Out of Sight, Out of Control:
Reversing hidden patient safety, data security & compliance risks unique to medical devices
Out of Sight, Out of Control:
Reversing hidden patient safety, ePHI security and compliance risks unique to medical devices.

The 30-Second Overview
Healthcare providers who fail HIPAA audits, put patients and their data at risk often share a common oversight: They’ve failed to identify every place where electronic protected health information (ePHI) is stored in their organization.

One widespread blind spot are medical devices that capture, store and transmit patient data on a regular basis. With a typical hospital averaging two medical devices per bed, failure to secure such devices presents two chief threats:

1. You can’t assess and secure ePHI if you don’t know where it resides.
2. Patient safety may be compromised by corrupted data or output of unsecured medical devices.

From data loss to patient misdiagnosis and the hefty penalties that follow, learn how to pinpoint and counter the risks that have impaired data security and compliance for many of your peers.

Learning Objectives:
- Identify hidden patient safety, data security and compliance risks unique to medical devices.
- Examine the business, clinical and legal repercussions of these common oversights.
- Identify action steps to minimize or reverse risks.

Your Challenge
As you work to protect your IT network, connected devices, and the patient data flowing through them, independent audits routinely expose a common blind spot and springboard for patient data breaches and even misdiagnosis: unsecured medical devices.

A typical healthcare facility averages about two medical devices per bed — from pulse oximeters to ultrasound machines and CT scanners — all collecting, maintaining and transmitting ePHI through the facility’s IT network and connected devices, daily.

Let’s say you’re faced with a HIPAA or Meaningful Use auditor. One of the first questions they would ask you is this: “Did you complete a risk assessment of all devices that hold ePHI?”

Often the answer is “no.” Because medical devices are unconventional, FDA-regulated machines (as opposed to traditional computers), they tend to fall outside the IT department’s expertise or scope of work. In turn, these devices often get left out of risk assessments, security and compliance efforts — an automatic “fail” of both HIPAA Security Rule and Meaningful Use attestation.
What’s at Risk?

As it happens, a lot. Failure to secure connected medical devices leaves facilities like yours vulnerable to a variety of risks, including:

- **Average cost of a breach = $2.4 million** (that’s federal penalties, corrective actions, legal costs and lost revenue).
- **Potential loss of Meaningful Use funds** or fines for incorrect attestation.
- **Financial and reputation “black eye”** following corrective action.
- **Loss or impairment of patient data.**
- **Patient misdiagnosis** or harm due to corrupted data or device malfunction.
- **Disruption of other devices** connected to the same network.
- **Delayed** patient testing, work backlogs, patient diversion.
- **Criminal and civil penalties.**

We know data breaches are bad news. Yet, of all the possible negative outcomes, a data breach may be the least of your worries. Worse yet, failure to secure medical devices can harm patients. “It’s one thing for a CT scanner to be down,” one CMIO told us. “It’s another thing if that CT scanner is impacted in a way that delivers an abnormally high dose of radiation,” as one hospital actually experienced.

$2.4+ million

Average cost of a breach

- Federal penalties
- Mandatory corrective action
- Legal costs
- Lost revenue
- Lost reputation
- Loss or impairment of patient data
- Patient diversion, work backlogs
- Disruption of connected devices
- Criminal and civil penalties
The Problem
Behind The Problem:

Enter the Land of Misfit Devices

Why are medical devices so vulnerable and, so often, non-compliant?

One obstacle is that the IT department in a typical hospital isn’t equipped (or even permitted, in some instances) to tinker with FDA-regulated, medical equipment. Similarly, the clinical engineers (CE) who fix the mechanics of that equipment when it breaks down aren’t equipped to discern how those devices, the IT network and patient data all impact one another.

Another challenge is the fact that about half of medical devices operate on a Windows system, which means they resemble a home computer screen. That familiarity has two unintended consequences: It makes those devices more vulnerable to viruses and malware, and invites clinicians to treat them casually, checking emails, installing their pedometer software or surfing the Internet between patient studies. (We’ve seen plenty of that.)

Ask which department owns the accountability for medical device security and compliance and you’ll find what one CIO called a “neverland” of finger-pointing over a bunch of devices that could take down several departments.

Case in Point: The Hospital Next Door

A few months ago, one healthcare facility — we’ll call them Acme Health Center — handed us a list of about 400 medical devices storing or transmitting patient data through their IT network. In conducting a risk assessment, we found nearly 1,300 devices — that’s 900 more than they knew about.

Far from an isolated example, this is typical of the more than 16,000 assessments we’ve conducted in the past four years. With clinicians or departments purchasing devices without coordination with CE or IT, switching them on and off (so they’re not always visible on the network) and moving them from room to room, it’s understandable how so many devices fall through the cracks.

Meanwhile, these devices are capturing patient data, and often communicating with the Internet and other machines in your network. Daily.

And what does HIPAA tell us about that? If there’s any ePHI in it, you’d better assess and secure it.
The Solution

1. **Complete a Thorough Risk Assessment**

   Chances are you’ve already completed some sort of risk assessment at your facility. The question is whether you’ve completed a thorough assessment of all places where ePHI resides — a requirement of both HIPAA and Meaningful Use. If you’re leaving out anything that generates, stores, maintains or transmits ePHI (say, an infusion pump or X-ray machine), you’re failing that requirement.

   Often overlooked are devices not on the facility’s network. For example, respiratory therapy devices generate patient data and reports, even though they are often not connected to the network. The same goes for portable X-ray and ultrasound machines: They’re plugged in during patient testing, and then taken to another room. Just because a device isn’t connected, it is not exempt from HIPAA privacy and security rules, or the threat of a breach.

   An often neglected or underutilized tool is the Manufacturer’s Disclosure Statement for Medical Device Security (MDS2). This form, developed by the HIMSS Medical Device Security Group, is designed to be completed by the manufacturer with device-specific information needed for that device’s risk assessment. The shortcoming of this form is that its completion by the manufacturer is voluntary, so we suggest requesting it during the device-analysis phase of your purchase decision.

2. **Collaborate with stakeholders**

   Collaboration is the single most overlooked component of effective change management, security and compliance in a healthcare facility. Earlier, we touched on the gap between IT and CE. This gap, however, extends beyond these two groups, because security and compliance don’t stop with them.

   Your risk management counterparts can provide input on security-related aspects like passwords and writing exceptions to your HIPAA policy, and help you review technology purchases from a risk management perspective. Supply chain can help evaluate purchasing decisions, operating efficiencies, and total cost of ownership. Facilities and infrastructure employees can help uncover issues related to shielding, cabling, physical security, infrastructure and more, so that those elements work together toward greater safety, security and compliance.

   Each department brings unique insight to choosing the right devices and risk level for your organization, so seek out their input and assistance.

3. **Craft policies that hold true system-wide.**

   In the spirit of collaboration, policy development must also be a joint effort. Policies impacting HIPAA compliance must be system-wide, not department-specific.

   Consider the hospital lab versus the radiology department, for example. Very few people — and virtually no patients — come in and out of the testing lab, so there’s virtually no chance of a patient seeing another patient’s private info. In the radiology department, however, there is a steady stream of patients in and out of the diagnostic area. So what might work as a privacy policy for the lab may not work for radiology.

   While this may sound like a case for department-specific policies, your organization won’t benefit from several sets of inconsistent, disjointed policies varying from one department to another. Nor would you benefit from a single policy that doesn’t take into account the differences between those departments. In collaboration with other departments, write a blanket, hospital-wide policy that meets everyone’s needs but note: You can include exceptions. For example, a policy may state “All computer screens displaying patient information will not be viewable by the general public.” In the lab, this works just fine. But what about in radiology?
Who is the general public — a patient who entered the area for a test, a janitor, a passerby? To address these concerns, you may write an exception specifying that the patient should not be brought into the room until their unique information is up on the screen, or you may add a screen block to make the screen not viewable from the patient’s vantage point.

With respect to medical devices, many hospitals write into their policy that all electronic devices must have virus protection or encryption applied to them, for instance. This works fine for traditional computers, but such actions could take a medical device out of its FDA-approved state, which is not only a punishable violation, but could also corrupt the patient data and output of that device.

So shoot for policies that hold true system-wide but apply appropriate exceptions so your policies are realistic and don’t create other problems. Worse than not having policies is having policies you don’t (or can’t) follow. If there’s a privacy breach, HIPAA officials may judge your organization based on your own policies if they’re stricter than federal regulations.

If Nothing Else, Do This.

If you act on one piece of advice from this resource, let it be this: **Ensure a thorough risk assessment of all places where ePHI resides.** Not only will that assessment fulfill federal mandates, it will give you a clear blueprint of your risk profile and the low-hanging fruit: low or no-cost steps you can take toward compliance.

It’s worth noting that if your risk assessment exposes problems, you don’t have to fix them all at once to be found compliant. If you can show a federal auditor that you’ve completed a thorough risk assessment, it’s acceptable if you haven’t yet plugged all the holes exposed by that assessment, as long as you have a plan to address them as resources become available.

As you map out your next steps, we’d urge you to consider what is at risk and not settle for band-aids and quick fixes. With multi-million-dollar fines, patient data and safety at stake, you can’t afford not to do so.

Next Steps

*If you found value in this resource, we’d love to talk to you.* Whether or not we end up working together, we’d gladly share lessons we’ve learned from more than 16,000 risk assessments.

We invite you to pick our brain and learn from our process — no commitment, no pressure. Schedule a 15-minute call and we’ll guide you toward greater security and compliance. Reach us at eProtex.com.

› **eProtex** helps healthcare providers keep medical devices safe for patients and their data, and compliant with federal mandates. The first data security company specialized in reversing the hidden risks to connected medical devices, eProtex solutions have been adopted by more than 100 healthcare providers nationwide.

eProtex.com • 855-377-6839 (Toll-free)