CYBER SECURITY FOR CONNECTED MEDICAL DEVICES

CANADIAN CENTRE FOR CYBER SECURITY

NOVEMBER 2021 | ITSAP.00.132

Internet-connected medical devices can provide life-saving treatments, such as administering medication, regulating heartbeats and monitoring blood pressure. Despite these positive outcomes, being connected to the Internet can expose the devices to cyber threats and increase the risk of harm to patients by disrupting or degrading the devices' performance.

WHY ARE MEDICAL DEVICES TARGETED?

Threat actors target medical devices for many reasons, including using them as a vector to access health care systems, collect the data stored on the devices, or gain insight into patented technology. The devices contain sensitive personal health information (PHI) and often connect with health care organization systems and networks which contain financial and research data. This information is of value to cyber threat actors and can be used to commit cybercrimes or sold for inappropriate use.

HOW DO THREAT ACTORS TARGET MEDICAL DEVICES?

Threat actors can compromise connected medical devices, including wearable devices and those that perform health monitoring. Some examples of how medical devices can be targeted include the following:

- Remote control capabilities, such as the ones found in insulin pumps, can be compromised by a threat actor to gain control of devices.
- Wireless communication features used to transmit data to health care providers, such as those found in pacemakers and implantable cardiac defibrillators (ICD), can be used by threat actors to gain access to devices and any stored data.
- Devices with outdated software or firmware, such as CT scan and MRI machines, can also be manipulated by threat actors and compromised for malicious purposes.
- Health care organizations' networks can also be compromised through connected medical devices or through more traditional cyber attack mechanisms.
- Medical devices with weak access controls, hard-coded credentials, or no authentication factors can be compromised through connected devices.

WHAT ARE THE IMPACTS?

Cyber attacks on medical devices can have devastating consequences, including risks to patient life. Manufacturers, health care organizations, cloud service providers (CSPs) and patients should understand the risks associated with these devices and the measures required to keep them safe and secure.

DEVICE MANUFACTURERS

Manufacturers should conduct pre-market risk assessments to address cyber security risks. Failure to perform these assessments could prevent you from obtaining a licence to market the device. Once on the market, manufacturers are responsible for monitoring and mitigating potential security risks and providing regular maintenance and updates to patch vulnerabilities throughout the lifecycle of the devices. Failure to mitigate these risks could result in legal issues and financial loss.

CLOUD SERVICE PROVIDERS (CSPs)

CSPs are responsible for the accessibility, integrity and safety of data stored on their platforms. Data transmission from devices to the cloud platforms or software should be secure and remain compliant with privacy legislation. Failure to do so could result in data loss or breaches and legal action.

HEALTH CARE ORGANIZATIONS

Health care organizations must exercise due diligence when purchasing medical devices. Cyber attacks and viruses could target an entire health care network, potentially compromising clinical data, PHI, and proprietary research initiatives. Also ensure the devices you procure will have long-term support, including software patches and vulnerability remediations.

PATIENTS

Patient health can be directly impacted by cyber attacks on medical devices, such as wearable devices and home health monitoring devices. Compromised patient devices can impact device functionality, data reported to health care providers, and urgent or emergency notifications.

CASE STUDIES

- **2017 NOTPETYA:** A ransomware attack that locked the drives of machines running on a certain operating system. Although medical equipment remained uninfected, the computers needed to view the data and images from these machines were inaccessible. NOTPETYA resulted in damages of $10 billion worldwide and delayed the ability to provide patients with medical services for weeks.
- **2017 WANNACRY:** A ransomware attack that crippled the United Kingdom's National Health Services. It hindered their ability to see patients and conduct medical procedures. In the United States, radiology equipment was impacted hindering the ability of some hospitals to provide patient care.
- **2020 UNIVERSAL HEALTH SERVICES(UHS)**: A ransomware attack that shut down the entire U.S. UHS network, rendering all data and systems unavailable. Over 400 health care organizations were impacted by the ransomware, resulting in approximately $67 million in lost revenue. UHS took 3 weeks to recover from the attack.
- **2020 BLUETOOTH LOW ENERGY (BLE):** Health Canada issued an alert that medical devices, such as pacemakers, blood glucose monitors, and insulin pumps with a BLE chip were vulnerable to cyber attacks. If successful, these cyber attacks could crash the devices, unlock them, or bypass security to access functions that should only be available to an authorized individual.

Communications Security Establishment
Centre de la sécurité des télécommunications

Canada

HOW CAN I PROTECT MY ORGANIZATION?

Securing connected medical devices is a shared responsibility between the manufacturer, the health care organization and the patient. Since many devices are now cloud-based, and there are security interdependencies between medical devices and the networks they connect to, cloud service providers (CSPs) are also responsible for the security of these devices. The table below provides device manufacturers, CSPs and health care organizations with measures they can implement to better protect medical devices from cyber attacks. These measures are based on Health Canada requirements, regulations and recommendations. For more information see Health Canada's medical device page.

Recommendations for Manufacturers and CSPs	Recommendations for Health Care Organizations
● **Manage Your Risks:** Develop a cyber security risk management process in parallel with your traditional device risk management processes. As a risk is mitigated in one process, the effect of the mitigation on the other process must also be considered. For example, adding a network connection to a device without security controls may not impact physical safety, but may act as a vector for cyber threat actors.	● **Protect Your Perimeter:** Take security measures, like installing firewalls, anti-virus and anti-malware software on all your networks. Segment your network, consider guest and operational networks.
● **Secure Your Designs:** Build cyber security controls into the design stage of your development process. Consider a manual override option for devices in the event of threats to patient safety. Design choices should maximize cyber security without hindering the safety aspects of the device. Develop a lifecycle plan for your devices to ensure you can support organizations, update and patch vulnerabilities, and decommission outdated or obsolete devices.	● **Secure Your Devices:** Protect your systems and devices with passphrases or strong passwords. Use a different passphrase or password for each device and account. Secure your accounts and devices with multi-factor authentication (MFA). With MFA enabled, two or more different authentication factors are needed to unlock a device or sign in to an account. Also consider encrypting your devices, especially those containing or accessing sensitive information Lastly, apply patches and updates as they become available to ensure your operating systems are updated.
● **Verify and Validate Your Devices:** Test your devices to ensure the behaviour and performance meets the design requirements. Conduct cyber security tests, such as penetration testing and vulnerability scans, that accurately demonstrate the device meets cyber security requirements.	● **Develop Your Framework:** Establish security policies and procedures to protect your data and govern the use of PHI. Consider the principle of least privilege: provide individuals only the set of access privileges that are essential to performing authorized tasks.
● **Monitor Your Deployed Devices:** Track and report any vulnerability that could impact the medical device. Provide patches and updates regularly to ensure your devices are secure and free of exploitable vulnerabilities. Consider implementing a software update mechanism into the device during the design phase.	● **Establish a Security Culture** Provide cyber security and privacy training to your staff and educate users about cyber threats that can impact medical devices and the PHI they contain. Emphasize the fact that every member of your organization is responsible for protecting sensitive information. For helpful information see the Get Cyber Safe website.
● **Secure Your Platforms:** Implement the necessary security and privacy controls on your cloud platforms to ensure clients' data and devices are protected. For example, ensure you have a robust backup process in place and apply MFA to all systems and applications to ensure data integrity and safety. A compromise in cloud infrastructure could result in devices or their networks being infected.	● **Manage Your Assets:** Backup your information to a secure storage site (e.g. external hard drive or a cloud-based backup site) that is not connected to your network. Retire any unsupported devices if possible. Unsupported devices no longer receive patches and updates from their vendors and are vulnerable to cyber threats.

Canadian Oversight for Medical Devices

- Health Canada reviews medical devices to assess their safety, effectiveness and quality before being authorized for sale in Canada.
- The Medical Devices Bureau of the Therapeutic Products Directorate (TPD) is the national authority that monitors and evaluates the safety, effectiveness and quality of diagnostic and therapeutic medical devices in Canada. For more information on their role, see the *Safe Medical Devices in Canada* fact sheet.
- The Food and Drugs Act (F&DA) provides Canadian device manufacturers with the *Medical Device Regulations*.
- Health Canada provides guidance on *Pre-market Requirements for Medical Device Cyber Security*.

LEARN MORE

Visit the Cyber Centre website (**cyber.gc.ca**) to learn more about cyber security topics and find our entire collection of publications, including:

- Cyber Security for Healthcare Organizations: Protecting Yourself Against Common Cyber Attacks (ITSAP.00.131)
- Internet of Things Security for Small and Medium Organizations (ITSAP.00.012)
- Artificial Intelligence (ITSAP.00.040)
- Supply Chain Security for Small and Medium-Sized Organizations (ITSAP.00.070)
- How Updates Secure Your Devices(ITSAP.10.096)
- Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threats to the Health Sector