Security Recommendations on Smart Insulin Injector

Overview of Portable Medical Device Cybersecurity Guidelines for Pocket Clinic Corp. ©

By: Abdon Katter, Daniel Morales, Emmanuel Ebedi, Gabriel Ade-Okpaise, James Kuzhilaparambil, and Md Faisal

pocket clinic

Last Updated: 2024/12/04

Table of Contents

Executive Summary

This report outlines cyber security recommendations for the insulin injection device developed by Pocket Clinic.The device uses a microcontroller that communicates using bluetooth to a mobile application, and that mobile application would be sending information to a cloud database. To correctly inform the security recommendations, it is also important to recognize the potential users that could access the information, including the user, their doctor or other medical professional who prescribed the use of the device, and the potential of other trusted users who may need access in the event of a lost or disconnected device/mobile phone.

As a medical device that will also handle personal identifiable information (PII), many regulations and guidelines have informed and supplemented the recommendations. This includes Canadian regulations and guidelines including Health Canada guidances, laws such as the Personal Information Protection and Electronic Documents Act (PIPEDA) and the Ontario Personal Health Information Protection Act (PHIPA); but American guidelines are also referenced to establish a stronger, adaptable baseline, such as the U.S. Food and Drug Administration (FDA) guidelines and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The report focuses on five key areas of recommendation for security - Secure Communications, User Access & Validation, Software Maintenance, Data Integrity & Confidentiality, and establishing baseline cybersecurity practices.

The Secure Communications section is focused on how to secure communication between the device and mobile app over bluetooth, referencing specific threats and mitigation methods.

The User Access and Validation section proposes features to restrict access to certain users, increasing device security.

The Software Maintenance section outlines the requirements for updating the device for cyber security and how it may differ from traditional firmware updates for approvals. The

The Data Integrity and Confidentiality Section focuses on best practices to ensure data validation and verification.

Finally, the Baseline Cybersecurity Practices section outlines practices and guidelines to ensure not only the device, but the company itself is secure to ensure the safety of the data, outlining information about device security in multiple factors, incident response and risk management, and available and cost effective cyber security solutions that can be investigated further or used to address and mitigate cyber security risks.

Secure Communications

In this section, the current threat landscape related to Bluetooth communication between Pocket Clinic's Insulin Injection Device and its associated app was reviewed after which mitigating strategies were recommended to keep patients' data safe in compliance with industry standards and guidelines from both Health Canada and the Food and Drug Administration (FDA).

This section of the report has the following objectives:

- Establishment of a secure communication channel via Bluetooth Low Energy (BLE) between the Client's Insulin injection device and its associated mobile application to ensure patients' information remains confidential, unaltered and available when needed; in other words, the confidentiality, integrity and availability of patients' information are not compromised when the device communicates with the app.
- Ensuring compliance with pre-market requirements for medical devices as mandated by Health Canada in addition to the guidance on cybersecurity for medical devices from the Food and Drug Administration.

Current Threat Landscape

  - Interception of Bluetooth communication.
  - Man-in-the-middle (MITM) attacks during pairing or transmission.
  - Replay attacks exploiting static encryption keys.
  - Sending oversized data packets over the Bluetooth's L2CAP layer to trigger a DoS - Denial of Service attack (also known as Bluesmacking).
  - Hijacking the advertising signal of a Bluetooth enabled device with the intention of sending spam and other junk data possibly masking a more dangerous attack (also known as Bluejacking).
  - Exploiting the Bluetooth connection to gain access and exfiltrate data (also known as Bluesnarfing).
  - Using Bluetooth to create a backdoor into the victim's device to eavesdrop on the victim's calls and conversations (also known as Bluebugging).

The following table outlines the potential threats and mitigation strategies for secure communication, referencing specific Common Vulnerabilities and Exposures (CVE) codes. Table 2 outlines recommended industry standards that relate to communication methods.

Table 1: Threat Description, Associated CVE and Mitigation Strategies

Threats	Description	CVE ID	Mitigation Strategies	Categories
Interception of Bluetooth Communication	Interception of poorly encrypted (or unencrypted) communication between device and app thus gaining access to patient's medical information in violation of PIPEDA and HIPAA regulations.	CVE-2023-46447	Use AES-256 for all transmitted data to prevent packet sniffing. *NIST SP 800-175B.* Key exchanges should be via Elliptic Curve Diffie-Hellman (ECDH) to prevent encryption keys from being compromised. *Bluetooth Core Specification (Amended) 5.4.* Disable discoverability of the device by default and only enable pairing when required. *ISO/IEC 27002:2022.* Implement frequency hopping i.e. switching frequencies during communication to reduce possibility of eavesdropping. *Bluetooth Core Specification (Amended) 5.4.*	Preventive Controls

Threats	Description	CVE ID	Mitigation Strategies	Categories
Man-in-the-Middle Attack (MITM)	Attackers position themselves between the app and device during pairing or communication, intercepting and potentially altering data.	CVE-2020-10135	Validate identities using signed certificates or cryptographic keys. *NIST SP 800-63B.* Use secure pairing methods QR codes, or NFC for secure key exchange. *Bluetooth Core Specification (Amended) 5.4.* Utilize unique session-specific keys for encryption during each pairing session. *NIST SP 800-56A Rev. 3.*	Preventive Controls
Replay Attack	Attackers capture and replay previously transmitted data packets to replicate commands that could increase the dosing interval and compromise patient safety.	Not Applicable	Regular rotation of encryption keys to render intercepted packets invalid. *ISO/IEC 11770-1:2010.* Include timestamps to packets to ensure uniqueness. *NIST SP 800-38D.* Use Hash-based Message Authentication Code (HMAC) to verify data integrity. *NIST FIPS 198-1.*	Preventive Controls

Threats	Description	CVE ID	Mitigation Strategies	Categories
Bluesmacking	Sending oversized data packets over the Bluetooth's L2CAP layer to trigger a DoS - Denial of Service attack.	Not Applicable	Monitor communication channels for signs of unusual traffic. *Bluetooth Core Specification (Amended) 5.4.*	Detective Control
Bluejacking	Hijacking the advertising signal of a Bluetooth enabled device with the intention of sending spam and other junk data possibly masking a more dangerous attack.	Not Applicable	Ensure devices are not discoverable by default. *ISO/IEC 27033.*	Deterrent Control
Bluesnarfing	Exploiting the Bluetooth connection to gain access and exfiltrate data.	CVE-2017-0785 (Android devices only)	Encrypt patient's data with AES standard and devices should be non-discoverable by default. *ISO/IEC 29192-2.*	Preventive Control
Bluebugging	Using Bluetooth to create a backdoor into the victim's device to eavesdrop on the victim's calls and conversations.	CVE-2020-10135	Ensure each device has a unique key and Monitor for unauthorized connections. *NIST SP 800-177 Rev. 1.*	Corrective Control

Table 2: Recommended Industry Practices

Category	Type	Description	References/Standards
Encryption Standards	End-to-End Encryption (E2EE)	Protect all transmitted data using AES-128 or AES-256.	*NIST SP 800-175B*
	Transport Layer Security (TLS 1.3)	Cryptographic protocol for securing communication channels preventing interception and alteration of patients' data.	*NIST SP 800-52R2*
	Elliptic Curve Diffie-Hellman (ECDH)	Used for secure key exchanges, reducing the risk of MITM attacks.	*NIST SP 800-56A Rev. 3, Bluetooth Core Specification (Amended) 5.4.*
Authentication and Access Control	Mutual Authentication	Require both app and device to validate their respective identities using certificates or unique keys.	*NIST SP 800-63B*
	Role-Based Access Control (RBAC)	Device features and app controls to be determined based on user roles (e.g. patient, healthcare professional or other caregivers).	*ISO/IEC 27002:2022*
	Multi-Factor Authentication (MFA)	Implement MFA for logins using any of the following techniques: something-you-are (biometrics) or something-you-know (one-time passcodes).	*ISO/IEC 29115*

Category	Type	Description	References/Standards
Bluetooth Security	LE Secure Connections	Use Bluetooth 4.2+ with ECDH for secure pairing and AES CCM for encryption.	*Bluetooth Core Specification (Amended) 5.4.*
	Out-of-Band Pairing	Establish secure initial connections using QR codes or near field communication (NFC) to prevent MITM.	*Bluetooth Core Specification (Amended) 5.4.*
Risk Management and Testing	Threat Modelling	Identify and address risks like interception of communication, and data tampering.	*NIST SP 800-30 Rev. 1*
	Testing and Validation	Simulate MITM attacks and validate data integrity using Hash-based Message Authentication Code – HMAC.	*NIST FIPS 198-1*
	Regulatory Alignment	Document testing procedures to meet Health Canada and FDA requirements.	*Health Canada Guidance Document and FDA Cybersecurity Guidance.*
Regulatory Requirements	Lifecycle Management	Integrate security measures from design to post-market monitoring.	*FDA Cybersecurity Guidance*
	Secure Firmware and OTA updates	Require signed firmware updates and secure over-the-air (OTA) deployment.	*FDA Cybersecurity Guidance*
	Post-Market Vulnerability Management	Continuous monitoring of the threat landscape for relevant vulnerabilities and deploying patches promptly.	*FDA Cybersecurity Guidance*

Category	Type	Description	References/Standards
Post-Market Cybersecurity	Incident Response	Develop a robust incident response plan to address breaches thereby minimizing patient data exposure.	*FDA Cybersecurity Guidance*
	Continuous Monitoring	Monitor for anomalies in communication patterns using automated tools.	*Health Canada Guidance Document, FDA Cybersecurity Guidance*
	Lifecycle Updates	Implement a secure process for timely software patches and updates.	*FDA Cybersecurity Guidance*

Steps to Securing Communication Between the Microcontroller and App

i. **Assigning Unique Certificates**:
Each sensor device will be assigned a unique digital certificate during manufacturing. These certificates will be signed by a trusted Certificate Authority (CA) to ensure device authenticity and facilitate secure communication (Kanneganti & Chellappan, 2023).

ii. **Establishing Secure Communication**:
All communication between the app and the sensor will utilize **TLS 1.3**, which provides robust encryption and ensures mutual authentication of the app and the sensor (Rescorla, 2018).

iii. **User Confirmation During Pairing**:
The app will display a pairing code during setup, and the user must confirm that the displayed code matches the one shown on the sensor. This step ensures that pairing is verified manually, preventing unauthorized connections (Dong & Kang, 2020).

iv. **Pairing via NFC or QR Code**:
Pairing will primarily be conducted through NFC or QR code scanning. This approach reduces reliance on Bluetooth signals alone, which can be intercepted more easily (Wang et al., 2022).

v. **Access Control and Least Privilege**:
Implement **least privilege access control** within the app to define which users have permissions to initiate pairing. This mechanism prevents unauthorized users from accessing or pairing with the device (Ferraiolo et al., 2016).

vi. **Logging Pairing Attempts**:
The app will log when and where pairing attempts occur. Users will receive in-app notifications or emails to alert them of unusual pairing activity.

vii. **Failed Pairing Alerts**:
If there are more than three failed pairing attempts within five minutes, the system will trigger an alert. Notifications can be sent via push notifications, email, or SMS (NIST SP 800-63B, Section 5.2.2; NIST SP 800-53 Rev. 5, AC-7)."

viii. **Session Termination for Anomalies**:
Implement a mechanism to terminate sessions if anomalies, such as unexpected

data transfers, are detected. This helps mitigate potential breaches (ISO/IEC 27001, 2013).

ix. **Key Revocation for Compromised Devices**:
If a device is compromised, its cryptographic key can be revoked remotely to prevent further unauthorized access (IEEE, 2021).

x. **User Education**: Provide an in-app tutorial to educate users on recognizing security alerts,following pairing best practices, and creating strong passwords. This training reduces the likelihood of user-induced vulnerabilities (AlFuqaha et al., 2015).

Connection Process during Internet Downtime

i. The user logs into the app using credentials (e.g., username/password, biometrics, or a multi-factor authentication system like OTP or TOTP).

ii. The app validates the user via a local database or a previously stored secure token (if offline).

iii. After successful login, the app ensures the authenticated user has the necessary permissions to connect to the sensor (e.g., based on user roles or access levels).

Section Conclusion

The secure communication measures proposed in this report align with current industry standards, Health Canada and FDA Guidelines. These measures protect patient data, protect patient safety, enhance consumer trust and increase the chances of regulatory approval for the Canadian and US markets.

User Access/Validation

The integration of continuous glucose monitoring (CGM) systems with insulin pumps are known as integrated continuous glucose monitoring (ICGM) systems. This device automates blood glucose monitoring and insulin delivery, significantly reducing the need for manual intervention. Modern ICGMs also offer features like real-time health data tracking via smart devices, providing users with greater convenience. However, alongside these benefits come security challenges.

ICGM systems have evolved into compact, wearable devices that primarily use Bluetooth technology for connectivity. While Bluetooth includes security features such as encryption, device authentication, and access control, additional safeguards like user authentication and validation depend on device manufacturers. Insulin pump systems face growing cybersecurity risks, making strong user access and validation mechanisms essential. Research is now focusing on innovative methods to secure these devices from unauthorized access and attacks, ensuring they remain safe for patients to use.

Health Canada's medical device regulations categorize glucose monitors as Class III devices, signifying a medium-to-high risk level.

Securing Access to Connected Diabetes Devices

The primary user of connected diabetes devices is typically the patient or owner, but authorized family members or caregivers who assist the patient can also be granted access. This Protection Profile assumes that any authorized user has access to the device's features, without distinguishing between specific roles. To prevent unauthorized access, it is essential for the user or caregiver to ensure that only authorized individuals such as the patient, immediate family, or caregivers can log in or operate the device. Securing user access begins with identifying where sensitive data is stored and determining who needs access to it.

One effective way to manage this is by creating an access control matrix. An access control matrix is a table that specifies which users (subjects) have permissions to access which resources (objects). A subject is an individual or role requiring access, while an object refers to files, resources, data, or tools necessary for tasks. This matrix helps define and limit access, reducing the risk of unauthorized use or exposure of sensitive information.

Physical Access Control

The loss or theft of connected insulin devices could lead to unauthorized alterations of critical data, software, and firmware. Physical access threats may occur through standard user interfaces, especially if the device lacks proper authentication. Attackers might also target external hardware ports or directly access the device's storage, causing potential damage. Additionally, attackers could misuse displayed or printed unique serial numbers during the pairing process with remote devices to establish malicious connections that seem legitimate. To address these threats, Serial numbers should be encrypted or hidden to reduce the risk of exploitation.

Multi-Factor Authentication (MFA) for Connected Devices

MFA software can be installed on either a Shared Health-managed device or a personal smartphone to enhance the security of connected diabetes devices. It uses minimal mobile data and can be configured to avoid using any data at all. When MFA is required, the Microsoft Authenticator app sends a push notification to the user's phone. If the push notification is not approved, a One-Time Passcode (OTP) can be used instead. This six-digit OTP allows the user to enter it into their smartphone when accessing or managing their connected diabetes device. During MFA registration, users can select either the OTP or the push notification as their primary authentication method.

We propose implementing MFA for integrated continuous glucose monitoring (ICGM) systems to enhance security. As MFA becomes the standard for protecting online services, it safeguards against unauthorized access and prevents sharing of login information, especially for sensitive data in connected diabetes devices.

Fingerprint Access Control for Insulin Pump

The Fingerprint-based Insulin Pump Security (FIPsec) system enhances insulin pump security by requiring fingerprint authentication before granting access. This approach blocks unauthorized requests and safeguards the pump from potential attacks after access attempts. Using an advanced matching method for user verification, FIPsec has shown a low error rate, making it an effective and reliable solution to prevent unauthorized access and ensure the pump's safety.

Access Validation for ICGM Systems

Automatically log users out after a period of inactivity to mitigate the risks of unauthorized access and ensure continuous protection of sensitive data. and limit the duration of user sessions and require re authentication for sensitive actions, such as dose adjustments or firmware updates, to enhance security.

These measures help ensure secure, controlled access to the ICGM system, reducing the possibility of unauthorized actions.

Voiceprint-Based Access Control

To improve convenience and usability, we recommend that manufacturers consider a voiceprint-based access control system. This system would feature anti-replay speaker verification and voiceprint-based key agreement to secure communication between the CareLink USB and insulin pump, ensuring accessibility for blind and visually impaired users.

Resistance to Physical Attacks Via Open Ports

This rule aims to address a security issue where ports like USB, used during development to load test software onto a connected diabetes device (CDD), remain enabled in the final product. If these ports aren't permanently disabled during manufacturing, they could pose a risk. For instance, someone could purchase a device, analyze its hardware and software, and find vulnerabilities to exploit through its Bluetooth connection. The rule does not focus on protecting user data, such as blood sugar readings, stored directly on the devices. Instead, the team developing these standards agreed that privacy is better managed by the systems where the data is sent and processed, like cloud platforms, rather than on the devices themselves.

Personalized Infusion Pattern-based Access Control

A personalized access control system (PIPAC) for wireless insulin pumps that can successfully detect two types of wireless attacks with great accuracy. We suggest a new security method called Personalized Infusion Pattern-based Access Control (PIPAC). This system uses machine learning to understand a patient's normal insulin use, including how much insulin they need, how fast, and when. The system uses this information to set safe limits and spot unusual activities. Two ways someone could attack insulin pumps through wireless connections:

- A single large overdose, where a lot of insulin is given at once.
- A slow, long-term overdose, where small extra doses are added over time.

Both attacks can happen quietly and put patients' lives at risk

PIPAC has two parts:

- One to detect unusual single doses (bolus insulin).
- Another to catch strange patterns in regular, ongoing doses (basal insulin).

Studies showed that it was highly effective at detecting both types of attacks. This approach prioritizes safeguarding drug administration by using real-time data and patient-specific information while establishing defenses against process-aware attacks.

Secure and Immutable Firmware for Insulin Pump

Firmware designed to prevent unauthorized modifications ensures the integrity of insulin pumps. This includes using read-only memory (ROM) or EEPROM, with built-in protections to block unauthorized reprogramming. By implementing such access control and validation measures, the system prevents tampering, ensuring the device operates securely and as intended.

Emergency Access Provisions for Insulin Pumps

a) Emergency Override: Implement an override mechanism to allow operation of the insulin pump in critical situations while ensuring that long-term security measures remain intact.

b) Temporary Access Codes: Enable healthcare providers or emergency contacts to gain temporary access through time-limited, revocable codes, ensuring secure, controlled access in urgent situations.

These provisions balance accessibility and security, ensuring the device can function in emergencies without compromising its overall protection.

Secure Folder

Secure Folder acts as a digital locker available on most smartphones and tablets running Android 7.0 or newer firmware. It enhances digital privacy by providing a secure space to store private information users don’t want others to access. With Secure Folder, users can store various types of data, including documents, directly on their phone. The folder is protected by an advanced security platform that encrypts user data. For added security, users can lock the folder with a password, PIN, or biometric

authentication. Additionally, users can add apps, such as glucose monitor apps, to the Secure Folder to operate separate accounts from the regular app version. The folder can also be hidden by removing its icon from the home screen and app drawer, keeping it discreet and out of sight. To use the Secure Folder feature, open your smartphone's settings, navigate to Privacy, and follow the steps to enable it.

Most smartphones released after 2021 include a built-in Secure Folder or similar app for protecting confidential files. It's best to use this in-built feature, as it provides optimized security and eliminates the need for additional apps.

Managing User Access for Lost or Stolen Mobile Devices in Connected Systems

If your mobile device linked to an integrated continuous glucose monitoring (ICGM) system is lost or stolen, take immediate steps to protect the device and the sensitive health data it holds. Use tracking, locking, and remote erasure features offered by iOS and Android devices. Enabling authentication, such as passcodes or biometrics, adds an extra layer of security. Additionally, log out of your ICGM app remotely and change any associated passwords to prevent unauthorized access.

Software Maintenance

Update Requirements

The most recent reference document by the FDA in regard to Cybersecurity stresses that Firmware and Software Updates should occur in a secure and timely manner in devices.

The guidance document lists these specific goals for a proper update policy:

- *Design devices to anticipate the need for software and firmware patches and updates to address future cybersecurity vulnerabilities. This will likely necessitate the need for additional storage space and processing resources.*
- *Consider update process reliability and how update process works in event of communication interruption or failure. This should include both considerations for hardware impacts (timing specifics of interruptions) and which phase of the update process the interruption or failure occurs.*
- *Consider cybersecurity patches and updates that are independent of regular feature update cycles.*
- *Implement processes, technologies, security architectures, and exercises to facilitate the rapid verification, validation, and distribution of patches and updates.*
- *Preserve and maintain full build environments and virtual machines, regression test suites, engineering development kits, emulators, debuggers, and other related tools that were used to develop and test the original product to ensure updates and patches may be applied safely and in a timely manner.*
- *Maintain necessary third-party licenses throughout the supported lifespan of the device. Develop contingency plans for the possibility that a third-party company goes out of business or stops supporting a licensed product. Modular designs should be considered such that third-party solutions could be readily replaced.*
- *Implement a secure process and mechanism for providing validated software updates and patches for users.*

(FDA, 2023)

Health Canada maintains a similar priority list relating to the monitoring and response to emerging risks. Their list of potential considerations include:

- **Post-market vigilance**: A plan to track, assess, and respond to newly discovered vulnerabilities.

- **Patching**: A plan to update the software to maintain the safety and effectiveness of the device either regularly, or in response to an identified vulnerability.
- **Vulnerability Disclosure**: A formalized process for obtaining cybersecurity vulnerability information, assessing vulnerabilities, developing mitigation and remediation strategies, and disclosing the existence of vulnerabilities and mitigation or remediation approaches to various stakeholders.
- **Information sharing**: Participation in Information Sharing Analysis Organizations (ISAOs) or Information Sharing and Analysis Centres (ISACs) that promote the communication and sharing of updated information about security threats and vulnerabilities.

(Health Canada, 2019)

These updates may not need to be tied to feature updates for the Pocket Clinic devices, but there should be a procedure in place to push updates for cyber security onto the devices. Some aspects of this process such as the technical details on how to update the software of the app and firmware on the device should overlap with existing processes that should not differ significantly for cyber security focused updates.

Approval Requirements for Cyber Security Focused Updates

While this may cause concerns that it may require reapproval, Health Canada guidance on what is considered a “significant change” of a medical device clarifies that changes that are made solely to strengthen cybersecurity and do not have any other impact on the software or the device as a ‘not significant’ change (Health Canada, 2024).

The FDA has a similar position on updates for cyber security. In a 2017 guidance document on software security updates, it mentions that proactive software security patches as well as adding encryption and additional access control for remote users as two events that do not require submitting a 510 (k) form, although they do recommend documenting the changes made to file (FDA, 2017).

In all cases, the rare situation a cybersecurity update would require significant changes to communication between device and app or other potential changes, these guidelines would need to be examined in greater detail to see if re-approval would be required.

Tracking Vulnerabilities

Tracking potential vulnerabilities is a large component of keeping updated for cyber security. The Open Web Application Security Project (OWASP) produces a list of the

most common cyber security vulnerabilities, and Vulnerable and Outdated Components has been a common issue in both its 2017 and 2021 lists (OWASP, 2024). The following sections will deal with how to stay updated on security concerns on the General and Application Updates, the cloud Service, and the Microcontroller. Updates also include ensuring aspects of Pocket Clinic's own security such as antivirus and antimalware systems are updated.

For finding vulnerabilities, the two best places to monitor are the NIST National Vulnerability database (NVD) and the CVE Database. Each keeps track of vulnerabilities that can be tracked and filtered for specific platforms and tools.

A cyber threat intelligence (CTI) platform (sometimes referred to as a Threat Intelligence Platform or TIP) could help ensure that the company stays notified on the current cyber security climate including potential risks and threats. There are also Open-Source Threat Intelligence (OSINT) tools that could also be used. potentially integrating into a Security Information and Event Management system, or SIEM (Bolen, 2024).

Updates for Application

Application updates would need to be provided through the app store of the device, whether Google, Apple or other Service. Cyber security news and notices should be monitored for potential hazards that may require investigation and updates. While security updates should be made available as soon as possible, considerations for times for updates to occur for the user to not interfere with the medical device should be taken, either by letting the user choose a time for updates or timing updates for when the medical device does not need to operate.

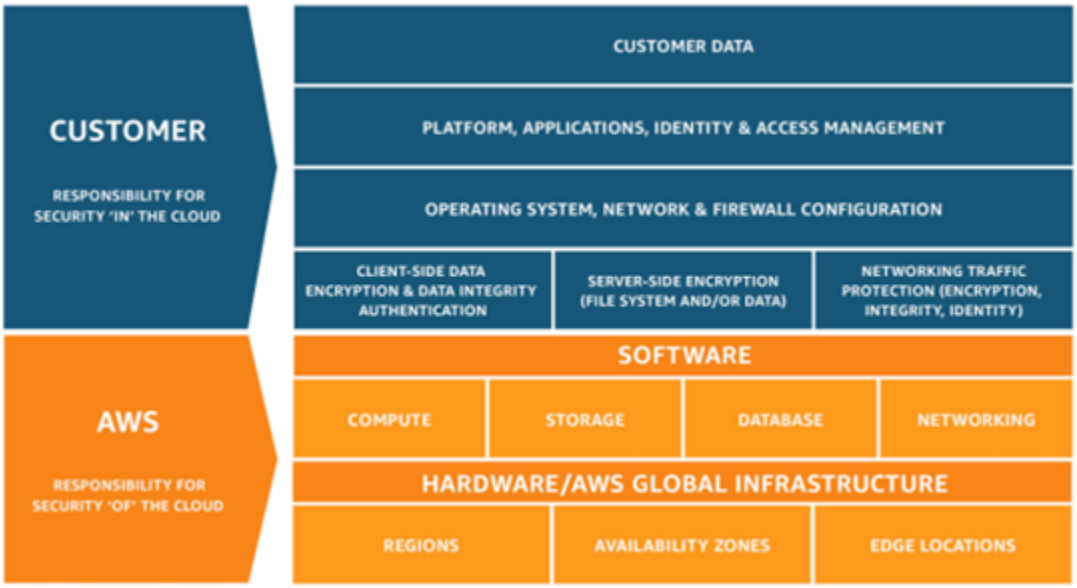
For looking for outdated libraries in the application software, a Software Composition Analysis (SCA) tool could automatically monitor any third party libraries that may be used in the code in order to check them for existing weaknesses (Crowdstrike, 2023). Taking note of and having a listing of libraries and resources used during development can also help to crosscheck and find where to look in the event that a library has a weakness discovered.

Updates for Cloud Service

For updates regarding security on the cloud system, Amazon hosts a page on AWS that outlines the most important security updates. For AWS products, it is important to monitor their published security bulletins. These bulletins can be found on the AWS webpage, which shares vulnerabilities for awareness and important security notices that require updates (Amazon Web Services, 2024a). Some vital security updates could

require more prompt updates, while others could wait for being packaged with normal updates.

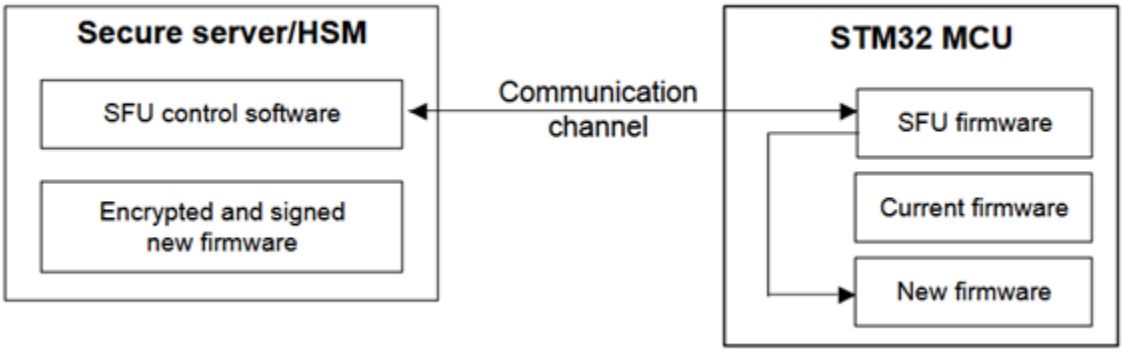
AWS assigns security in the cloud by a shared responsibility model – with Amazon responsible for the software and hardware that powers the cloud services, while the customer is responsible for the security of the customer data, identity management, systems they use and the client, server and networking encryption. Their model is shown in Figure 1.



AWS Shared Responsibility Model. Image sourced from AWS Cloud Services (AWS, 2024b)

Updates for Microcontroller

The microcontroller website describes details on how to process a secure firmware update (SFU) to download new firmware images to the device when required. The microcontroller security reference document outlines the process of how the update proceeds in more detail, summarized in Figure XX (STMicroelectronics, 2024).



Firmware update process with the SFU. Image sourced from Microcontroller Guidance Document (STMicroelectronics, 2024).

Similar to how the process may be prioritized for the application, updates for the microcontroller can be done over the air, timed for when the device is not in use or at the user's discretion. If there are multiple devices being used, having one device updated while not in use is also an ideal strategy to ensure it is not medically necessary and can be inoperable for a longer period of time.

Data Integrity and Confidentiality

FDA Data Integrity and Confidentiality Requirements

As per the most recent guidance document provided by the Food and Drug Administration concerning medical device cyber security, it is important to verify the integrity of all incoming data. Below are the guidelines set by the FDA regarding data integrity and confidentiality.

- Verify the integrity of all incoming data, ensuring that it is not modified in transit or at rest. Cryptographic authentication schemes verify data integrity, but do not verify data validity. Therefore, the integrity of all incoming data should be verified to ensure that it is not modified in transit or at rest.
- Validate that all data originating from external sources is well-formed and compliant with the expected protocol or specification. Additionally, as appropriate, validate data ranges to ensure they fall within safe limits.
- Protect the integrity of data necessary to ensure the safety and effectiveness of the device.
- Manufacturers should ensure support for the confidentiality of any/all data whose disclosure could lead to patient harm. Loss of confidentiality of credentials could be used by a threat-actor to effect multi-patient harm. Lack of encryption to protect sensitive information and or data at rest and in transit can expose this information to misuse that can lead to patient harm.

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submission (P. 37)

With Pocket Clinic's portable insulin injection device, sensitive information necessary for the proper operation of the device is stored and used by the device and mobile application. Information such as insulin dosage, glucose levels linked to an insulin bolus dose, and other patient data are transmitted. In order for this device to properly function it is imperative that information is sent and received correctly.

As data is communicated between a mobile device application and portable insulin pump through Bluetooth it is important that data integrity is maintained both during in-transit remote communications and when stored in memory. Additionally, it is important that the information sent and stored during use of the device must remain confidential. In compliance with HIPAA and PIPEDA, patients' medical and personal identifiable information (PII) must not be compromised.

Vulnerabilities and Threats to Data Integrity and Confidentiality

Bluetooth communications are widely used in many industries and as such have a wide range of documented vulnerabilities. In particular improper configuration can leave Bluetooth transmissions susceptible to a "*Man-in-the-Middle"* attack. This cyber attack involves a malicious third-party intercepting data in-transit and possibly modifying the information. If there are no controls in place to verify the data's validity, the endpoints would have no way of knowing that incoming data actually originates from the intended sources. Depending on the severity of the attack, the attacker may also gain access to sensitive information which threatens confidentiality.

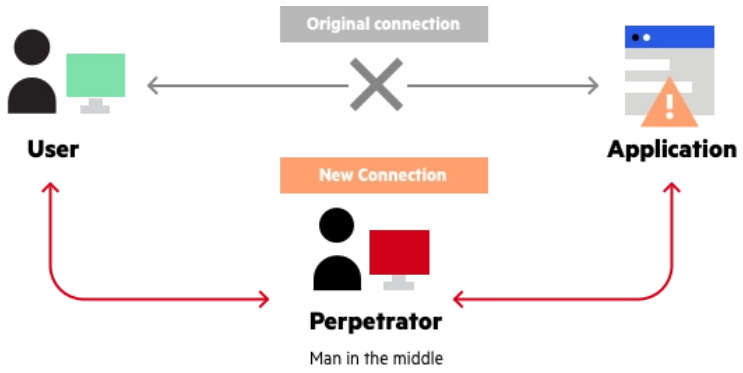


Illustration of a MitM Attack – Image Sourced from imperva

There exists a specific vulnerability as an entry on the Common Vulnerabilities and Exposures (CVE) Database that is relevant to Pocket Clinic's Bluetooth Device. CVE-2023-24023 describes a vulnerability affecting Bluetooth Core Specification 4.2 to 5.4 in which attackers can use a MitM attack in order to force short key length and expose encryption keys. As the STM32WB15 Microcontroller is compliant with Bluetooth version 5.4, Pocket Clinic's system is at risk to this specific vulnerability.

According to Bluetooth's security notice, the following is recommended in order to mitigate the vulnerability.

Maintaining Data Integrity & Confidentiality

Data Validation and Verification

All data transmitted through remote communications must be verified such that it is determined to be unmodified and received only from the intended source. Information must also be valid and accurate especially due to the risks of patient health. Below lists some recommended practices to ensure both verification and validation of information.

Data Verification	***Data Validation***
Cryptographic Authentication	Format Checks
Data Signing/Certificates	Safety Range Checks
Data Hashing	Consistency Checks
Checksums	Presence Checks

Proper validation and verification will protect data confidentiality and ensure data integrity. These practices must be maintained all throughout the software development process. Proper quality assurance and testing must be done consistently with any updates or changes to the system.

> Implementations are advised to reject service-level connections on an encrypted baseband link with key strengths below 7 octets. For implementations capable of always using Security Mode 4 Level 4, implementations should reject service-level connections on an encrypted baseband link with a key strength below 16 octets. Having both devices operating in Secure Connections Only Mode will also ensure sufficient key strength.

Bluetooth.com Security Notice on the BLUFFS Vulnerability

Access Control

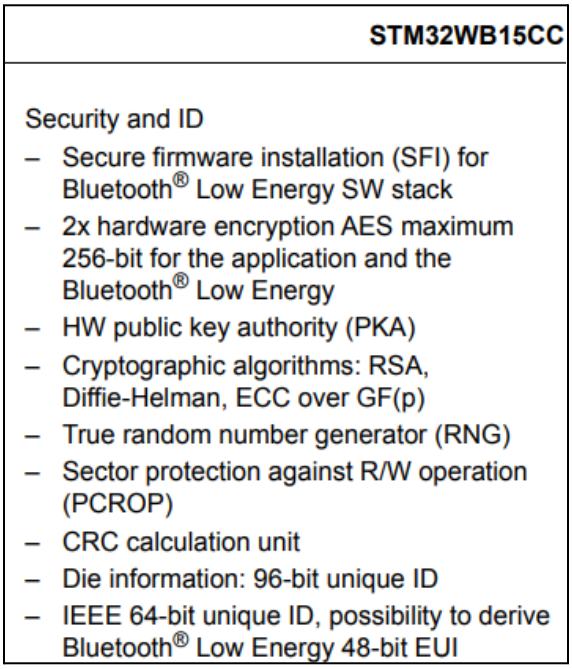
As noted in the section on authentication, properly restricting communication between the mobile application and the insulin device will help maintain data integrity. Authenticating that all data received comes from an account belonging to the user will prevent any unauthorized data tampering.

Proper authentication also protects the patient information from being accessed by unauthorized parties, maintaining privacy.

Data Encryption

Encrypting sensitive data during both end-to-end transmission and through use of secure communication protocols and at-rest using disk encryption aid in both data integrity and confidentiality. Bluetooth 5.4, which is used by the microcontroller allows for encrypted and authenticated data transmission. It is important to configure device-to-device communication properly such that it utilizes these security methods.

Implementing disk encryption will mitigate the effect of any data breaches. It is important that any stored patient information be encrypted using secure cryptographic methods. According to the STM32WB15 datasheet, the microcontroller supports many security protocols and cryptographic algorithms. Ensure that the application-layer utilizes these encryption methods.



STM32WB15CC
Security and ID – Secure firmware installation (SFI) for Bluetooth® Low Energy SW stack – 2x hardware encryption AES maximum 256-bit for the application and the Bluetooth® Low Energy – HW public key authority (PKA) – Cryptographic algorithms: RSA, Diffie-Helman, ECC over GF(p) – True random number generator (RNG) – Sector protection against R/W operation (PCROP) – CRC calculation unit – Die information: 96-bit unique ID – IEEE 64-bit unique ID, possibility to derive Bluetooth® Low Energy 48-bit EUI

Excerpt of Security Features on the STM32WB15CC Microcontroller Datasheet

Logs and Auditing

Keeping access and event logs will aid in monitoring as well as post-incident forensic analysis. Access logs can keep track of user access, activity, and can proactively warn against intrusion attempts. Proper logging can detect unusual activity using user baselines such as known locations and active use hours, notifying the system when an access out of the ordinary occurs. In the case of an incident, maintaining logs will aid in diagnosing the attack and help make security changes post-incident.

Baseline Cybersecurity Practices

While the majority of the report focused on the device's security, an essential part of ensuring the security of the data is ensuring that baseline cybersecurity practices are followed for both the device and the company itself. These first six areas will focus on a specific risk and mitigations to counter and mitigate each risk.

1. Physical Security

- **Risk:** Unauthorized physical access to medical devices.
- **Mitigation:**
    - Device Hardening: Implement physical security measures to prevent unauthorized access to medical devices.
    - Tamper Detection: Use tamper-evident seals and sensors to detect and respond to physical tampering.
- **Validation Tests:**
    - Conduct physical penetration tests to evaluate the effectiveness of device hardening and tamper detection mechanisms
- **Implementation:**
    - Install tamper-evident seals and sensors on devices. Ensure physical access controls, secure storage and handling of devices.

2. Network Security

- **Risk:** Unauthorized access to the network.
- **Mitigation:**
    - Firewalls: Deploy firewalls to monitor and control incoming and outgoing network traffic based on predetermined security rules.
    - Intrusion Detection Systems (IDS): Implement IDS to detect and respond to potential security breaches in real-time.
- **Validation Tests:**
    - Perform network penetration tests and regular monitoring using IDS to validate firewall configurations and network security.
- **Implementation**:
    - Configure and maintain firewalls and IDS. Regularly update network security protocols.

3. Endpoint Security

- **Risk**: Malware and virus attacks on devices.
- **Mitigation**:
    - Antivirus and Anti-Malware: Ensure all devices have up-to-date antivirus and anti-malware software to protect against malicious attacks.
    - Endpoint Detection and Response (EDR): Use EDR solutions to continuously monitor and respond to threats on endpoints.
- **Validation Tests**:
    - Regularly update and scan devices with antivirus and anti-malware software. Use EDR solutions to monitor and respond to threats.
- **Implementation**:
    - Regularly update and scan devices with antivirus and anti-malware software and use EDR solutions.

4. Security Policies and Procedures

- **Risk**: Lack of clear security policies leading to inconsistent security practices.
- **Mitigation:**
    - Access Control Policies: Develop and enforce policies that define who can access what information and under what conditions.
    - Incident Response Procedures: Establish clear procedures for responding to security incidents, including roles and responsibilities.
- **Validation Tests:**
    - Conduct security policy audits and simulate incident response scenarios to ensure policies are effective and procedures are followed.
- **Implementation:**
    - Develop detailed access control policies and incident response plans. Train staff on these policies and procedures.

5. Regular Security Assessments

- **Risk**: Undetected vulnerabilities in the system.
- **Mitigation:**
    - Penetration Testing: Conduct regular penetration testing to identify and address vulnerabilities before they can be exploited.
    - Vulnerability Scanning: Use automated tools to regularly scan for and remediate vulnerabilities in the system.
- **Validation Tests:**

    - Schedule regular penetration testing and automated vulnerability scans to identify and address vulnerabilities.
- **Implementation:**
    - Establish a schedule for regular penetration testing and vulnerability scanning. Address identified vulnerabilities promptly.

6. Supply Chain Security

- **Risk:** Security risks from third-party vendors and suppliers.
- **Mitigation:**
    - Vendor Risk Management: Assess and manage the security risks associated with third-party vendors and suppliers.
    - Secure Software Development Lifecycle (SDLC): Ensure that security is integrated into every phase of the software development lifecycle.
- **Validation Tests:**
    - Perform security assessments of third-party vendors and conduct regular audits of the SDLC to ensure security is integrated throughout the development process.
- **Implementation:**
    - Develop a vendor risk management program and integrate security into the SDLC. Regularly review and update security practices.

Additional Baseline Cybersecurity Practices

These practices go over other additional steps to security, including reiterating compliance requirements including steps of an incident response plan.

1. Device Security

- Secure Boot: Ensure that the device boots using only trusted software by implementing secure boot mechanisms.
- Hardware Security Modules (HSM): Use HSMs to manage and protect cryptographic keys.

2. Data Security

- Data Anonymization: Implement data anonymization techniques to protect patient privacy while using data for analysis.

- Data Loss Prevention (DLP): Use DLP solutions to monitor and protect sensitive data from unauthorized access or transfer.

3. Mobile App Security

- App Hardening: Apply techniques such as code obfuscation and anti-tampering measures to protect the mobile app from reverse engineering and tampering.
- Secure App Development: Follow secure coding practices and conduct regular code reviews to identify and fix vulnerabilities.

4. Cloud Security

- Cloud Access Security Broker (CASB): Use CASB solutions to enforce security policies and monitor cloud usage.
- Secure Configuration: Ensure that cloud services are configured securely to prevent unauthorized access and data breaches.

5. Compliance and Regulations

- HIPAA Compliance: Ensure that all security measures comply with relevant regulations such as the Health Insurance Portability and Accountability Act (HIPAA).
- Regular Compliance Audits: Conduct regular audits to ensure ongoing compliance with industry standards and regulations.
- Risk Management: Conduct device-specific risk management, including risk assessments and mitigation strategies.
- Verification and Validation: Perform verification and validation testing to ensure the device meets security requirements.
- Documentation: Provide detailed documentation, including risk assessments, security measures, and testing results.
- FDA Requirements
    - Secure Design: Ensure that the device is designed with security in mind, including secure boot and hardware security modules (HSM).
- Health Canada Requirements
    - Medical Device Cybersecurity Strategy: Develop a comprehensive cybersecurity strategy, including secure design and risk management.

6. Incident Response

This Incident Response Plan description follow NIST categories, however there are similar equivalent steps that can be found in other methods.

- ***Preparation***
    - Incident Response Plan: Develop a comprehensive incident response plan that includes roles, responsibilities, and procedures for responding to security incidents.
    - Training: Conduct regular training for staff on incident response procedures.
- ***Detection and Analysis***
    - Monitoring: Implement continuous monitoring to detect potential security incidents.
    - Analysis: Use tools and techniques to analyze and understand the nature and impact of the incident.
- ***Containment, Eradication, and Recovery***
    - Containment: Implement measures to contain the incident and prevent further damage.
    - Eradication: Remove the cause of the incident and ensure that the system is clean.
    - Recovery: Restore affected systems and services to normal operation.
- ***Post-Incident Activities***
    - Review: Conduct a post-incident review to identify lessons learned and improve future response efforts.
    - Reporting: Document the incident and report it to relevant authorities as required.

Cost-Effective/Readily Available Cybersecurity Solutions

The following list identifies some resources that can be used for cost-effective solutions which can be used, such as a wide variety of open-source tools.

1. Risk Assessment and Management:

- Open-Source Tools: Utilize open-source risk assessment tools like OWASP Risk Assessment Framework. These tools are free and widely used in industry.
- Regular Audits: Conduct regular internal audits to identify vulnerabilities without the need for expensive third-party services.

2. Security Policies and Procedures:

- Templates and Frameworks: Use free or low-cost templates from reputable sources like NIST or ISO to develop security policies and procedures.
- Policy Management Software: Consider affordable policy management software like PolicyTech, which offers a cost-effective way to manage and enforce policies.

3. Access Control:

- Role-Based Access Control (RBAC): Implement RBAC using built-in features of your existing IT infrastructure, such as Active Directory.
- Multi-Factor Authentication (MFA): Use free or low-cost MFA solutions like Google Authenticator or Microsoft Authenticator to enhance access control.

4. Network Security:

- Open-Source Firewalls: Deploy open-source firewall solutions like pfSense, which provide robust security features without high costs.
- Network Segmentation: Use VLANs (Virtual Local Area Networks) to segment your network, which can be done with existing network hardware.

5. Endpoint Security:

- Antivirus and Anti-Malware: Utilize free or low-cost antivirus solutions like Avast or Bitdefender for endpoint protection.
- Regular Updates: Ensure all devices are regularly updated and patched using built-in update mechanisms.

6. Data Protection:

- Encryption Tools: Use open-source encryption tools like VeraCrypt for data at rest and Let's Encrypt for data in transit.
- Data Backup Solutions: Implement affordable cloud backup solutions like Backblaze or use built-in backup features of your operating systems.

7. Incident Response:

- Incident Response Plan Templates: Use free templates from sources like SANS Institute to develop an incident response plan.
- Regular Drills: Conduct regular incident response drills using internal resources to keep costs low.

8. Security Awareness Training:

- Online Training Platforms: Utilize free or low-cost online training platforms like Cybrary or Infosec IQ for employee training.
- Phishing Simulations: Use free tools like Gophish to conduct phishing simulations and improve employee awareness.

9. Monitoring and Logging:

- Open-Source SIEM: Deploy open-source Security Information and Event Management (SIEM) solutions like Wazuh for continuous monitoring and logging.
- Log Management Tools: Use free log management tools like Graylog to analyze and review logs.

10. Compliance and Auditing:

- Compliance Checklists: Use free compliance checklists from sources like HIPAA Journal or PIPEDA/PHIPA resources to ensure regulatory compliance.
- Internal Audits: Conduct regular internal audits using existing staff to minimize costs.

References

Addictions & Mental Health Ontario. (2023, October 23). *Privacy Toolkit – Addictions & Mental Health Ontario*. https://amho.ca/our-work/quality-data/privacy-toolkit/

AlFuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347-2376.

Amazon Web Services. (2024a). Security Bulletins. https://aws.amazon.com/security/security-bulletins/

Amazon Web Services. (2024b). Shared Responsibility Model. https://aws.amazon.com/compliance/shared-responsibility-model/

Avast. (n.d.). *Avast | Download Free Antivirus & VPN | 100% Free & easy*. Avast Antivirus. https://www.avast.com/en-us/index#pc

Bitdefender - global leader in cybersecurity software. (n.d.). Bitdefender. https://www.bitdefender.com/en-ca/

Bluetooth Core Specification (Amended) 5.4. Available at: https://www.bluetooth.com/specifications/specs/core-specification-amended-5-4/. Assessed on 2024-12-01.

Bolen, Scott. (2024). How to Implement CTI Strategies to Protect Your Small Business in 2025. https://medium.com/@scottbolen/how-to-implement-cti-strategies-to-protect-your-small-business-in-2025-7a0547ccdd69

Chase, M., Coley, S. C., Connolly, J., Daldos, R., & Zuk, M. (2022, November 14). *Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook*. MITRE. https://www.mitre.org/news-insights/publication/medical-device-cybersecurity-regional-incident-preparedness-and-response

Crowdstrike. (2023). Software Composition Analysis (SCA). https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/software-composition-analysis/

CVE. (2024). CVE – Search CVE List. https://cve.mitre.org/cve/search_cve_list.html

CVE-2017-0785: Available at: https://nvd.nist.gov/vuln/detail/CVE-2017-0785.

CVE-2019-9506: Available at: https://nvd.nist.gov/vuln/detail/CVE-2019-9506.

CVE-2020-10135: Available at: https://nvd.nist.gov/vuln/detail/CVE-2020-10135.

CVE-2023-46447: Available at: https://nvd.nist.gov/vuln/detail/CVE-2023-46447.

Cybersecurity courses & Cyber Security training online | Cybrary. (n.d.). https://www.cybrary.it/

Dhaliwal, J. (2024, August 12). What Should I do If My Phone Gets Stolen or Lost? McAfee Blog. https://www.mcafee.com/blogs/mobile-security/what-are-the-risks-of-a-lost-or-stolen-mobile-device/

Diabetes Technology Society. (n.d.). https://www.diabetestechnology.org/dtmost.shtml

Diabetes Technology Society. (n.d.-b). https://www.diabetestechnology.org/dtsec.shtml

Dong, Z., & Kang, C. (2020). Secure device pairing using visible light communication. *IEEE Access, 8*, 11234-11245.

Eng, R. K. B. (n.d.). How are medical devices regulated in Canada? https://info.orthocanada.com/media-centre/how-are-medical-devices-regulated-in-canada

FDA Cybersecurity Guidance for Medical Devices. Available at: White Paper: Bluetooth for Medical Devices, Accessed on 2024-11-29.

FDA. (2017). Deciding When to Submit a 510(k) for a Software Change to an Existing Device. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/deciding-when-submit-510k-software-change-existing-device

FDA. (September 2023). Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions

Ferraiolo, D. F., Kuhn, R. D., & Chandramouli, R. (2016). Role-based access control. *Artech House*.

Fingerprint access control for wireless insulin pump systems using cancelable Delaunay triangulations. (2019). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/8731872

GeeksforGeeks. (2022b, November 4). How to create a secure folder on your phone? https://www.geeksforgeeks.org/how-to-create-a-secure-folder-on-your-phone/Microsoft Multi-Factor Authentication (MFA) Enrolment QRG. (2023)

Google Authenticator - Apps on Google Play. (n.d.). https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2

Graylog. (2024, November 20). *SIEM, Log Management & API protection*. https://graylog.org/

Health Canada Guidance Document: Pre-market Requirements for Medical Device Cybersecurity. Available at https://www.canada.ca/en/health-canada.html, Accessed on 2024-11-29.

Health Canada. (2019). Guidance Document: Pre-market Requirements for Medical Device Cybersecurity. https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/application-information/guidance-documents/cybersecurity/document.html

Health Canada. (2024). Draft guidance on how to interpret 'significant change' of a medical device: Types of changes. https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/application-information/guidance-documents/interpret-significant-change-medical-device/types-changes.html

Information and Privacy Commissioner of Ontario. (2015). Frequently asked questions Personal Health Information Protection Act. In *Frequently Asked Questions*. https://www.ipc.on.ca/wp-content/uploads/2015/11/phipa-faq.pdf

Information and Privacy Commissioner/Ontario, & Cavoukian, A. (2004). *A guide to the Personal Health Information Protection Act* (Debra Grant, Ed.). https://www.ipc.on.ca/wp-content/uploads/Resources/hguide-e.pdf

ISO/IEC 27001:2013. (2013). Information technology – Security techniques – Information security management systems – Requirements. *International Organization for Standardization*.

ISO/IEC 27002:2022: Information Security Controls. Available at: https://www.iso.org/standard/75652.html, Accessed on 2024-11-30.

Kanneganti, P., & Chellappan, S. (2023). IoT security challenges and solutions in modern manufacturing. *IoT Journal, 10*(3), 122-137.

Let's encrypt. (n.d.). https://letsencrypt.org/

M, S., & S, P. (2022). Towards securing Wireless insulin pump system using unsupervised deep learning technique. Research Square (Research Square). https://doi.org/10.21203/rs.3.rs-2109728/v1

Medical Device Access Management. (n.d.). Imprivata. https://www.imprivata.com/platform/access-management/medical-device-access-management

Microsoft Mobile Phone Authenticator App | Microsoft Security. (n.d.). https://www.microsoft.com/en-us/security/mobile-authenticator-app

National Institute of Standards and Technology (NIST). (2020). Framework for improving critical infrastructure cybersecurity. *NIST Special Publication 800-53 Rev. 5*.

National Institute of Standards and Technology. (2024). NVD Search and Statistics. https://nvd.nist.gov/vuln/search

NIST FIPS 198-1: The Keyed-Hash Message Authentication Code (HMAC). Available at https://csrc.nist.gov/publications, Accessed on 2024-11-28.

NIST SP 800-175B: Guideline for Using Cryptographic Standards in the Federal Government. Available at https://csrc.nist.gov/publications, Accessed on 2024-11-30.

NIST SP 800-56A Rev. 3: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. Available at https://csrc.nist.gov/publications, Accessed on 2024-11-30.

Office of the Privacy Commissioner of Canada. (2018, January 8). *PIPEDA compliance and training tools*. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/

Office of the Privacy Commissioner of Canada. (2021, August 13). *PIPEDA Self-Assessment Tool*. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/pipeda_sa_tool_200807/

OWASP Risk Assessment Framework | OWASP Foundation. (n.d.). https://owasp.org/www-project-risk-assessment-framework/

OWASP. (2024). OWASP Top Ten. https://owasp.org/www-project-top-ten/

Patient Infusion Pattern based Access Control Schemes for Wireless Insulin Pump System. (2015, November 1). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/6954561

PfSense® - world's most trusted open source firewall. (n.d.). https://www.pfsense.org/

Policy Management Software | PolicyTech. (n.d.). NAVEX. https://www.navex.com/en-us/platform/employee-compliance/policytech-policy-management-software/

Process-Aware attacks on medication control of Type-I diabetics using infusion pumps. (2023, June 1). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/10026248

Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3. *RFC 8446*.

Security for IoT systems: Standards and practices. *IEEE Standards Association*.

Smith, J. (2023). Understanding HIPAA compliance in healthcare. *HIPAA Journal, 15*(2), 123-134. https://www.hipaajournal.com/understanding-hipaa-compliance

STMicroelectronics. (2024). Introduction to security for STM32MCUs. https://www.st.com/resource/en/application_note/dm00493651-introduction-to-stm32-microcontrollers-security-stmicroelectronics.pdf

The MITRE Corporation & U.S. Food and Drug Administration. (2017). Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook. In *Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook*. https://www.mitre.org/sites/default/files/2022-11/pr-2022-3616-medical-device-cybersecurity-regional-preparedness-response-companion-guide.pdf

VeraCrypt - Free Open source disk encryption with strong security for the Paranoid. (n.d.). https://veracrypt.eu/en/

Voiceprint-Based access control for wireless insulin pump systems. (2018b, October 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/8567568

Wang, Z., Li, H., Xu, J., & Liu, Y. (2022). Enhancing IoT security through QR code pairing. *Future Generation Computer Systems, 130*, 353-368.

Wazuh. (2024, January 17). *Wazuh - Open source XDR. Open Source SIEM.* Wazuh. https://wazuh.com/

Wright, J. (n.d.). *GoPhish - Open Source Phishing Framework*. https://getgophish.com/