[H1] Connected Medical Devices: Perception vs. Reality in Shadow IT

Connected medical devices have become one of the largest, fastest-growing segments in the modern healthcare network. These devices run some form of an operating system, connect to the corporate network, and gather/store/communicate information. According to a [HIPAA Journal article, 82% of healthcare organizations](https://www.hipaajournal.com/82-of-healthcare-organizations-have-experienced-a-cyberattack-on-their-iot-devices/%22%20%5Cl%20%22%3A~%3Atext%3DThe%20biggest%20threat%20from%20these%20IoT%20cyberattacks%20is%20theft%20of%20patient%20data.%26text%3DWhen%20asked%20about%20the%20consequences%2Ccan%20also%20threaten%20patient%20safety.%22%20%5Ct%20%22_blank) have experienced a cyberattack on their IoT devices. Still, most organizations don’t view them as the endpoints they are, with the security and privacy risks they hold. In fact, the facilities department typically manages these devices, with little-to-no oversight or involvement by the information technology (IT) or security teams.

**[H2] Shadow IT Risk to Data Privacy and Security**

Healthcare has an ingrained IT problem that stems from the fact that medicine has been in practice for some [25,000 years](https://www.bartonassociates.com/history-of-physicians). Healthcare is not viewed as a modern enterprise, and the same holds true typically for its IT network. However, it is one of the most complex environments centered on its vital electronic healthcare record (EHR) systems. Considering the strict data privacy requirements with HIPAA and other compliance regulations, these hundreds of connected, and often unaccounted-for, devices suddenly become critical open doors for data leaks or additional security and privacy risks. One glaring example is the often ignored but vulnerable imaging suite.

# [H3] The Cave of Secrets

The modern hospital, and most smaller healthcare providers, have some form of an imaging suite. Regardless of size, this suite typically contains some massive and expensive imaging devices like x-rays, CT and MRI scanners, and similar devices. These devices are rarely, if ever, owned by the organization using them. More often than not, hospitals lease these machines with restrictions on what the user can change or update, such as admin passwords, default services, vulnerabilities, and a myriad of other things. These weaknesses led to the major disruptions to NHS and other healthcare systems in [2017 by the WannaCry](https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin) ransomware, which still is [affecting just under half of healthcare organizations today](https://www.fiercehealthcare.com/tech/lingering-impacts-from-wannacry-40-healthcare-organizations-suffered-from-attack-past-6-months).

To combat the lack of control over these connected medical devices in the imaging suite, many organizations use network segmentation to segregate them from the rest of the network. But, these devices produce, process, store, and transmit crucial health information. That information needs to get into a system or back into the EHR to be useful to providers. Despite the segregation that is logically in place, it is not uncommon to find numerous services freely communicating with the rest of the network and the internet. The open communication this allows is antithetical to acceptable security practices and negates the network segmentation’s effects.

# [H2] Connected Devices as Endpoints

As with most world problems, collaboration, open-mindedness, and perspective can drastically improve the position and reduce most healthcare organizations’ overall risk. First, there can be no real separation between the facilities team (or whichever team is responsible for deploying and maintaining connected medical devices) and the IT or security groups. Collaboration between these teams and a fundamental change in how these endpoints are viewed can significantly increase security and lower overall risk. The necessary sea change is to stop viewing these connected devices as anything other than an endpoint. All connected devices, be they an infusion pump or an IP connected camera, are endpoints. They are connected to the network, gathering, storing, transmitting, and processing information, meaning they are decidedly as much of an endpoint as a workstation or server.

# [H2] It’s All About Perspective on Connected Devices

The proliferation of mobile devices, cloud services, and virtualized networks exacerbate the problem. Whether staff introduces new tools or apps without IT consent or shares or stores sensitive company or patient data, connected devices can quickly get out of control. Changing the perspective about how vulnerable and risky this growing category is can tremendously improve an organization's security posture.

The Securolytics [IoT Security Appliance](https://securolytics.io/iot-security-products/) is purpose-built to protect healthcare networks and data - beginning with [continuous visibility of connected devices](https://securolytics.io/iot-security-products/%22%20%5Cl%20%22visibility) and eliminating shadow IT problems.

We make it easy to gain control over your connected devices with the Securolytics IoT Mini - starting with making it FREE of charge. We'll ship it to you for FREE. You plug it into any network port, and in no time, you'll accurately and efficiently detect, catalog, and identify vulnerabilities on all connected medical and IoT devices on your network.

Ready to get started? Let us know.

[CTA - form to request MINI]