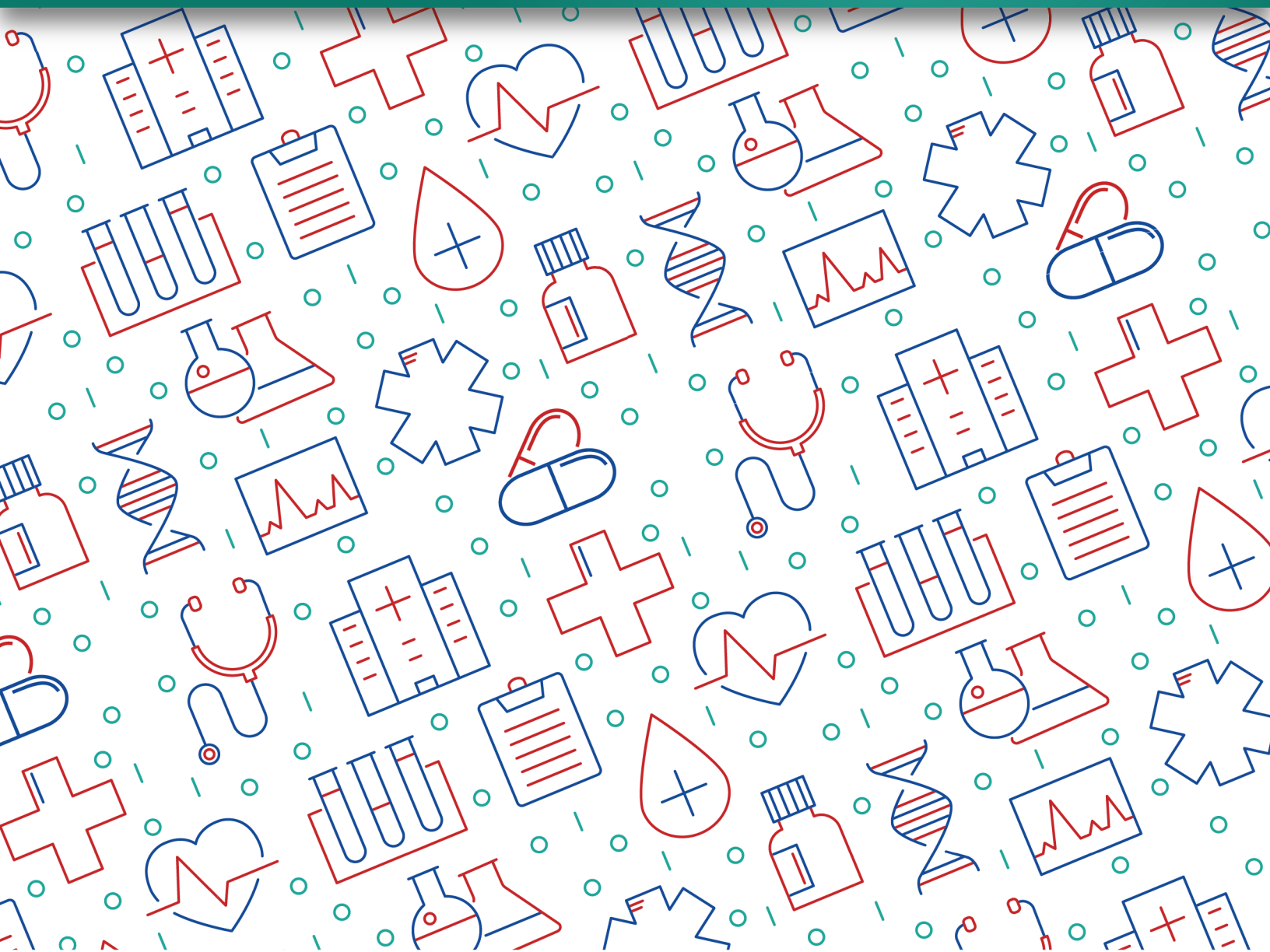


OWASP Secure Medical Device Deployment Standard

VERSION 2.0






PROJECT TEAM

PROJECT LEAD

Christopher Frenz

CONTRIBUTORS

K S Abhiraj
Hillary Baron
Christian Dameff
Aaron Guzman
Siren Hofvander
Ashish Mehta
Brian Moussalli
Michael Roza
Igor Amorim Silva
Srinivas Tatipamula



With the growth of electronic medical records systems and the increasing use of network-enabled medical devices, hospitals and other healthcare-related facilities are becoming more interconnected than ever. While this increasing level of interconnectedness often results in improvements to both the quality and efficiency of patient care, it is not without some potential security drawbacks. Many medical devices are extremely costly to upgrade or replace and such legacy systems within healthcare facilities are often commonplace. Moreover, many medical devices were engineered with patient safety and life-saving as the sole functions of the device and traditionally little attention was paid to the security of these devices. These trends are evidenced by recent FDA recommendations (mentioned below) as well as numerous security studies that find many medical devices rife with security vulnerabilities (<https://www.helpnetsecurity.com/2016/03/30/1400-flaws-automated-medical-supply-system/>). Additionally, such networked-enabled medical devices within hospitals or patients are often not deployed with security in mind, which can further add to the ease of compromise. With the explosion of botnets and other malware that now target IoT devices (of which medical devices can be considered a subtype) the need for security-minded deployments of medical devices is now more essential than ever.

This guide is intended to serve as comprehensive guide to the secure deployment of medical devices within a healthcare facility.

- FDA Premarket Cybersecurity Guidance
<https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf>
- FDA Premarket Interoperability Guidance
<https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482649.pdf>
- FDA Postmarket Cybersecurity Guidance
<https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf>
- FDA Cybersecurity Guidance
<https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm>

PURCHASING CONTROLS

One of the best ways to preserve the security of any healthcare environment is to take measures to prevent the introduction of security vulnerabilities by ensuring that only devices that provide a reasonable measure of security are acquired.

Security Audit/Evaluation

Prior to any medical device being purchased or brought onto any network, the device should be compared to the organization's internal security standards and a determination should be made as to whether or not the device is capable of meeting those standards. The device should comply with password policies, account lockout policies, and other security controls that the organization considers essential. Organizations that have not adopted internal standards with regards to what constitutes a secure medical device are encouraged to do so. Any organizations that have not evaluated their standards within the last year are encouraged to revisit them to ensure they continue to meet organizational needs and are not in need of updates. Organizations can gain ideas for the type of questions that should be asked by looking at the companion list of OWASP Medical Device Purchasing Assessment Criteria (<https://www.owasp.org/images/7/73/MedicalDevicePurchasing.pdf>) or the Mayo Clinic criteria (<https://www.mayoclinic.org/documents/medical-device-vendor.../doc-20389647>). Organizations may also want to familiarize themselves with the FDA premarket and postmarket guidance in order to determine how well the device complies with these recommendations.

Privacy Impact Assessment

In a similar manner, a Privacy Impact Assessment (PIA) should be performed prior to any system acquisition in order to validate that the device possesses the requisite security controls, ensuring that patient data is collected, stored, and transmitted in a way that is consistent with organizational policy. One set of applicable guidelines for performing a PIA is the HIMMS PIA Guide (https://www.himss.org/sites/himssorg/files/HIMSSorg/Content/files/D87_HIMSS_PIA_Guide_.pdf). Alternative guidance on conducting a PIA can be found in the European Union's Guidelines on Data Protection Impact Assessment (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=44137). Where applicable, preference should be given to solutions that were designed with Privacy by Design principles in mind (<https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf>).



Support Evaluation

Any device purchased will be considered supportable by the vendor for only a finite period of time. Given the critical role played by patching vulnerabilities in maintaining the security of any system, particular attention should be given to what kind of support the vendor will provide for the device software, how frequently they release patches, and for how many years they will continue to provide patches. Given the long active lifetime of many medical products, paying attention to the long-term commitment to patch systems is a critical security consideration that should weigh in on purchasing decisions. Related to this, consideration should be given to vendors' policies concerning security issues.

It is particularly noteworthy that organizations know that it is a myth that routine patching of medical devices causes issues requiring FDA recertification. As per official FDA statements, the FDA does not prohibit the routine patching of medical devices and any vendor using this statement as a way to avoid addressing security issues should raise a red flag (<https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM544684.pdf>). However, verification and validation that patches will not impact the functionality of the device may be required and may delay the availability of some patches. More detailed explanations of what constitutes routine patching can be found in the FDA Postmarket Guidance reference above.

PERIMETER DEFENSES

Wherever possible, medical devices should be fully denied access to anything external, though there are some cases where this might not be possible since medical devices may need to connect to update servers, transmit data to cloud-hosted medical records systems, transmit data to third-party services for assessment (e.g. remote radiology reading services), etc. These controls are designed to control the flow of information between medical devices and external resources and services.

Firewalls

Firewalls at the perimeter are an essential control to ensure that communications between medical devices and external resources are either outright denied, where feasible, or restricted to just the communications that are essential for the device to function properly. In the case where a medical device is reachable over the internet, particular attention should be taken to ensure that the device has a separate administrative interface and that external access to the administrative interface is not possible from outside the organization's internal network.



Network Intrusion Detection/Prevention System (NIDS/NIPS)

Network Intrusion Detection/Prevention Systems (NIDS/NIPS) at the perimeter can be helpful in detecting exploit attempts coming from external parties as well as traffic going to command and control sites and ransomware key generation sites. As such, NIDS/NIPS at the perimeter can be useful for their potential to provide early warning of an attack attempt or successful compromise of a network-enabled device. NIPS systems have the added capability to automatically take measures that can potentially stop an attack. If using NIPS automatic response capabilities, extensive testing should be completed before device use to ensure that potentially life-affecting communications are not interrupted or blocked as false positives.

Proxy Server/Web Filter

For devices that communicate with external resources via http and/or https, a proxy server or web filtering appliance may allow for even finer-grained control over communications than a firewall would. Moreover, many proxy servers have the ability to perform antivirus (AV) scans of web traffic. Where this is possible, it is recommended to use a different AV engine than the one used on internal endpoints, as that will help to maximize the chance of successful detection for any malware vector. Additionally, many appliances have the ability to perform SSL stripping and these appliances can often be used as a part of a data loss prevention (DLP) system as a result. DLP may be advisable for use with medical devices that may require internet access in some form, but would not normally be used to transmit Personally Identifiable Information (PII) or Personal Health Information (PHI) to an external entity.

NETWORK SECURITY CONTROLS

Network Segmentation

Network segmentation is highly useful in preventing the spread of malware and other threats through a network and is highly beneficial in containing a threat in the event an endpoint or device is successfully compromised. All medical devices should be on an isolated network segment that restricts communication of the devices to just the systems that are required for the device to function. All other communications should be restricted. Network segmentation is often achieved through the creation of VLANs and ACLs to control the flow of traffic in VLANs, but can also be achieved by using a separate physical or isolated virtual network infrastructure, which is particularly useful in areas where a concentration of the same type of medical device will be deployed in a given area. Network segmentation can also be achieved using policies enforced via Network Access Control or via Software Defined Networking (SDN)-based microsegmentation (e.g. NSX). Where feasible, medical device deployments should try to target a zero trust architecture.

Internal Firewalls

Internal firewalls can be used to improve upon network segmentation and to further restrict communications of devices to just the systems (internal and external) that they need to interact with. Firewalls, particularly next generation models, can also provide ways of monitoring and restricting traffic in ways that ACLs in switches cannot, as they typically allow for deeper levels of traffic inspection. Internal firewalls are also highly useful for protecting “one-off” devices, such as an MRI machine, where isolation is sought but the presence of only a single device does not warrant the purchase of an entirely separate physical network infrastructure. Internal firewalls help to promote a zero trust model with regards to the communication with medical devices.



Internal Network IDS/IPS

If traffic from network segments containing medical devices is routed through an internal NIDS/NIPS, signatures can be created to detect default login credentials, attempts to connect to command and control IPs, and other forms of network traffic that may indicate an attack on a medical device or a successful compromise of a medical device. While similar in function to an NIDS/NIPS at a perimeter, this helps take into account that a compromised endpoint within the organization may be used as a staging ground to launch an attack against the medical devices. If using NIPS automatic response capabilities, extensive testing should be done first to ensure that potentially life-affecting communications are not interrupted or blocked as false positives.

Syslog Server

Whenever possible, medical device logs should not be stored only on the device itself but should be exported to a distinct syslog server to allow for the collection and analysis of events that affect the device. This is critical in cases where the device itself is no longer trustable or a security issue makes the log data on the device inaccessible in some manner. It is also advisable to send log data from switches and firewalls to a syslog server to ensure that medical devices are not in communication with any malicious or unknown IP addresses.

Log Monitoring

Related to the above control, some form of Security Information and Event Management (SIEM) or log analysis should be performed on the collected log data. For example, a high occurrence of failed login attempts on a device or even a high occurrence of successful logins across a large number of devices (outside of scheduled maintenance) may be indicative of an attack from IoT malware like Mirai. Analysis such as the above is more effective if a baseline of log events associated with normal operations is established first. Log analysis can also play a role in incident investigation if an incident occurs.



Vulnerability Scanning

Medical devices should be routinely scanned to ensure that they are properly configured and that out-of-date software does not leave them susceptible to compromise. As such, medical devices should be included as part of any larger vulnerability management program that the organization has in place. Not all medical devices and features may be readily assessed by traditional vulnerability scanners and specialized scanners may have to be considered. Even with specialized scanners, there is such diversity amongst medical devices that manual compliance auditing may be needed in some cases, as indicated in the device security section below. Reporting found vulnerabilities to manufacturers is highly encouraged.

DNS Sinkholes

While some medical devices may require DNS to function properly (e.g. to transmit results by hostname, to connect to update servers, etc.), it is highly likely that these devices will only need to be able to resolve a very limited number of addresses. The security of a medical device deployment can be improved by having dedicated DNS servers for the device that can only resolve the limited number of IP addresses required for the device to function. All other DNS requests can be sinkholed. In sinkholing, a DNS server can return a false or controlled IP address. Using a controlled IP address will enable event logs to be collected and analyzed by the sinkhole server. DNS sinkholes can also be a valuable tool for detecting compromised medical devices that may not run an organization's typical set of endpoint protections.



DEVICE SECURITY CONTROLS

Some of the most critical controls to protect any network-enabled medical device will need to be implemented within the device itself. These are recommended configurations that take advantage of such controls. Not all devices will support all controls, but security audits prior to purchase should identify such deficiencies as well as the appropriate controls to compensate.

Change Default Credentials

As widely illustrated by the recent Mirai and Bashlight botnets, the use of default credentials is a highly effective means of leaving any IoT device highly vulnerable, and medical devices are no exception to such vulnerabilities. All devices should have their default credentials changed prior to deployment on the network and devices with hard-coded credentials should not be used. While it may not be feasible for organizations to conduct their own reverse engineering assessments to uncover hard-coded credentials, organizations should consider checking to see if any Common Vulnerabilities and Exposures (CVE) or other public sources exist which document the use of hard-coded credentials. Account credentials used in place of the defaults should be compliant with organizational password policies.

Account Lockout

Changing the default password does not matter if the device can easily be compromised with a dictionary attack or brute force attack. Account lockout features should be configured to block logins after three to five login attempts.

Enable Secure Transport

Devices should be configured to send data only in a secure format and secure protocols like ssh and https should be used in place of insecure protocols like telnet and http. Insecure networking protocols should be disabled wherever possible. Please note that enabling such secure protocols requires that these same features be supported on the electronic health records (EHR) interface side and/or on the side of any other systems with which the device will be communicating.



Spare Copy of Firmware/Software

In the event that a device is compromised or runs into some other software issue, having a spare copy of the device's firmware or software is critical to restoring the device to functional state in a timely manner. Further, it is advisable to have a hash of the files that comprise the latest known good version of the software or firmware to ensure that a mechanism exists for verifying the integrity of software components. Staff should be trained and competent in procedures to reload software and firmware on the various kinds of medical devices supported. For manufacturer-managed devices where organizations are not provided a spare copy of the firmware, organizations should ensure that device recovery is incorporated into the SLA of their support contract.

Backup of Device Configuration

In addition to the software or firmware used to run the device, there are most likely custom configurations required for the device to run properly on the organization's network. Backing up these custom settings after changes occur will help to ensure that devices can be restored to functional status in as timely a manner as possible. It is recommended that at least one backup copy be stored locally and that another copy be stored in a remote location to facilitate recoverability in the event of a local disaster. For manufacturer-managed devices, organizations should ensure that such backups are incorporated into the SLA of their service contract.

Baseline Configurations

Related to the controls above, baseline configurations should be established for each device to ensure the proper configuration of the device with regards to clinical functionality and security. In the event a device-specific backup is not available, this baseline configuration can be applied to ensure the quick restoration of the device in a manner that is compliant with organizational security policies. Baseline configurations should be stored in a secure location to prevent any tampering by unauthorized individuals. Organizations should ensure that their baselines are updated whenever approved changes are made to device configurations. Ideally, changes should be made as part of a formalized change management process. For manufacturer-managed devices, organizations should ensure that such baselines are incorporated into the SLA of their service contract.



Encrypt Storage

Medical devices should support encryption of any PHI and/or PII stored on the device. This feature should be turned on in case of device theft or an unauthorized user gaining physical access to the device.

Different User Accounts

Admin accounts and user-level accounts should be possible, and ideally the admin account should be bound to the management interface and unusable on any internet-facing interface. Any unnecessary accounts should be disabled.

Restrict Access to Management Interface

The management interface of the device has the potential to do the most damage to the device if compromised, as it will more easily allow access to the administrative functions of the device. Communication to this interface for making changes to the device should be locked down to only authorized terminals.

Update Mechanisms

Whether via automatic download or the manual installation of new software/firmware, all devices will require updating at some point. Mechanisms should be put in place to identify the need for updates and to ensure the routine update of all medical devices so that unpatched vulnerabilities remain minimized. The OWASP Embedded AppSec Project provides specific recommendations for mechanisms that can be used to securely update medical and other IoT devices (https://scriptingxss.gitbooks.io/embedded-appsec-best-practices//executive_summary/3_firmware_updates_and_cryptographic_signatures.html). Similar guidance is also available from NIST (<https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200-draft.pdf>) and ENISA (https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport).



Compliance Monitoring

As time passes, changes are often made to systems (either intentionally or unintentionally) and applied updates may introduce changes to devices. Compliance monitoring should be performed routinely to ensure that updates or other changes to devices are consistent with baseline configurations and organizational security policies.

Physical Security

Security controls should be put in place to ensure that physical access to medical devices is limited only to authorized individuals and that physical theft of the device is prohibited.

INTERFACE AND CENTRAL STATION SECURITY

It is not uncommon to have one or more computers attached to medical devices to be used for the collection and analysis of medical device data (a central station) or a PC/appliance attached to medical devices to be used to send data to the EHR system (an interface). While they can be distinct systems, in many cases they are hosted on the same system. These security controls pertain to the security of these devices. In particular, securing interface systems is important as these are often the points at which the isolated medical device network is bridged with the organization's main internal network.

OS Hardening

Since this guide is specific to providing guidance on medical devices it will not go into depth on OS hardening techniques, but techniques like the removal of unnecessary services, password protection, the installation of AV, and other common OS hardening techniques should all be employed. Please consult guidance specific to the operating system for further details.



Encrypted Transport

As with the medical devices themselves, these systems will be used to send and receive data and as such should make use of the same secure protocols discussed in the device configuration section.

Message Security – HL7 v3 Security Standards

Interface systems will often be used to transmit data to an organization's EHR, picture archiving and communication system (PACS), or other clinical system and HL7 messages are the standard format for accomplishing this. The exchange of HL7 messages should be done using the HL7 v3 standard, as this provides for security provisions not present in earlier versions of the HL7 standard. Please note that the use of HL7 v3 requires not just that the medical device support the messaging format, but that the EHR or other systems the device will be communicating with also support it.

SECURITY TESTING

All the controls in the world are useless if misconfigurations and vulnerabilities are rampant. Security testing will help uncover shortcomings in devices or within the setup that surrounds them. It is better to discover such issues via testing so they can be addressed via fixes or via the addition of compensating controls, than to later discover the weakness exists during the forensic phase of an incident response.

Penetration Testing

A penetration test can be an effective means of assessing how effective device and network configurations are at turning back an attack on medical devices installed on the organization's network. The results can be used to help further improve defenses and may reveal flaws in the device that can be presented to the manufacturer for patching in an upcoming update release. For organizations that do not have the resources to conduct their own pen tests, they may want to consider reaching out to organizations that conduct independent security assessments of medical devices to see what kinds of vulnerabilities may have been revealed in the course of their own testing.



INCIDENT RESPONSE

Eventually all organizations will face the compromise of one or more devices. One of the things that differentiates an organization that has a mature security program from ones that does not is how effective they are at detecting, containing, and eradicating such threats.

Incident Response Plan

Organizations should have detailed plans in place to deal with the compromise of medical devices before such an incident becomes a reality for the organization. Organizations should have a clear-cut plan in place that defines how they will react to an incident and who will be responsible for what actions during the detection, containment, eradication, and recovery phases. It is also important that all staff are made aware of the plan and are trained to respond appropriately and effectively. For organizations without any sort of incident response plan in place, a good starting resource is the SANS Institute InfoSec Reading Room (<https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>).

Mock Incidents

It would be highly beneficial for any organization to conduct a mock incident regarding the compromise of medical devices to ensure that they have an effective incident response plan in place and that employees are adept at carrying out that incident response plan. Mock incidents provide a great way to identify security deficiencies as well as effective practices and to use the lessons learned to further improve the organization's security posture. Tabletop exercises can be useful here, but clinical simulations like those done at the CyberMed Summit (<https://www.youtube.com/watch?v=JUNqo5erVI0>) are also highly useful in preparing clinicians for dealing with the potential for a compromised medical device.
