OPTUM™

TechTarget Custom Media

A TECHTARGET WHITE PAPER

# Security Implications of BYOD in Health Care

White Paper

Technology is reshaping how health care operates, requiring new approaches to information and cyber security. Advancements in mobile technologies provide physicians and nurses with new tools to deliver care and stay connected to patients outside of the four walls of a hospital or clinic. In addition to clinicians, administrators and patients are also demanding remote access to medical and financial records, often using their own devices.

Mobile capabilities can enhance how clinicians deliver care, patients experience care, and administrators support operations. However, increased mobility, the Internet of Things (IoT), and bring your own device (BYOD) can also expose an organization to new vulnerabilities across the technology environment, especially at endpoints. Hospitals and health systems must be able to balance all end-user needs and expectations when adopting mobile, BYOD, and other digital capabilities.

## Unique impacts of BYOD on health care security

There is increasing convergence when it comes to health data and devices that interact with the health care environment. In the health care industry, BYOD and IoT trends mean patients and clinicians are using smart devices to generate and access medical data. These devices can also connect to a hospital or health care practice's core network. This exchange of data and enhanced connectivity is convenient, but it can also bring massive risk.

"The risk of BYOD is high and on the rise".

BYOD brings increased responsibility for clinicians when they use personal devices in their professional lives. Clinicians can be easy targets for cyberattacks. A simple email attack can become a bridge between a BYOD device and a hospital's entire network. Medical information is also highly distributed information, which means some clinical functions, such as reading and signing radiology images, can be outsourced. Exchanging information with third parties outside of the protected network, or providing access to these networks, increases security risks.

In order to ensure that clinicians can safely share and access medical information, the IT organization should consider implementing protection controls that:

1. Determine the right environment;
2. Establish ease of use;
3. Enhance security for patients and the organization;
4. Determine what the security protocol will allow for BYOD devices;
5. Ensure proper segmentation on wireless and BYOD devices; and
6. Isolate, encrypt, and protect data if a device is lost, stolen, or exposed to third-party malware.

## The most overlooked gaps in health care security

The movement toward a more connected and integrated health care ecosystem is beneficial for both patients and clinicians. However, the distributed and shared nature of the health care ecosystem opens up a whole new world of control challenges that make health information especially vulnerable. Some of the gaps include:

### User-installed tools:

One of the most overlooked security gaps in health care is using BYOD and wireless IoT devices without security controls in place to protect to protect sensitive data. For example, if the device owner has installed jailbreak tools (a software tool designed to remove restrictions imposed by the operating system [OS]), the device is unlocked, or there is no corporate hygiene established for how the device interacts with the core network, the organization is at high risk for data leaks.

### Medical devices:

Medical devices that are closed-system, have an unprotected or out-of-date OS, or have a modified OS, are potential vulnerable pathways for cyber attacks. When a health care organization connects third-party devices with unknown security controls to their corporate environments or relies on the manufacturer for security, they're making themselves an easy target for attacks.

### Lack of awareness:

Health care IT often fails to understand employee technology behavior that may leave the organization at risk for phishing attacks. A lack of employee awareness about phishing scams also increases the likelihood that the organization will fall prey to a phishing attack.

### Lack of monitoring:

Malware is becoming more and more sophisticated, infecting organizations of all sizes every day. Malware can bring operations to a standstill, or it can remain undetected for years, allowing unauthorized access to networks.

## Recommended BYOD practices in a health care environment

BYOD is here to stay. This section includes some best practices as well as things to watch out for when implementing BYOD in a health care environment.

### Safely enabling a BYOD culture

Organizations that still have a "no BYOD" policy are finding that strict policies aren't entirely enforceable. Technology is so user-friendly that end users can easily find ways to access or download sensitive corporate and health data to their personal devices. As a result, there's no hygiene established, no monitoring or even rudimentary security around personal devices in the workplace. This only results in more security vulnerabilities and threats than if the organization allowed BYOD in the first place.

Other organizations are grappling with how to safely enable BYOD while conforming to data protection regulations and best practices. There is a spectrum of ways to approach BYOD security in a health care setting, but the objective is to make it easy for clinicians to continue owning and using their own devices, while establishing health checks that protect medical data.

### Mobile security without cumbersome logins

Securing data as it passes through mobile devices, and securing the devices themselves, is a unique challenge. The health care practice needs security on par with what's at stake, but clinicians won't tolerate cumbersome endpoint security protocols.

### Use of device containers

Device containers give organizations the ability to apply partitions on a BYOD device where corporate apps and data are housed. Security protocols only apply to what's in the "container" and not what's on the entire device. While this approach provides some security, it still leaves vulnerabilities in the BYOD strategy.

### Application management

With application management, clinicians can download and use corporate-sanctioned apps on their own devices. This approach makes apps easy to manage, but it doesn't provide enough data security.

### Content lockers

Content lockers are usually add-ons to container solutions. Content lockers funnel data into a secure repository, giving clinicians access to corporate data from their own device. This approach makes it easy for administrators to control data, but still leaves the device itself vulnerable, which leaves the network vulnerable.

### Virtual desktops (VDI)

VDIs allow a device to host a corporate desktop virtual machine. All corporate data stays in the data center. However, additional measures also need to be taken to ensure the device itself is secure.

### Updated approach to endpoint security

Traditional approaches to mobile security aren't enough. Even if IT has network protections against malware, monitoring tools, or antivirus, as soon as an employee disconnects from the corporate network and connects to an unsecured network, they risk infecting their device. Once an employee brings an infected device into the corporate network, the network is now subjected to the lowest security level. There is too much at stake for health care organizations to operate with coffee shop- or hotel-level security.

Instead, the organization must have security outside of the network that isolates the data logically from the device. IT must establish increasing controls, and ensure they persist to all endpoints. For example, if a clinician has a smartphone with jailbreak software, they will be blocked from interacting with the corporate network. The IT team must also enable antivirus, and tools to prevent phishing, malware, and plagueware on endpoints. User privileges must be assigned on a need to know basis, by establishing controls that restrict or forbid access to organization information assets when the user is disconnected from the organizations network. BYOD permissions are enforced by policy once the user is connected.

## Assessing your BYOD strategy

Identifying vulnerabilities and threats and establishing a BYOD strategy that keeps health care data secure without impeding the convenience and benefits of BYOD for the end user is a complicated endeavor. The best approach to a streamlined, secure BYOD policy is to partner with an experienced consultant who understands the changing technology and threat landscape and the unique risks and workflows of health care IT.

BYOD can help clinicians deliver better patient care and increase mobility, communication, and quality of life. However, connecting privately owned devices to the corporate network can expose the health practice to data leaks. BYOD can enhance a health practice, but it's important to balance end-user needs with stringent security requirements.

## Partnering with Optum for an integrated approach to security

Optum is a health services and innovation company, dedicated to modernizing infrastructure, advancing care, and empowering consumers. With more than 100,000 people worldwide, Optum brings the necessary expertise to advance health care security in a digital world.

Optum's security solutions cover the spectrum of your information and network security needs, assessing your organization's exposure to threats and vulnerabilities, shoring up security infrastructure and managing your security operations while also helping to minimize threats and protect highly personal and sensitive data.

Learn more about how Optum can address overlooked gaps in your security strategy and help your organization move toward a more integrated security approach, visit **www.optum.com/security**.


**visit www.optum.com**

11000 Optum Circle, Eden Prairie, MN 55344