SOZO® Security Overview

Dated 17 May 2021

Impedimed Inc. 5900 Pasteur Court, Suite 125, Carlsbad, CA 92008 Toll Free: +1-877-247-0111 Email: info@impedimed.com
www.impedimed.com
PM-129 Rev E

Table of Contents

1 INTRODUCTION

ImpediMed is a medical device company that designs and produces medical device hardware and software. The company is committed to quality as evidenced by its certification to ISO 13485, Medical Device Quality Management System standard, and the fact that software is developed to ISO 62304:2006 Standard for Medical Device Software. The company is also committed to security and maintains HITRUST Privacy and Security Certification. The company meets ISO 14971 for its risk assessment and management of medical device design and production. ImpediMed is also compliant with many regional regulatory requirements including HIPAA. ImpediMed conducts annual HIPAA compliance assessments as well as Privacy and Security Risk Analysis to respond to the ever-evolving threats to data security. ImpediMed produces a range of bioimpedance spectroscopy (BIS) measurement medical devices including SOZO®. The SOZO solution is network connected and as a medical device manufacturer, ImpediMed is required to ensure that the devices that it manufactures are:

- Safe for use as indicated
- Cannot compromise patient care and
- Have appropriate levels of security controls in place.

This document provides a description of the product, product security features, identifies data that SOZO collects and how it is handled and secured, details of the information security processes and approaches adopted across the development lifecycle of the product as well as ImpediMed's Security practices and policies. This document is written for the 4.0 version of MySOZO and the SOZO Tablet app.
This document also provides a summary of the penetration testing that has been undertaken by an external security company.

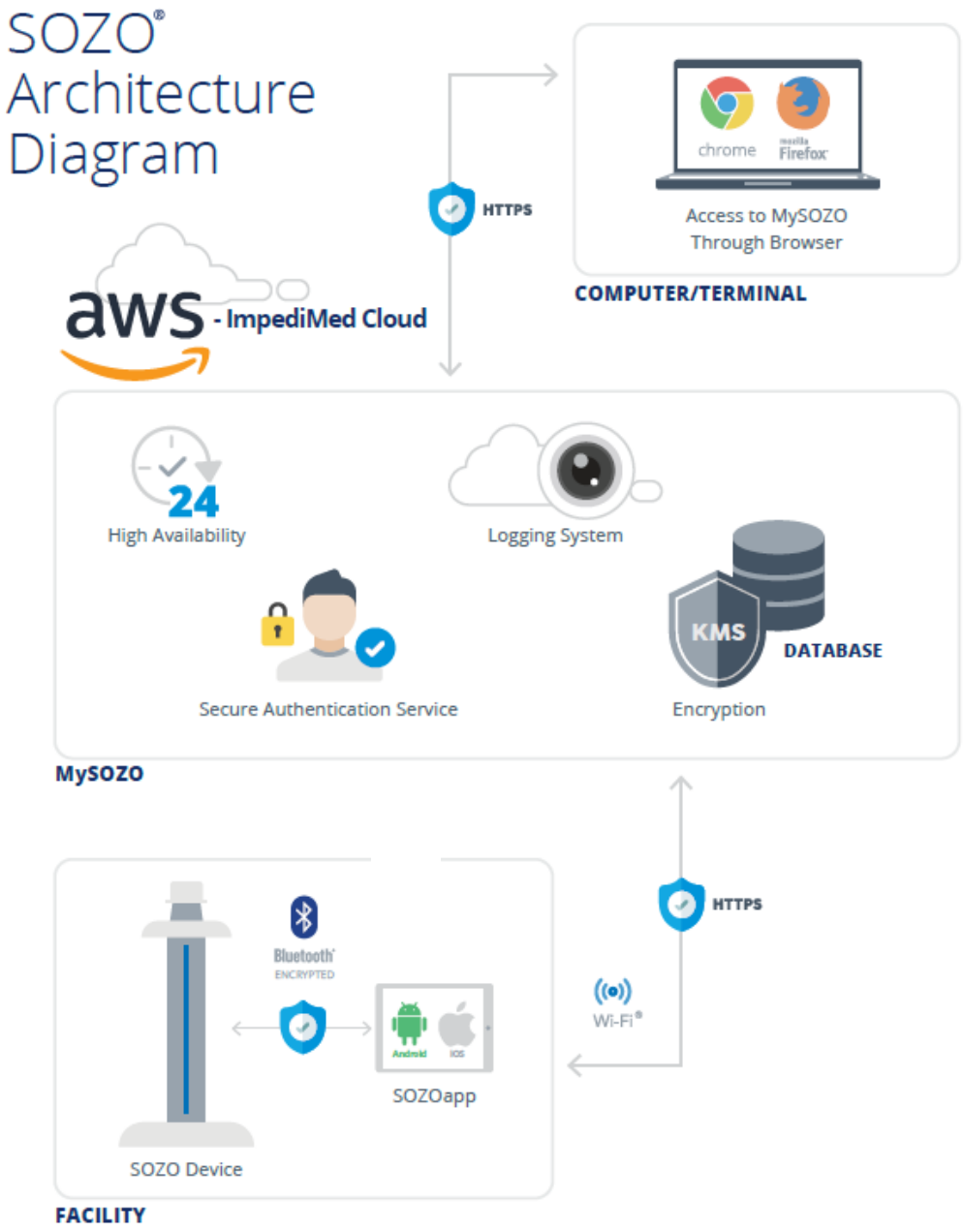
2 SOZO SUMMARY

SOZO is a solution that is comprised of a number of parts and across which different data is handled and secured.

ImpediMed produces the following components:

- SOZO Device – A hardware medical device used to take bioimpedance spectroscopy measurements of a subject who places their bare hands and feet upon the device. The device has no user interface but is controlled via Bluetooth®.
- SOZO Tablet – The SOZO Tablet is an Android Samsung Galaxy Tablet or an Apple iOS iPad Tablet provided by ImpediMed. The SOZO Tablet in conjunction with the **SOZO App** acts as the user Interface for the **SOZO Device**. The Tablet can rest atop the SOZO Device or be hand-held by clinicians when mobility is desired.

- SOZO App – A custom piece of software produced by ImpediMed used to create patient records, control the SOZO device and take measurements. The SOZO App is pre-installed on the SOZO Tablet. The SOZO App communicates with the SOZO device using an encrypted Bluetooth connection and transmits all data to the customers database on MySOZO.com over a client provided, secure private Wi-Fi network. Designed to run on a standard Samsung Android Galaxy Tablet or Apple iPad Tablet that ImpediMed supplies as part of the SOZO solution.
- MySOZO – A Web-based application hosted and managed by ImpediMed via Amazon Web Services. The SOZO Tablet App transmits measurement data from the SOZO Device to Https://www.MySOZO.com over an encrypted channel using TLS 1.2. Each customer is provisioned a logically containerized database for data storage. Clinicians and Administrators may access MySOZO to view their measurement data, patient history, analytical reports, manage user access as well as run security auditing reports.



3 SOZO SECURITY CONTROLS

SOZO has been designed with security and privacy as central requirements to its design and uses an audited Secure Software Design Life Cycle process with expert security design reviews and external highly detailed Penetration Testing (which is outlined in more detail in the ImpediMed Software Development Lifecycle for Security).

3.1 Authentication and Authorization

All Access to MySOZO requires Unique ID's and Complex Passwords. There are no shared accounts in the MySOZO system, this is to aid in non-repudiation.

Administrators create the Clinician accounts, which in turn triggers an email to the clinician with a unique time-sensitive token allowing the clinician to create their initial passwords. Administrators may also create additional administrator accounts following the same process.

Administrators can trigger another password email if a Clinician forgets their passwords. Users may also select the "forgot password" option at the login screen of MySOZO.com to trigger a password change email containing a time sensitive token link.

Administrative tasks such as user creation and security setting configuration require re-authentication for added security.

Password Complexity Requirements:

- 8 Character minimum
- 1 Upper Case, 1 Lower Case, 1 Symbol, and 1 Numeral
- Passwords cannot be repeated until 3 different passwords have been utilized.

Password expiration is set to 3 months by default, however administrators may set the expiration length according to their organization's best practices.

To prevent brute force and dictionary attacks, MySOZO provides a 30-minute lock-out period following the input of 5 failed logins.

By Default, following 60-minutes (configurable by Administrators) of activity, the SOZO system will require re-authentication.

All credentials are encrypted in transmission with TLS 1.2 and in storage via AES-256-bit encryption, passwords are also salted in the credentials database on MySOZO. Authentication to MySOZO.com utilizes JWT Secure Token Based authentication.

Multi-Factor Authentication

End-User Administrators may also enable Multi-Factor Authentication (MFA) for all users through the MySOZO Web Portal. End-Users may utilize their choice of TOTP Authenticator Applications for use with the MySOZO Web Application.

Active Directory Integration

The MySOZO application can be configured to utilize the customer organization's directory services. Both Active Directory Federation Services and Azure Active Directory may utilize SP-initiated SSO SAML 2.0 for authentication.

Following Active Directory Integration, settings and tasks such as password expiration, password history, MFA configuration and user management can be performed from the customer's Active Directory tenant.

Role-Based Access

There are three types of SOZO Accounts:

- Administrator Role – The Administrator role can create and manage Clinician accounts, trigger password resets, configure password expiration lengths, as well as monitor security logs and run audit reports.
- Clinician Role – The Clinician role can create and manage patients, take measurements, review measurement and patient history, reset their passwords using the "forgot password" option, and run multiple reports in relation to patient measurements.
- Multi-Role – The Multi-Role has privileges from both the Administrator and Clinician Role. This role is not required and should be provisioned at the customer's discretion.

3.2 Encryption

Data-In-Transit

- **SOZO Tablet to the SOZO Device** – Utilizes Bluetooth Security Mode 4. This Security Mode uses Secure Simple Pairing (SSP), in which a P-192 Elliptic Curve Diffie-Hellman (ECDH) key is utilized for link key generation to achieve AES-CCM (Apple iOS) and E0/SAFER+(Android OS) Encryption. The Android version of the Tablet utilizes Bluetooth 4.0 Classic and the iOS Version utilizes Bluetooth 4.0 BLE.
- **SOZO App to MySOZO** – The SOZO app installed on the SOZO Tablet requires an encrypted Wi-Fi connection to communicate with MySOZO.com. The SOZO Tablet supports WPA2-PSK and WPA2-Enterprise with 802.1x Authentication. SOZO App to MySOZO communication is encrypted over port 443, utilizing TLS 1.2.
- **Web Browser to MySOZO** – Administrators and Clinicians can access the MySOZO Web Portal from a workstation utilizing either a Google Chrome browser, Mozilla Firefox browser or Edge Chromium Browser. Communication between the browser and MySOZO is encrypted utilized TLS 1.2, over HTTPS port 443.

Data-at-Rest

- **SOZO Tablet and App –** The SOZO Tablet and App do not store any ePHI, however the device tablet supports native encryption using AES-128 with Cipher-block chaining and ESSIV:SHA256. We recommend all customers encrypt the SOZO Tablet. The SOZO Tablet supports most Mobile Device Management applications.
- **MySOZO**- The MySOZO database located on ImpediMed Servers is encrypted on the database level, as well as on the storage media with AES-256-bit encryption.

3.3 Security Logging and Auditing

Administrators will have access to multiple reports and logs in order to identify suspicious behavior and manage user activity. These logs cannot be modified by end-users or ImpediMed staff. The following information is logged:

- **Login information**- Successful, Failed, User Account, Time Stamp.
- **Data and Patient Records**- Creation, Deletion, Modification of records, Targeted data/record, User initiating action and Timestamp.
- **Administrative Functions**- Creation, Access/View, Deletion, Modification and exporting of Data. Creation, Modification and Deletion of users/settings. Targeted User/Setting/Data, User initiating action, and Timestamp.

4 MySOZO SECURITY CONTROLS

MySOZO is a web application hosted by ImpediMed on Amazon Web Services infrastructure. The SOZO App installed on the SOZO Tablet, transmits data to MySOZO where the Web Application performs its algorithms from the raw data and produces L-Dex Measurement results. Clinicians and Administrators may also access MySOZO web portal from Https://www.MySOZO.com. All data is stored on MySOZO, the SOZO App transmits the following data to MySOZO:

- Clinician Name
- Patient Name
- Patient Height
- Patient Weight
- Patient Age (D.O.B if over 89)
- Raw Measurement Data
- Date of Measurement

The above data is classified as Protected Health Information and as such, ImpediMed has implemented the following Security controls to protect the Confidentiality, Integrity and availability of the data as well as to adhere to Federal regulatory requirements such as the Health Insurance Portability and Accountability Act (HIPAA). ImpediMed maintains HITRUST Privacy and Security Certification and ISO: 13485 certification. Amazon Web Service's data center maintains HITrust, ISO 27001, and SOC 1, SOC 2 Certifications.

4.1 Physical Security Controls

- Badge Access Required
- Multi-Factor authentication required for access to Data Center
- Data physically behind multiple locking mechanisms
- Security Personnel at points of Entry
- Closed Circuit Television (CCTV) at points of entry, egress and within the facility
- Intrusion Detection Alarm System
- Physical Access logging and monitoring

4.2 Access and Authorization

All Employees undergo an in-depth background screening prior to employment. Access to ImpediMed resources are based on a least-privilege and need-to-know basis. All access to the MySOZO back-end requires Multi-factor authentication as well as the same complex password requirements as the SOZO system. Access to MySOZO back-end is based on IP address filtering, employees must be on ImpediMed's secured network to access the system. Access to MySOZO supporting systems are monitored and audited periodically.

4.3 Encryption

ImpediMed's Encryption methods for systems containing ePHI/PII are compliant with FIPS 140-2 security requirements for cryptographic modules.

Data-in-Transit- All data in transit is encrypted with TLS 1.2 AES-256-bit Encryption.

Data-at-Rest- All data-at-rest is encrypted with AES-256-bit Encryption, this includes backups. ImpediMed workstations, mobile devices and servers are encrypted with AES-256-bit encryption as

well. Data-at-rest encryption utilizes a Key Management Service in which only vetted and authorized ImpediMed users have access to on a “need-to-know basis”. FIPS 140-2 validated hardware security modules protect ImpediMed encryption keys. Access to this KMS system is monitored and audited periodically.

4.4 MySOZO FedRAMP Compliance

AWS US East-West (Northern Virginia, Ohio, Oregon, Northern California) has been granted a Joint Authorization Board Provisional Authority-To- Operate (JAB P-ATO) and multiple Agency Authorizations (A-ATO) for moderate impact level. The services in scope of the AWS US East-West JAB P-ATO boundary at Moderate baseline security categorization can be found within AWS Services in Scope by Compliance Program.

For US based customers, the MySOZO Web Application is hosted on in-scope AWS Services, specifically AWS US East (Northern Virginia).

4.5 High Availability and Back-ups

AWS hosted ImpediMed Servers provide redundancy and fault tolerance, fail-overs are automatic and seamless with a Recovery Time Objective of at max 5 minutes. Load balancing is also utilized to manage bandwidth and provide high availability over 9 nodes. ImpediMed systems are backed up to 2 Availability Zones in the event of a Zone failure. The physical location of customer data is stored in 1 of 3 regions dependent on the customer’s location; Data is stored within the same region in adherence with Security best practices.

ImpediMed Servers perform full back-ups daily and can restore backups that are up to 15 days old. Backups are encrypted, and restoration procedures are tested periodically.

The AWS Data Center maintains the use of fully redundant power systems without impact to operations, 24 hours a day. Mechanisms are in place control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels. AWS data centers are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems. Scheduled maintenance is performed and recorded for each of these systems.

4.6 Network Security

All Network edge locations are secured utilizing Firewalls with Intrusion prevention systems. All systems within the MySOZO architecture are segregated in their own virtual private networks and where required, only allow communication between these networks by IP address and/or MAC address filtering. This prevents unauthorized access to private data systems from public facing sites. Communication to the MySOZO back-end also utilizes IP address filtering, all ImpediMed staff accessing these systems must be on ImpediMed’s secure network. All network communication is encrypted at both data centers and ImpediMed locations.

4.7 Security Auditing and Monitoring

Systems supporting MySOZO are monitored and audited periodically. The following are monitored

and reviewed by ImpediMed:

- User Access Logs
- User Activity Logs
- Role-Based Access reviews
- Network and Firewall Activity
- Virus Scan logs
- Physical Security Maintenance logs
- Physical Access logs
- System Availability variables
- Backup monitoring

5 SOZO SOFTWARE SECURITY CONTROLS AND APPROACHES ADOPTED

The following section outlines some of the security controls that have been included into the software. The list is not exhaustive but outlines that security features that most clients have questioned when discussing the various solution elements:

5.1 SOZOapp – Android Application

Most of the logic of the application is handled by the MySOZO backend REST API and the communication occurs through secured API calls however the Android application itself implements the following security provisions:

- SOZOapp is not a publicly available app. It is only available directly from ImpediMed so is not widely available for inspection by many potential attack agents.
- There is no temporary or permanent storage of patient's, user's or measurement's data locally or in the Android KeyStore.
- Values entered in the application by the user are also checked against white list filters before they are sent to the back-end API.
- Requires authenticated and authorized actors to use the application through a login screen, command-line interface platforms cannot access MySOZO. A user needs to enter his/her credentials and upon successful authentication and authorization is able to login to the application. The authentication and authorization checks are undertaken by the MySOZO back-end secure API.
- Unique identification of the android device, for enrollment purposes, is performed using a hash of the android.os.Build.SERIAL number.
- The Android application ensures that it communicates with the correct Bluetooth device utilizing Bluetooth Security Mode 4. This Security Mode uses Secure Simple Pairing (SSP), in which a P-192 Elliptic Curve Diffie-Hellman (ECDH) key is utilized for link key generation to achieve E0/SAFER+ Encryption.
- The application implements robust logout functionality and includes an automated timed logout facility.

5.2 SOZOapp – Apple iOS Application

Most of the logic of the application is handled by the MySOZO backend REST API and the communication occurs through secured API calls however the iOS application itself implements the following security provisions:

- SOZOapp is not a publicly available app. It is only available directly from ImpediMed so is not widely available for inspection by many potential attack agents.
- There is no temporary or permanent storage of patient's, user's or measurement's data locally or in the iOS KeyStore (KeyChain).
- Values entered in the application by the user are also checked against white list filters

before they are sent to the back-end API.
- Requires authenticated and authorized actors to use the application through a login screen, command-line interface platforms cannot access MySOZO. A user needs to enter his/her credentials and upon successful authentication and authorization is able to login to the application. The authentication and authorization checks are undertaken by the MySOZO back-end secure API.
- Unique identification of the iOS Device, for enrollment purposes, is performed using a hash of the iOS.Build.SERIAL number.
- The iOS application ensures that it communicates with the correct Bluetooth device utilizing Bluetooth Security Mode 4. This Security Mode uses Secure Simple Pairing (SSP), in which a P-192 Elliptic Curve Diffie-Hellman (ECDH) key is utilized for link key generation to achieve AES-CCM Encryption.
- The application implements robust logout functionality and includes an automated timed logout facility.

5.3 MySOZO Back-end REST API

The MySOZO backend API is a crucial part of the application as it does all the heavy lifting of the application's logic and data management. The security provisions of the MySOZO backend Rest API are:

- Before a SOZOapp can communicate with the MySOZO it needs to be setup with the MySOZO network address and Backend API port AND for this to be successful a valid set of MySOZO credentials need to be supplied.
- Unauthenticated users (SOZOapp or SOZO web portal) have access only to the login/logout functionality. All other calls require an authenticated user.
- For authorization purposes the users of the system are separated in distinct roles. Access to certain functionalities are permitted based on these roles.
- Session Management is performed with the use of Tokens. Tokens are created and verified in the back end by the API's. The session length can be set by the clinic administrator in the "settings" section of the SOZO portal.
- The API always validates each user input and uses parametrized queries to prevent SQL injection type attacks.
- Regarding server-side validation of data, the API makes use of white list filters for data validation purposes of user provided data. The white list filters allow only valid data to reach the backend database. The data must also comply with data field specific validation rules.
- Each call to an API back end REST API call may be logged outlining the user, time and backend API call that was called.
- The application returns generic messages in cases of error, in order to avoid the disclosure of unnecessary information. Application debug logs are enabled by default.
- The Application returns generic messages for a failed login, in order to prevent username enumeration issues.
- The web server's header has been changed, in order to prevent attackers from fingerprinting the server type.
- The application makes use of UUIDs (Unique Universal Identifier) for referencing objects in the system. As such, attackers cannot guess valid IDs of objects for use in further attacks.
- Explicit error handling is performed in order to track the application flow and find uncaught errors. There are no areas of code that are not enclosed by error handlers to stop potential hackers from taking advantage of any induced exceptions.

5.4 MySOZO Web Portal

The MySOZO Web Portal provides a secure web-based mechanism to send information to MySOZO back end API. The connection is secured HTTPS. All security controls of the web portal are implemented at the MySOZO backend REST API level; however some additional controls are provided by the Web Portal itself such as:

- Cross-site Scripting (XSS) prevention, by using a framework which handles XSS escapes by default
- White listing user provided data to prevent malicious or incorrect values to reach the backend calls.
- Not persisting any patient data on the web browser.

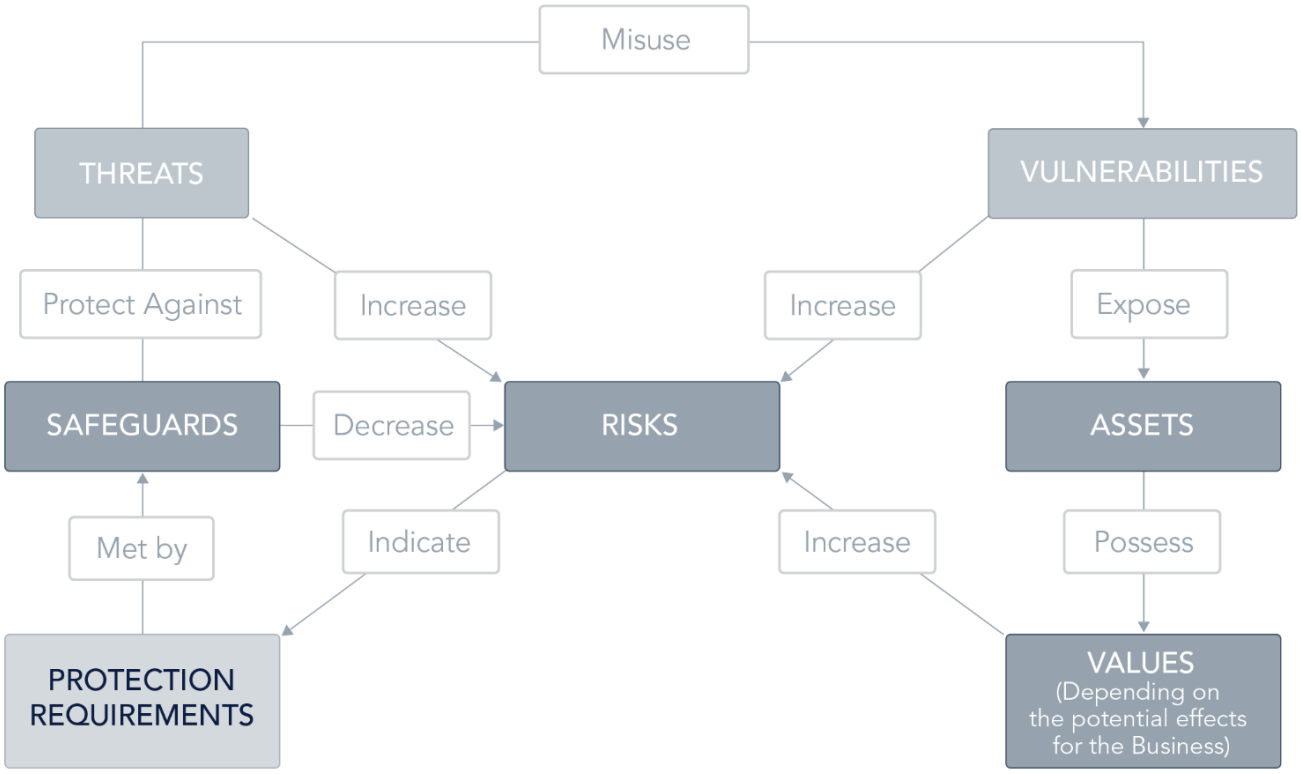
5.5 MySOZO Backend Database, Logging, and At-Rest Data

The MySOZO backend database is the only source of long-term storage of patient health information data that is considered to be “at rest”.
The database employs AWS Aurora that has been used extensively within highly secure environments and security analysis of the software is openly available. The Aurora database stores user credentials, patient personal and medical information and medical measurements.
Additionally, the security provisions implemented at the database level are:

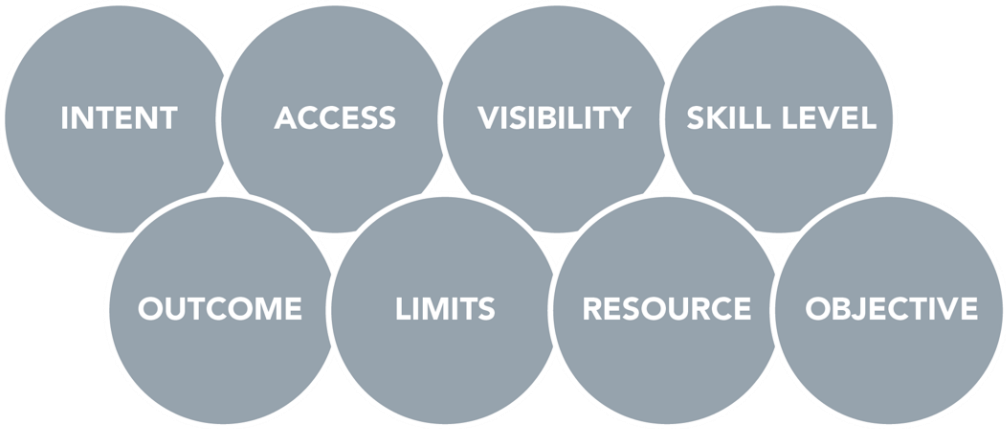
- Stored procedures are utilized for all data I/O from the Database to standardize and secure the input values. Input values that enter the SQL queries are properly used in parameterized queries to prevent any SQL Injection attacks.
- The passwords are stored hashed using SHA-256 in the database to prevent attackers from retrieving clear text passwords.
- Stored Procedures implement action audit logs which are stored in the database

6 IMPEDIMED SOFTWARE DEVELOPMENT LIFE CYCLE FOR SECURITY

ImpediMed engineers are required to work to strict processes and procedures to design and develop medical devices. ImpediMed is externally audited and certified to EN-ISO-13485 for Medical Device Quality Systems (and processes) and for its medical device software lifecycle. In addition, ImpediMed is externally audited and certified to HITRUST Privacy and Security framework for its Information Security Management and for design, development, customization, implementation, maintenance and support of medical applications.
The processes require an ongoing commitment to continual security vigilance and improvement covering all software related activities and processes. ImpediMed has developed a compliant model of Threat agents based upon a set of common characteristics or attributes which it continually monitors and updates and uses wide variety of sources to identify vulnerabilities (including software and technology vulnerabilities) that Threat agents can miscues. The classical high-level view is outlined below:



However, although the language of the above model remains valid throughout this document, ImpediMed have adopted a Threat Model based upon building up a profile of possible attackers - Threat Agents (based upon work undertaken by Intel). This systematic analysis offers a way of identifying the most likely attack vectors. The Threat Agents are identified by scored sets of attributes:



Threat Agents can be a customer competitors, opportunities or idealists. They can be complete strangers, service users or even trusted employees. They may have various motivations and objectives; they can be highly skilled or careless and unsystematic employees. They may act within the constraints of applicable regulations or may engage without legal or ethical constraints. They may be lone individuals or part of an organized group. The model fundamentally identifies the Threat Agents by answering the questions:

- Who is the agent?

- From where does the agent threaten the asset?
- Why is the agent motivated?
- How will the agent affect the company?
- Does the agent have any limits on his actions?
- Is the threat viable?
- Do the agent hostile actions require extensive funding?
- How easy is it?
- Do his actions require special skills?
- Is he going to be identified by his actions?
- Are we able to discover the occurring attack?

The Threat Agent model is updated as reviewed as part of the ongoing ISMS alongside continual awareness checking and developer training for new technical vulnerabilities (eg OWASP vulnerability database for the different technologies adopted). Threat agents build organizational awareness, assist in the environmental aspects affecting vulnerability scoring and assist in defining appropriate vulnerability responses and appropriate implementation of security controls.

7 SECURITY DESIGN CONTROLS AND DESIGN REVIEW

ImpediMed include requirements to avoid specific vulnerabilities (and have validated tests recorded as part of the Verification and Validation Reports for each software release) and for low level design and software vulnerabilities, automated code analysis tools are used alongside third party security design and code security analysis services. This makes the prevalence of vulnerabilities less likely to be incorporated in a manner that the Threat agents could misuse. The approach taken by ImpediMed is in line with FDA and EU pre-and post-market cyber security guidance recommendations.
The Medical Device Design and Software Control standards that ImpediMed is legally obliged to meet alongside the incorporation of Security Management ensures a lifecycle that incorporates strict requirements management, design controls, design verification and requirements validation. All the software is designed such that every sub component of the software (the software units) is subject to thorough design review and testing to ensure that all possible software failure modes are accounted for and handled and that the existence of common code design and code security vulnerabilities are reduced as far as possible.

7.1 Penetration Testing Overview

After each major software release candidate, the software is externally Penetration Tested.
The testing methodology employed to test the ImpediMed SOZO software is based upon the best practices described in the latest version of the OWASP Testing Guide, the OWASP Application Security Verification Standard, and the NIST Technical Guide to Information Security Testing and Assessment.
Whilst some penetration agencies will use automated tools and ‘white hat hackers’ to look for ‘external’ penetration test vulnerabilities, ImpediMed and its penetration testing company believe that this can still hide many hidden implementation vulnerabilities. Instead, ImpediMed allow the security penetration test team full access to the design documentation and software source code so that the penetration testing company can gain much better insight into the types of potential vulnerabilities that could be exploited.
ImpediMed Software is penetration tested in two phases:

- Code Review
- Testing

7.2 Penetration Testing Code Review

The external source code review is a manual review process that at times may be assisted the use

of static analysis or other tools.
The code analysis undertakes information gathering to collect information about the target application and its assisting technologies. Multiple aspects of the software are examined including:

- Program flow
- Data input and output points
- Program parameters
- User-controlled inputs
- Dependencies to other software in the system
- Interaction with the operating system,
- storage and hardware of the hosting environment
- Interaction with specialized hardware (e.g. cryptographic hardware modules)
- Manipulation of sensitive data
- Manipulation of other data
- Enforced security controls
- Ability to produce and execute new executable code

The enumeration of input/output points and technologies used by the software provides unique opportunities to lay out a complete “attack surface” of the software and allows security researchers to form a much more complete “attack plan”.
Another important step in this process is the enumeration of all third-party software. Each of these components will be checked for known vulnerabilities (CVEs, 0-days) that may cause security issues to the software under investigation.
Finally, within the information gathering stage configuration files are also inspected in order to identify configuration controls whose default / erroneous (or sometimes valid) settings introduce a security risk to the application's operation
During the *Code Auditing* step the actual code review takes place. The code review focuses on the part of the code that is considered in scope. The penetration testers will also check additional sources such as the codebase of third-party libraries for previously unknown vulnerabilities.
Code auditing takes advantage of design documentation and high-level understanding of the application code via the data collected in the information gathering stage. It analyses the software logical and functional units and these are reviewed for possible connections to unsafe input handling methods. From an attacker's perspective, controlling or affecting input data is the main way of influencing the execution flow of an application, bringing the execution to either error handling states or invalid/unauthorized states (which are often common sources of vulnerabilities in code) that traditional external systems only penetration testing would not have the insight to try and take advantage of.

7.3 Penetration Testing

As a result of the code review the penetration testing that is undertaken is much more targeted and aggressive and is able identify many more types of vulnerabilities than normal techniques. Typically, after each software release and code review penetration tests will target software units across the entire “attack surface” to ensure coverage of:

- Configuration and Deployment Management issues
- Identity Management Issues
- Authentication
- Authorization
- Access Control
- Session Management
- Data Validation
- Error Handling
- Communication and Protocol Security

- Weak cryptography
- Business Logic Errors
- Client-Side Issues
- Handling of sensitive information
- Unsafe use of third party software

7.4 Penetration Testing Vulnerability Scoring

Due to the in-depth penetration testing approach, there is more likelihood that vulnerabilities will be discovered. However, not all code and solution security vulnerabilities can be taken advantage of by all of the threat agents in all circumstances.
Many vulnerabilities will be extremely hard to take advantage of (e.g. requiring uplifted /administrative security rights or perhaps physical access that might facilitate gaining certain rights).
It is for this reason that the security risks are evaluated according to the risk they might impose to the key hosting organization and its users (clinicians and patients).
The scoring is based upon the CVSS v3.0 standard and relies upon the Threat model described earlier to determine the potential likelihood and impacts.

7.5 Outcome of Penetration Testing

The current Penetration Result summary is available upon request.
The ImpediMed patching policy is to patch any High and Medium Vulnerabilities in the next patch release of the Software and repeat the penetration testing with significant software releases.

8 ImpediMed Organizational Security Controls

ImpediMed has developed and implemented organizational Security Controls in response to ever-evolving threats to data security. These controls are based on regulatory requirements such as HIPAA as well as industry best practices such as NIST and HITRUST requirements.

8.1 HIPAA Security Regulations Compliance

ImpediMed Security and Privacy controls fulfill the following HIPAA requirements:

- Security Standards (45 C.F.R. § 164.306)
- Administrative Safeguards (45 C.F.R. § 164. 308)
- Physical Safeguards (45 C.F.R. § 164.310)
- Technical Safeguards (45 C.F.R. § 164.312)
- Organizational Requirements (45 C.F.R. § 164.314)
- Policies and Procedures (45 C.F.R. § 164.316)
- Notification to the Secretary (45 C.F.R. § 164.410)
- General Rules; Uses and Disclosures of PHI (45 C.F.R. § 164.502)
- Organizational Requirements; Uses and Disclosures (45 C.F.R. § 164.504)

8.2 HITRUST Privacy and Security Domains

- Information Protection Program
- Endpoint Protection
- Portable Media Security
- Mobile Device Security
- Wireless Security
- Configuration Management
- Vulnerability Management
- Network Protection
- Transmission Protection
- Password Management
- Access Control
- Audit Logging & Monitoring
- Education, Training and Awareness
- Third Party Assurance
- Incident Management
- Business Continuity & Disaster Recovery
- Risk Management
- Physical & Environmental Security
- Data Protection & Privacy

8.3 ImpediMed Security Policies and Procedures

ImpediMed also maintains and updates the following policies and procedures as a part of it's Privacy and Security Compliance Program:

- Privacy and Security Compliance Policy
- Risk Management Policy
- Privacy and Security Risk Analysis Policy
- Documentation for Security Compliance Policy
- Breach Determination and Reporting Policy
- Acceptable Use Policy

- Workforce Member Termination of Access Policy
- Physical Security and Clean Desk Policy
- Phishing, Malware and Hack Protection Policy
- Security Auditing and Monitoring Policy
- Password and Authentication Policy
- Management of reported Security and Privacy Incidents
- Business Continuity, Data Criticality, Backup and Disaster Recovery Policy
- Access Controls and Data Classification Policy
- Data Integrity Controls Policy
- Record Retention and Data Destruction Policy

9 Certifications

9.1 ImpediMed

In order to validate the security and quality assurance of ImpediMed products and services, ImpediMed maintains the following certifications: **EN-ISO-13485 Medical Devices** and **HITRUST Certification**. Information regarding quality control and current certifications are accessible to customers via the link below:

https://www.impedimed.com/about/quality-and-registration-certificates/

9.2 Third-Party Service Providers

All Third-Party Service Providers that support or provide infrastructure for ImpediMed products and services undergo annual vendor assessments in which availability, security and SLA performance are audited. All Third-Party Service Providers which access, transmit, or store ImpediMed data must provide ImpediMed with a current copy of a SOC 2 or equivalent report.