As healthcare providers integrate technologies to improve efficiency, cost-effectiveness, patient outcomes, and compliance with government initiatives, complex IT infrastructures may simultaneously raise their IT risk exposure. Network-connected medical devices, in particular, may create vectors for attacks on networks, on the devices themselves, and on the patient information they contain.

It raises special concerns when medical devices and Electronic Medical Records (EMR) systems share network infrastructures to integrate information within and across facilities. Complex, distributed, inconsistently secured systems are vulnerable to malware attacks, and can be exploited for access to patients' most personal information.

Medical Device Challenges
Device-specific and external factors combine to make medical devices hard to protect. Devices are:

- **Growing more complex**, and therefore more likely to be connected to core IT networks
- **Tightly regulated** by FDA, CE, and others, extending their lifecycles and raising the cost of updates
- **Configured by manufacturers**, limiting hospitals' ability to embed protection
- **Long-lived**, so that many designs still in service never anticipated today's threats
- **Managed separately from networks**, typically by Biomedical Engineering instead of IT

External factors to consider include:

- A **dangerous threat landscape**, with exponential increases in highly sophisticated malware
- **More and tighter regulations**, especially for privacy and security

- **Out-of-date security strategies**, inadequate to withstand today's sophisticated attacks
- Poorly protected medical devices exposed to attacks across networks, on removable media, and from within
- **Standard software**, operating systems, and network technologies, exposing medical devices to the full range of IT risks

Risk Assessment
Medical devices introduce distinct cyber security and privacy risks, each with its own challenges.

Cyber security attacks, outlined in Figure 1, include:

- **Network-based attacks**—traditional IT malware introduced over a network
- **Removable-media attacks**, for example introduced during support or maintenance
- **Device-introduced attacks** from devices returned after repair, or demonstrator or loaner systems
- **Network proliferation**—attacks that use a device as a point of entry, then penetrate the enterprise by exploiting similar devices

IEC 80001² and other standards offer guidance on protecting networked medical devices using a risk-management approach.

---

2. IEC 80001 “Application of Risk Management for IT Networks Incorporating Medical Devices”
Security Risks

Figure 1: Cyber attacks reach medical devices over the network, on portable media, or during lifecycle events—and then spread on the network.

Healthcare IT systems must safeguard electronic Protected Health Information (ePHI), including information stored or transmitted by medical devices.

ePHI concerns, outlined in Fig. 2, include:

- **Network breach**, using network-based techniques to gain access to ePHI on the device
- **Interception**, for example of unencrypted wireless transmissions or backup data
- **Removable-media breach** copying ePHI from the device to portable media
- **Device breach**, when a stolen, out-for-repair, or end-of-life device leaves the facility carrying unencrypted ePHI

Assessing risks for a specific device requires understanding the ePHI it carries: how much data, transient or permanent, means of access, and so on. This information can be requested from the device manufacturer, for example through the NEMA MDS[2] form.³

Privacy Risks

Figure 2: Electronic Protected Health Information (ePHI) breach and interception vectors parallel those of cyber attacks.

Protective Strategies

With so many medical devices spread across complex organizational and IT landscapes, the right processes and tools are essential for success (see Fig. 3). Only comprehensive risk management can secure today's complex medical device infrastructure and protect the data it contains:

- **Asset discovery**—Symantec’s Altiris™ solution allows automated discovery of networked devices, and manual management of non-networked devices.
- **Configuration control**—Symantec’s Altiris solution obtains system parameters like OS and patch level, for identification and remediation of risks.
- **Process and policy management**—Symantec’s Workflow tool helps manage lifecycle events such as maintenance schedules, and management processes such as device onboarding or end-of-life.
- **Device cyber security**—antivirus technologies for embedded systems—especially medical devices—are compromised by the need to update definitions and the risk of false positives. Instead, Symantec’s Critical System Protection uses an intrusion prevention (whitelisting) approach that protects the device against malware and allows for tight control of device

configuration (lockdown), reducing risks and management burdens.

- **Network and device access control**—access to devices and their network connections should be tightly controlled. Policies can enforce cyber security protections when inadequate technical controls are embedded by the manufacturer.

- **Encryption and key management**—proper network-layer encryption is essential to reduce risks of clear text interception of ePHI, especially with wireless devices. Symantec’s PGP™ products provide key management as well as encryption—essential in complex environments with many devices.

**Protective Strategy**

*Figure 3: Comprehensive device management blocks threat vectors and secures devices during critical lifecycle events.*

**Conclusion**

Symantec is taking a leading role in developing medical device protection strategies. Hospitals can use Symantec’s suite of products to reduce the risk medical devices pose to their IT infrastructure, and use those same solutions to manage their entire IT environment. Visit [www.symantec.com/healthcare](http://www.symantec.com/healthcare) and learn how we can help you identify, manage, and mitigate your risks.