased productivity, flexible-care options, and a competitive edge will prioritize an effective, employee-friendly BYOD policy.

Regardless of a healthcare organization's strategy, planning for BYOD and a growing remote workforce is necessary. Any solution must be scalable to accommodate future expansion. As your workforce grows, so does your BYOD program. Selecting a mobility solution that will meet your organization's evolving needs and attract and retain empowered employees is critical to future success.

Implementation Challenges

Many healthcare organizations consider MDM as the only mobile security option. This solution was once the obvious choice. However, in addition to employee privacy concerns, IT administrators should consider other MDM drawbacks.
Healthcare organizations handle large amounts of sensitive data, including PHI and proprietary business and financial information. An effective mobile security strategy must prioritize protecting this information.

MDM relies on securing devices rather than data, so strict, sometimes overreaching BYOD protocols are necessary. Employees often resist policy adoption or circumvent security protocols to enhance productivity and protect personal privacy. PHI is confidential data, so there's no room for system failure. One employee oversight or technical issue would lead to a substantial data breach and subsequent HIPAA violation.

When employees access organizational resources off-site or with personal devices, MDM offers minimal data control. If an employee views or edits data with an unapproved application or backs it up in a personal cloud, exposure risks dramatically increase.

What Does it Cost?

Cost is a significant concern for any IT solution, and BYOD is no different. When employees use their own devices, there are immediate cost savings. No hardware purchase is required. However, some organizations will continue to issue devices, such as uniform tablets used hospital-wide that can also be employed at home and for in-home patient visits. The purchase of these devices is a sunk cost.

However, with an MDM solution, maintenance of these devices is expensive. With MDM, IT must continually maintain, manage, and update every device. Alternatively, IT can centrally manage both company-issued BYOD and employee-owned devices with a virtual solution, substantially lowering an organization's financial investment.

Administrative resources represent a variable cost that security executives should keep in mind. Centrally managed devices and associated servers and admin consoles are significantly less costly than individually controlled devices. When addressing an organizations' mobile security needs, weigh the costs of MDM against Virtual Mobility.

Endpoint Security Solutions

Hospitals need endpoint security solutions that foster BYOD adoption, grow with increasing remote care and workplace demands, and are budget-conscious. Striking a balance between data protection, regulatory compliance, and organizational efficiency is possible once IT leaders look beyond traditional MDM solutions.

Hypori Virtual Mobility™ is a scalable, secure, and cost-effective endpoint security solution that empowers healthcare organizations to make the remote transition. Hypori® provides a streamlined virtual experience that connects employees to enterprise data through a user-friendly app.

Hypori's innovative design keeps organizational data on the corporate network and completely separate from personal data. A centralized administration hub allows IT to ensure that protected data is accessed, modified, and transmitted using approved applications.

Hypori equips healthcare organizations with the tools and flexibility to meet today's mobile security challenges. It integrates mobile security with the best features of virtualization to enable rapid enterprise deployment and efficient management. Hypori is healthcare's productivity solution.

Healthcare is the #1 Most Cyberattacked Industry
But You Can Be Safe With Hypori Virtual Mobility

Learn More in Our Free Webinar
Maximizing Mobile Device Security in Healthcare

WATCH NOW