The Case for Medical Device Cybersecurity Hygiene Practices for Frontline Personnel

Stephen L. Grimes and Axel Wirth

Role of and Need for Medical Device Cyber Hygiene

As medical devices and systems became more sophisticated over the past two decades, they began incorporating microprocessors, software, sensitive data, and connections to networks (including some to the Internet). These changes provided more features and greater versatility, collectively improving patient care, but they also resulted in a growing number of devices and systems with security vulnerabilities. Cyber adversaries simultaneously have become more sophisticated and more effective at taking advantage of these vulnerabilities with their attacks.

Regulators, standards organizations, and industry expert groups all have been focused on developing the regulations, standards, guidelines, and tools necessary to identify and manage these new security risks. Examples of the aforementioned organizations and groups include the Food and Drug Administration (FDA), National Institute of Standards and Technology (NIST), MITRE, Healthcare Sector Coordinating Council (HSCC), Center for Internet Security (CIS), Health Information Sharing and Analysis Center (H-ISAC), Association for the Advancement of Medical Instrumentation (AAMI), International Organization for Standardization (ISO), American National Standards Institute (ANSI), International Electrotechnical Commission (IEC), and National Electrical Manufacturers Association (NEMA). Consequently, a wealth of resources are available on how medical device manufacturers and healthcare delivery organizations can adopt one or more frameworks to drive various aspects of their medical device/system security risk management programs.[1]

However, one area that still gets little attention is the need for frontline staff (i.e., those who operate and those who provide technical support to medical devices/systems) to know and exercise safe security practices. In fact, the greatest security exposure for the installed base of medical devices and systems is in how the medical device owners, operators, and technical support staff acquire, care for, operate, maintain, support, and eventually dispose of those devices/systems.

Therefore, a critical element in any effective medical device security management program is the engagement of appropriate stakeholders in cybersecurity practices, education, and training.[2]

Collectively, the cybersecurity practices followed by device owners, operators, and technical support staff are commonly referred to as cybersecurity hygiene (or cyber hygiene). Medical device/system cyber hygiene is defined as those practices that maintain security and reduce the device's/system's and the organization's security risk and exposure. Cyber-hygiene practices are integrated into the organization's security management program through the establishment of policies, procedures, education programs, and compliance audits that are targeted at the organization's frontline staff.

Specific Cyber-Hygiene Practices for Frontline Staff

The following is a fairly comprehensive list of 20 interdependent practices that should be understood and followed by most frontline personnel involved in either the operation or support of medical devices and systems. If adhered to, these cyber-hygiene practices can go a long way toward preventing security-related compromises. Of note, although this list represents what are considered "leading practices," any first-time implementation of a new process, practice, or tool should always be preceded with an assessment to verify

***Stephen L. Grimes**, FACCE, FHIMSS, FAIMBE, AAMIF, is the principal consultant at Strategic Healthcare Technology Associates in Swampscott, MA. Email: stephen.grimes@shcta.com*

Corresponding author

***Axel Wirth**, CPHIMS, CISSP, HCISPP, AAMIF, FHIMSS, is the chief security strategist at MedCrypt in San Diego, CA. Email: axel@medcrypt.co*

whether the security benefit gained by the implementation is not offset by the introduction of significant care delivery, workflow, or safety risks.

These cyber-hygiene leading practices (*followed by the rationale supporting them*) include:

1. Keep any device operating system (OS), application software, third-party software, firmware, and security related configuration (e.g., antimalware software) up-to-date (i.e., use the latest version and vendor-recommended configuration).
   Outdated software with unpatched vulnerabilities represents one of the most commonly exploited vulnerabilities. Work with manufacturers to ensure available patches and updates are vetted by the manufacturer and that the patches/updates are overseen by healthcare technology management (HTM)/information technology (IT) security.
2. Do not connect new memory devices (e.g., USB, SD cards, CDs, removable drives) to a device without first scanning them for potential security compromise.
   Malware inadvertently has been installed in medical devices because the media with the update also contained malicious code. Media should not be attached to or installed on a device without first scanning with a security application with up-to-date malware definitions to ensure the media is free from malicious code. Some organizations may choose to limit the use of external storage to sanctioned devices.
3. Do not attach peripherals (e.g., storage devices, displays, chargers, printers, mobile phones) unless approved by the manufacturer and/or HTM/IT security.
   Peripherals can contain application code (including malicious code) that could install itself on a device. Installation of a peripheral or any code (particularly malicious code) from a peripheral can affect a medical device's performance adversely unless the device was specifically designed to attach to that peripheral.
4. Do not install applications (e.g., music, games, utilities) on device unless approved by the manufacturer and/or HTM/IT security. This also includes applications and agents that are commonly used for IT endpoint management purposes but may not be approved/appropriate for use on the medical device.
   Medical devices often use modified versions of OSs and software. Installation of applications not designed for a medical device can add vulnerabilities and cause unintended and unexpected results when installed on a medical device running a modified OS or software. Installation of applications not designed for a medical device also can significantly increase exposure to security risks, as well as compromise the device's performance.
5. Do not use email applications (including web-based email) or other communication applications on devices unless the manufacturer intended the device for email or communications use. If the manufacturer intends the device for email use, do not open mail, mail attachments, or URLs from unknown sources.
   Opening mail from unknown sources, opening unknown attachments, or clicking on URLs to unknown locations can result in the download of malware that exfiltrates sensitive data, destroys data, or encrypts data for ransom on the device and potentially on its connected network or that hijacks the device's operation.
6. Do not use browsing applications on a device unless the manufacturer intends the device for browsing or the browser is required for operation of the device (e.g., accessing operating instructions). In addition, when the manufacturer intended the device for browsing, do not visit websites (URLs) unless approved by the manufacturer and/or HTM/IT security.
   Surfing the web and visiting unapproved websites can result in the download of malware that can exfiltrate sensitive data, destroy data, or encrypt data for ransom on the device and potentially on its connected network or that can hijack the device's operation.
7. Do not connect to unknown or unsecured networks (wired or wireless) without using a VPN (virtual private network) application

(or other secure connection technology) or obtaining approval from HTM/IT security.
Connecting to an unapproved or unknown network can expose the medical device to device hijacking or introduction of malicious code.

8. Use unique and strong passwords (never default or common passwords) for each individual user and use multifactor authentication when possible or when required (e.g., for remote access or high-privilege access). Coordinate password change processes with HTM/IT security and relevant stakeholders.
Continued use of default passwords after initial installation and configuration can lead to use by unauthorized individuals who have looked up the manufacturer default. The use of shared or common passwords contributes weak security—where someone who is no longer authorized can still use the common password. Strong, unique passwords with multifactor authentication (e.g., use of a token or texted "security code") are ideal.
9. Limit device access to only authorized personnel and use role-based access to limit authorization to personnel based on the level of their need to access device functions.
Use- or role-based access ensures that clinicians can only access "clinical" functions, technical support can only access "diagnostic/troubleshooting" functions, and administrators can access the master controls for security (e.g., creating roles, assigning users).
10. Backup data, applications, and configurations regularly and verify the integrity of those backups.
Data and applications can be lost due to device failure, corruption, erasure, malicious encryption (e.g., ransomware). Backing up frequently and staggering backups can protect data from catastrophic loss and can speed up recovery. Verifying the integrity of backups ensures data are, in fact, backed up properly and suitable for restoration. Backup processes should be compliant with all relevant recovery, privacy, and data retention requirements.
11. Use a strong encryption protocol for data "in transit" (e.g., WPA3) and data "at rest" (e.g., on storage media) whenever possible. Prior to the initial implementation of any encryption protocol, confirm that it does not affect workflows or system performance unacceptably.
Use of "strong" encryption can prevent compromise of sensitive data.
12. Segregate vulnerable systems on to separate (isolated) networks and use firewalls (for network segments and/or individual devices as appropriate).
Segregating medical devices (particularly those with significant vulnerabilities) on networks that have firewalls and fewer vulnerability exposures (based on the nature of other devices on the network and other network elements).
13. Lock down, disable, or physically block hardware ports (e.g., USB, SD, HDMI, ethernet, proprietary test ports) and network ports (e.g., TCP/UDP ports) not needed for intended use on the device or system.
Unused ports can be exploited by an attacker or by malicious code. Unused ports should be physically locked or configured as unavailable.
14. Physically secure devices by locking away or "permanently" mounting to prevent theft of a device or the sensitive information (e.g., protected health information [PHI], individually identifiable health information [IIHI]) it may contain.
When possible, medical devices accessible to unauthorized personnel should be physically locked away to prevent unauthorized use or, where appropriate, physically mounted to prevent theft.
15. Use a real-time location system (RTLS) to track and locate devices containing sensitive information (e.g., PHI, IIHI) where appropriate.
RTLSs can track and locate medical devices within and potentially outside a facility. For particularly sensitive and "portable" devices, a tracking/locating system can help in quick retrieval.
16. Consult with HTM/IT security before selecting and acquiring a new medical device that utilizes microprocessor(s) or runs software.

Security issues should be considered prior to acquiring new microprocessor-based medical devices. HTM/IT security should be given the opportunity to obtain an MDS² (Manufacturers Disclosure Statement for Medical Device Security) form and ensure the new device can securely operate in the planned environment.

17. Do not connect a new device (e.g., purchased, leased, loaned) or a device returning from a repair provider to the network until that device has been configured for secure operation and scanned for malware.
Devices that have not been in continuous possession of the organization may not have an optimum security configuration and therefore may be more vulnerable to compromise. Those devices may also have acquired malware and should be scanned by HTM/IT security before connecting to the network.
18. Discontinue use, discard, or replace (with HTM/IT security's support) any devices/systems with known vulnerabilities when they can no longer be updated or patched in a manner that eliminates or sufficiently reduces those vulnerabilities (or if external protective measures, such as network segmentation or firewalls, are not practical or sufficient).
Some devices may have significant vulnerabilities that cannot be easily or effectively mitigated. Eventually, these devices will likely have to be removed from service, discarded, and potentially replaced.
19. Remove sensitive data (e.g., PHI, IIHI, personally identifiable information, user and network credentials, research data) from any devices before discarding or transferring to new owners and document any data removal.
Prior to disposal or transfer of devices, any sensitive data must be permanently removed by a process approved and overseen by HTM/IT security.
20. Report unusual or unexpected device operation to HTM support services.
Any unusual or unexpected device operation should be reported immediately to HTM services to determine whether there is a technical problem with the device—or whether there may be a cyber compromise.

The security of medical devices will remain a major focus of healthcare providers for the foreseeable future. To remain relevant, all medical device owners, operators, and technical support staff must stay up to speed on the concept of medical device cybersecurity and associated cyber-hygiene practices.

Conclusion

Although the importance of these medical device/system cyber-hygiene practices cannot be understated, their existence will have little effect unless all appropriate stakeholders (e.g., device owners, operators, tech support) are educated on and adopt them. The security chain is only as strong as its weakest link, and it only takes one stakeholder's one-time failure to learn and practice appropriate cybersecurity to result in a major cyber compromise.

Cyber vulnerabilities and threats continually evolve, which means cyber-hygiene practices must also evolve to address those vulnerabilities and threats. Any new cyber-hygiene practices must also be passed on to and practiced by relevant stakeholders. Therefore, the process of updating cyber-hygiene practices, educating stakeholders, and auditing their compliance must remain ongoing.

If you haven't already realized it, the security of medical devices will continue to be a major focus of healthcare providers for the foreseeable future. For any device owner, operator, or technical support professional hoping to remain relevant, this is the time to ensure you are up to speed on the concept of medical device cybersecurity and associated cyber-hygiene practices.

References

1. Grimes SL, Wirth A. *Medical Device Cybersecurity: A Guide for HTM Professionals*. Arlington, VA: Association for the Advancement of Medical Instrumentation; 2018.

2. Schneider J, Wirth A. Balancing patient safety, clinical efficacy, and cybersecurity with clinician partners. *Biomed Instrum Technol*. 2021;55(1):21–8.