SOZO® Privacy Impact Assessment

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-109-US Rev G

TABLE OF CONTENTS

1.0 INTRODUCTION

ImpediMed is the world leader in the design and manufacture of medical devices employing bioimpedance spectroscopy (BIS) technologies for use in the non-invasive clinical assessment and monitoring of tissue composition and fluid status. ImpediMed is committed to quality as evidenced by its certified processes to ISO 13485 Medical Device Quality Management System standard, and 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.

This document outlines the Privacy Impact Assessment (PIA) for the suite of SOZO® products.

SOZO has been designed to ensure privacy of subject data that is collected. The analysis within this document shows that there are no Personal Privacy Issues that have been identified at this time and that the SOZO system satisfies the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy regulations.

Note: Within this document the terms Client and Customer refer to the SOZO owner who purchased the SOZO product. A person who has measurement data taken using SOZO is referred to as the Subject.
A patient could be a subject but not all subjects are patients.

2.0 SOZO® OVERVIEW

The SOZO solution consists of several separate components. These include:

- SOZO measurement device
- SOZOapp installed on the ImpediMed supplied tablet
- MySOZO Web Application hosted by ImpediMed

3.0 SOZO DEVICE

The SOZO device takes bio impedance spectroscopy (BIS) measurements of a human subject. The device is controlled by the SOZOapp using commands sent over Bluetooth by the SOZOapp. The device can be told to perform a self-test, update the firmware, and take measurements for a subject that is positioned upon the device. Self-test results and measurement results are sent back to SOZOapp over encrypted Bluetooth.
The device has no knowledge of the subject being measured or their identity. No data is stored upon the device and when results are sent to SOZOapp there is no patient identifying information.

4.0 SOZOAPP

The SOZOapp is an Android and iOS application designed to be used upon the ImpediMed supplied tablet as the user interface to control the SOZO device. Users must sign into SOZOapp using login credentials that have been setup upon the MySOZO Web Portal by a user with administrative rights or with their organization credentials if Active Directory SSO has been configured.

SOZOapp allows users to create a patient/subject records. The information captured about a subject is the minimum amount of data required to safely identify a patient within a health information system (Patient Demographic details – patient name, sex at birth, age, Medical Record Number). Additional patient data is also captured to allow correct analysis of the patient data (patient date of birth, patient height, patient weight). Patient data is never stored upon the tablet within SOZOapp. End-Users may choose to anonymize patient name, MRN and date of birth (by entering only birth year).

The SOZOapp communicates with the MySOZO Web Application through a customer secured network environment using a customer supplied and configured WIFI access point. All data sent between the SOZOapp and the MySOZO Web Application is encrypted using Secure Sockets Layer (SSL)/Transport Layer Security (TLS 1.2) encryption. Raw BIS measurement data for a subject taken using the SOZO device are sent to the SOZO Tablet App which transmits the measurement data to the MySOZO Web Application.

5.0 MYSOZO

MySOZO is 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. The Database is encrypted using AES-256-bit encryption to aid in confidentiality.

MySOZO is setup with customer supplied administrator email address which triggers an email to the Customer Administrator with a one-time use token to create their credentials.
The customer administrator can then setup clinician user accounts or additional administrators, which will trigger an email to the clinician with a one-time use token used to create initial credentials.

Only customer clinician users can use SOZOapp to create patient records and direct the SOZO device to take measurements. Only customer clinician users can access patient and measurement data within SOZOapp and through the MySOZO Web Portal.

Customer administrator accounts can create and manage clinician accounts, configure security settings, configure Active Directory Integration and monitor/audit security-related events.

6.0 DATA TYPES COLLECTED

The data that is collected and stored by ImpediMed on the MySOZO Web Application Database is outlined in detail within **Appendix A** of this document. All the data falls into one of the following categories:

Data Type	Data Description	Requirements to protect data
Personally Identifiable Information (PII)	Data that can be attributed to an identifiable person. Including patient demographics (such as name, date of birth and address details) that can be used to identify a person. Protected Health Information (PHI) falls under this definition. Used to identify a patient record or for patient care purposes.	Access to data must be strictly controlled. Shared responsibility between Data Controller and Data Processor.
Patient Identifying Index	An index identifier that can be used to identify an individual. Usually a number that is often displayed with Patient Identifying Demographics and often printed out (e.g. a Medical Record Number (MRN) or other widely used hospital or national number (such as NHS number in the UK)	Access to data must be strictly controlled. Shared responsibility between Data Controller and Data Processor.
Non-patient identifiable data (non-personal data)	Data about an individual that cannot be attributed to an individual and cannot affect the persons privacy.	Can be shared under a data sharing agreement without risk of impacting subject privacy.

Data Type	Data Description	Requirements to protect data
Operational Data	Data about devices and measurements taken without any patient identifying information. This information may be used by ImpediMed to fulfill various regulatory requirements with respect to medical device post market surveillance, to better understand any failures or issues with systems and a particular client's usage and measurements taken and ultimately to improve software and to develop new product features.	No personal data or person identifying data. Can be used for software improvement without risk to privacy.

7.0 MYSOZO PORTAL PERSONALLY IDENTIFIABLE INFORMATION (PII) ELEMENTS, SOURCES AND USES

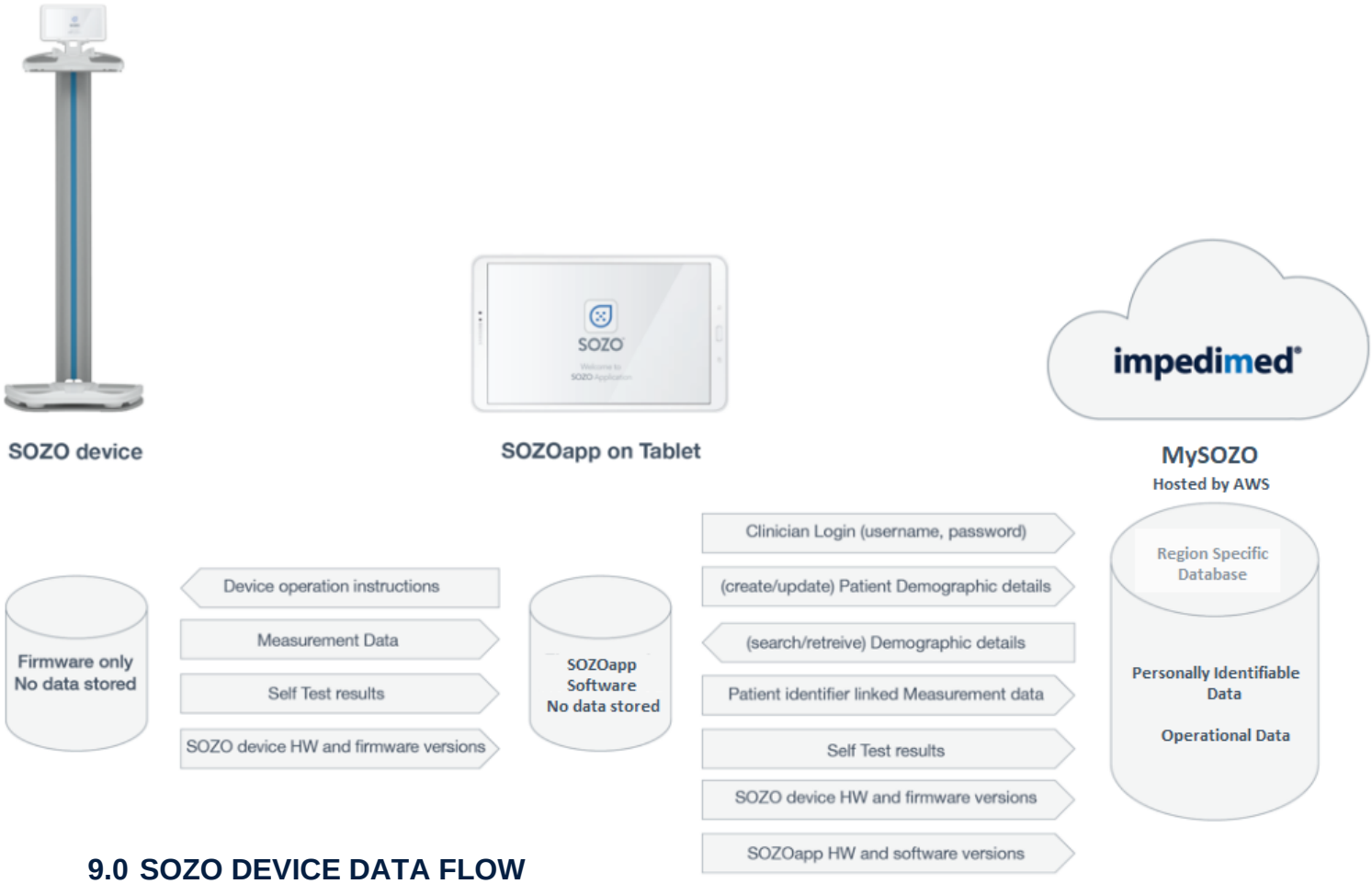
The following data set lists the data considered Personally Identifiable Information that is accessible from the MySOZO Web Portal by Clinicians and/or Clinic Administrators. ImpediMed staff do not have access to front-end visibility/access to this data.

PII Element	Source	Use
Administrator Full Name	Provided by the Clinic/End-user Administrator to ImpediMed	Required to identify Administrators at Customer locations.
Clinician Full Name	Provided by the Clinician to the Administrator	Required to identify Clinicians at Customer locations.
Country Code and Phone Number	Provided by the Clinic/End-user Administrator to ImpediMed	Used to contact administrators and clinicians by administrators and clinicians within the same organization.
Clinician Email Address	Provided by the Clinician to the Administrator	Used to send credential creation emails and report status emails.
Administrator Email Address	Provided by the Clinic/End-user Administrator to ImpediMed	Used to send credential creation emails and security report status emails.
Patient Full Name	Provided by Patient and entered into MySOZO by the Clinician	Used to identify patients by Clinicians during measurements and historical reporting.

PII Element	Source	Use
Patient Sex	Provided by Patient and entered into MySOZO by the Clinician.	Used to identify patients by Clinicians. Patient Sex is also utilized by the SOZO algorithm as a variable during the calculation of L-Dex Analysis, Fluid Analysis and Tissue Analysis.
Patient Email	Provided by Patient and entered into MySOZO by the Clinician	Used by Clinicians to contact patient as required for treatment.
Patient Country Code and Phone Number	Provided by Patient and entered into MySOZO by the Clinician	Used by Clinicians to contact patient as required for treatment.
Patient Address	Provided by Patient and entered into MySOZO by the Clinician	Used by Clinicians to contact patient as required for treatment. Used by Clinicians to identify patient.
Patient Date of Birth	Provided by Patient and entered into MySOZO by the Clinician	Date of Birth is utilized by the SOZO algorithm as a variable during the calculation of L-Dex Analysis, Fluid Analysis and Tissue Analysis.
Medical Record Number	Provided by Clinician and entered in MySOZO	Used by Clinician to identify patient and manage patient history.
Measurement Data (see Appendix A for full details)	Collected by SOZO Device from the Patient	Raw Measurement Data is utilized by the SOZO algorithm as a variable during the calculation of L-Dex Analysis, Fluid Analysis and Tissue Analysis.
Patient Biometrics (see Appendix A for full details)	Collected by SOZO Device from the Patient	Biometric Data is utilized by the SOZO algorithm as a variable during the calculation of L-Dex Analysis, Fluid Analysis and Tissue Analysis.
Assessment Date	Collected by SOZO Device when a measurement is initiated by a Clinician	Assessment date is utilized for historic measurement reports to identify trends in patient L-Dex Analysis, Fluid Analysis and Tissue Analysis.

8.0 SOZO DATA FLOWS AND STORAGE SUMMARY

The figure below outlines the data that is stored and sent between SOZO components. Detailed data content and examples of such data is outlined in Appendix A.



9.0 SOZO DEVICE DATA FLOW

Clinicians input patient demographic data into the SOZO App installed on the SOZO Android/iOS Tablet located at the customer's premises. The Patient demographic data as well as Device Operational data is transmitted to MySOZO utilizing TLS 1.2 over port 443 hosted by AWS and managed by ImpediMed. Following the entry of patient demographic information, a measurement can be initiated. The patient places their bare hands and feet on the SOZO Device, the SOZO Device then transmits the raw measurement data to the SOZOapp on the tablet over encrypted bluetooth channel. The SOZOapp on the tablet transmits the raw measurement data to MySOZO utilizing TLS 1.2 over port 443 hosted by AWS and managed by ImpediMed. The location of the MySOZO database is dependant on the region of the Clinician. Following the transmission of raw measurement data, MySOZO uses a proprietary algorithm to display L-Dex, Tissue and Fluid Analysis results to the SOZO app on the Tablet. Neither PII or Operational data is stored on the SOZO Device or SOZOApp on the Tablet.

10.0 MYSOZO WEB PORTAL DATA FLOW

Clinicians may input Patient demographic data and access measurement data from their web browsers via the MySOZO Web Portal. Patient demographic data is entered by the Clinician to the MySOZO Web Portal hosted by AWS and managed by ImpediMed. The Data is stored on the MySOZO database. Data is not stored on the Clinician workstation. MySOZO Database location is dependent on Clinician location.

11.0 MYSOZO STORAGE

Customer Region	MySOZO Database Region
United States	United States
European Union	Ireland
Asia Pacific	Australia

Detailed data content for data that is stored in the SOZO system is outlined in appendix A

12.0 FORMAL DATA ROLES AND RESPONSIBILITIES OF THE CUSTOMER AND OF IMPEDIMED

The data that is collected by the Customer and stored by ImpediMed is a shared responsibility as outlined in ImpediMed Business Associate Agreement. The customer is normally the purchaser and user of SOZO. ImpediMed does not release any information to the subject/patient directly. The customer has the direct relationship with the subject/patient and has the primary responsibility to gain the patients explicit consent of data collection, make the subject aware of the data that is collected and stored and how it is processed. In addition, the customer has the responsibility to implement appropriate administrative and technical controls to safeguard customer systems with access to sensitive subject/patient data. The customer shall be responsible for notifying the subjects/patients of data breaches, following the breach notification from ImpediMed. In this instance, the customer takes on the role and responsibility of the “Data Controller” and “Covered Entity”.

ImpediMed shall provide the software and infrastructure in which subject/patient shall be stored and transmitted to. In this instance, ImpediMed shall take the role of “Data Processor” and “Business Associate”. ImpediMed has the responsibility to implement appropriate administrative and technical controls to safeguard the confidentiality, integrity and availability of subject/patient data. ImpediMed is responsible for notifying Data Controllers/Covered Entities of data breaches, as well as notification to the appropriate governing bodies.

13.0 BUSINESS ASSOCIATE AGREEMENT

Prior to the use of the SOZO device all customers shall sign a Business Associate Agreement with ImpediMed which adheres to HIPAA and HITECH regulations. The Business Associate agreement shall address:

- Roles of the Customer and ImpediMed
- Safeguards
- Reporting
- Security Incidents
- Access to Protected Health information
- Amendments to Protected Health Information
- Accounting Disclosures
- Subpoenas, Court Orders, and Governmental Requests
- Consents and Authorizations
- Permitted Use and Disclosures
- Notice of Privacy Practices
- Compliance with the law and regulatory requirements
- Internal Practices, Books and Records
- Assurances and Audit
- Term and Termination
- Reporting of Illegal, Unauthorized or Improper Uses or Disclosures and Remedial Actions

14.0 PATIENT/SUBJECT CONSENT

ImpediMed does not maintain a direct relationship with patient/subjects, therefore it is the customer's responsibility as the Data Controller and Covered entity to acquire explicit consent from the patient/subject prior to the collection of Personally Identifiable Information (PII). Consent of data collection should include the description of the data collected, why it is processed, and where it is stored, as well as adhere to the appropriate local regulations.

15.0 DATA ACCESS AND PROCESSING

Customer - Data Controller

Data Type	Who will access/process data?	How will they access/process data?	Why will they access/process data?
Personally Identifiable Information (PII) – Patient: Weight, Height, Sex, Date of Birth, Phone Number, Address, Email, Measurement and Biometric Data	Customer Clinicians	Using the SOZOapp on the tablet, or the MySOZO Web Portal using a web browser	Clinicians will access this data to identify patients, analyze patient history, and view L-Dex, Fluid and Tissue Analysis to aid in patient care

Data Type	Who will access/process data?	How will they access/process data?	Why will they access/process data?
Patient Identifying Index- Name, Medical Record Number, Patient Number	Customer Clinicians	Using the SOZOapp on the tablet, or the MySOZO Web Portal using a web browser	Clinicians will use to identify patients
Personally Identifiable Information (PII) – Clinician & Administrator: Name, Email, Address, Country Code and Phone Number	Customer Administrators	MySOZO Web Portal using a web browser	Customer Administrators shall access data to manage Clinician accounts and monitor security related events

ImpediMed - Data Processor

Data Type	Who will access/process data?	How will they access/process data?	Why will they access/process data?
Personally Identifiable Information - ImpediMed Customer details: Name, Email, Address, Country Code and Phone Number	Automated tooling. ImpediMed Administrators and Sales	Using encrypted Email communication or MySOZO admin Web Portal	To associate operational usage data against a SOZO Device and to enable the email contact to be notified of updates or any potential issues. Additionally, to configure MySOZO back-end for new customers and trigger initial administrator account creation email
Operational Data - SOZO hardware device details and firmware/software versions.	Automated tooling. ImpediMed Administrators, Clinical and Regulatory	Using MySOZO admin Web Portal	To make appropriate firmware and software versions available to a client's SOZO systems
Operational Data – Non-person identifiable measurement types taken	ImpediMed Administrators, Clinical and Regulatory	Using AWS Back-End reporting	To analyze for usage and to provide correct billing models for clients
Non–patient identifying measurement data – See Appendix A	ImpediMed Administrators, Clinical and Regulatory	Using AWS Back-End reporting	Future hardware and software development using the non-identifiable data

Data Type	Who will access/process data?	How will they access/process data?	Why will they access/process data?
Personally Identifiable Information – Patient: Name, Age, Sex, Date of Birth, Country Code, Phone Number, Measurement Data, Biometric Data	Automated tooling. ImpediMed Technical Support Team, Clinical and Regulatory	Using MySOZO admin Web Portal	Automated tooling will store and backup this data. ImpediMed Support team utilizes data to troubleshoot customer technical issues as required, following authorization from the Covered Entity/Data Controller. ImpediMed Support team also access this data for permanent data erasure

16.0 THIRD-PARTY ACCESS

No PII data is shared with any third parties. While Amazon Web Services (AWS) hosts the physical infrastructure of MySOZO, their Policy prevents AWS personnel from accessing ImpediMed data. ImpediMed and AWS have signed a Business Associate Agreement in which AWS agrees to use appropriate administrative, physical, and technical safeguards, and comply with the applicable state law and the HIPAA Rules, including, without limitation, subpart C of title 45 of the CFR part 164, with respect to all Protected Health Information, including Electronic Protected Health Information and Electronic Personally Identifiable Information, to prevent Use or Disclosure of Protected Health Information other than as provided for by the Business Associate Agreement or Required by Law.

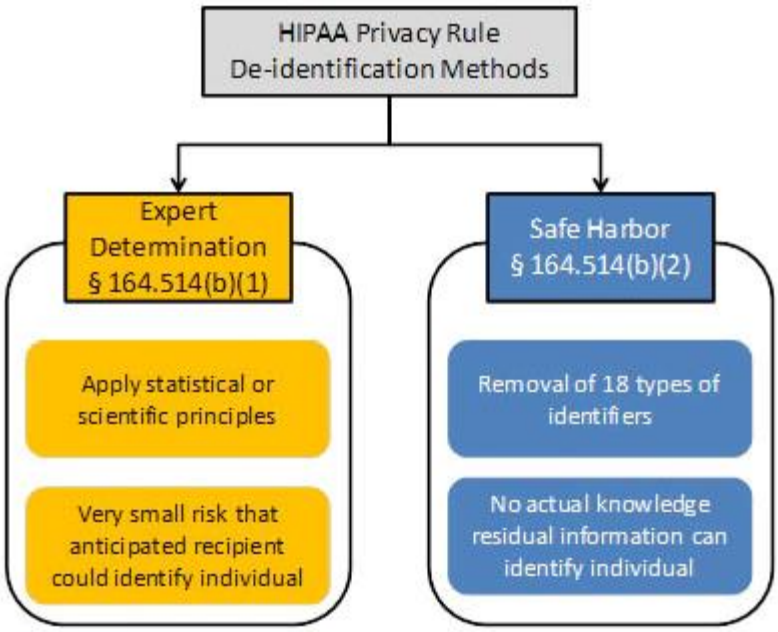
17.0 DATA USE FOR QUALITY CONTROL, SOFTWARE IMPROVEMENT AND REGULATOR REQUIREMENTS BY IMPEDIMED

ImpediMed utilizes De-Identified data and Operational data to fulfill regulatory requirements, software improvement and for Quality Control.

18.0 DETERMINING THE DATA SET IS DE-IDENTIFIED

The HIPAA Privacy Rule states that once data has been de-identified, covered entities can use or disclose it without any limitation. The information is no longer considered PHI and does not fall under the same regulations and restrictions as PHI.

De-identification under HIPAA provides two approaches for adequate de-identification:



The data that is extracted by ImpediMed utilized for Quality Controls, Software Improvement and Regulatory requirements meets the definition of Safe Harbor per §164.514(b), except for the single data type of measurement date. Because ImpediMed does retain the measurement date, ImpediMed has chosen to follow Option 1 (Expert Determination) and as defined by §164.514(b). A full report of the expert determination is available upon request, with the first pages of the report attached as Appendix C to this document. The expert that ImpediMed has chosen to complete the expert determination is dEpid/dt Consulting Inc and the qualification of the experts as well as a summary of their determination is shown in Appendix C. Based on this determination, ImpediMed fulfills the requirements listed in the HIPAA standard as the data set being **de-identified via Expert Determination**.

Patients are indexed using an identifier that is managed by MySOZO (which is inaccessible to ImpediMed or the customer). The identifier has no meaning to ImpediMed or the customer and cannot be used by either party to identify the subject of the measurement data. This patient pseudonym is not available within software user interface, printed or exportable outputs and can only be accessed by certain protected software components.

19.0 DATA SETS UTILIZED BY IMPEDIMED

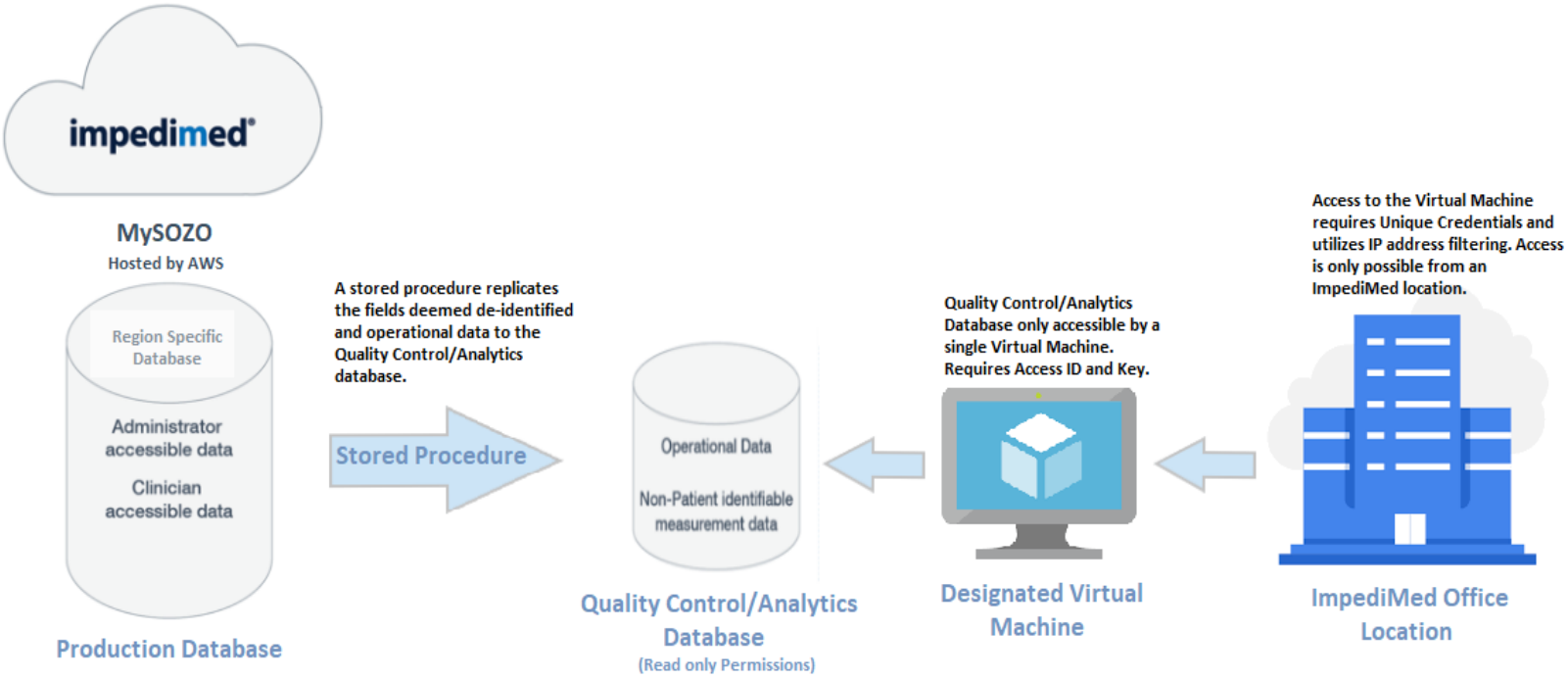
The Following table consists of the Data set utilized by ImpediMed and deemed De-Identified via Expert Determination. See Appendix A for field descriptions. See Appendix C for Expert Determination of De-identification report.

Non-Patient Identifiable Data Set	
Pseudo_id	Weight
Gender	(Body) Element Selection
Height	Risk Side Selection
Age	Limb Dominance Selection
Measurement Date	Patient country
Patient State Province	

The following table consists of the Operational Data set utilized by ImpediMed to fulfill regulatory requirements, software improvement and for Quality Control. See Appendix A for field descriptions.

Operational Data Set	
Facility ID	Utcoffset
Facility name	Time Zone
Facility country	Serial Number
Facility city	Firmware Version
Facility address	Calibration Date
Facility state province	Application Version
Facility Postal Code	SOZO Cloud Lambda Version
Assessment Type	Result ID

20.0 DATA FLOW FOR IMPEDIMED'S USE OF DE-IDENTIFIED DATA



A stored procedure on the production database is executed on a schedule and pulls values from selected fields into a region-specific separate database used for Data Analytics, Quality control and Software Improvement. The field values that are pulled into the Data Analytics Database are deemed de-identified by expert determination (See Appendix C). Statistically the fields exported to the Data Analytics database are highly unlikely to be re-identified. The size of the database also aids in the anonymization. Access to the Data Analytics database is only possible from a single Virtual Machine. A unique Access ID and Key are required to access the Quality Control Database from the Virtual Machine. Access to the Virtual Machine requires multi-factor authentication in the form of IP address filtering and Unique Credentials from an ImpediMed office. PHI data remains in the production database which is under high standard of security and privacy.

21.0 DATA RESEARCH USE

Impedimed as the Data Processor and Business Associate does not utilize patient/subject data for clinical research purposes. All research conducted by ImpediMed relates to software and hardware improvement. Only operational data and non–patient identifying measurement data (see appendix A for data details) is utilized for these purposes.

22.0 DATA ACCURACY AND SECURITY

Data Accuracy is a shared responsibility of ImpediMed and the Customer, as the Customer Clinicians collect, input and access the subject/patient's data they are responsible for verifying the accuracy of the data. ImpediMed as the Data Processor implements administrative and technical controls to ensure data is not corrupted or modified without authorization while at-rest and in-transit.
ImpediMed implements administrative and technical controls to ensure the confidentiality, integrity and availability of data based on regulatory requirements, NIST guidelines and security best practices. ImpediMed has implemented Security controls to 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)

Data is encrypted at-rest and in-transit, daily backups are performed and encrypted, Intrusion prevention systems are in-place, live-threat detection software is utilized, background checks are performed on all ImpediMed workforce members, Privacy and Security Risk Analysis are performed, and Privacy and Security Training is conducted periodically. Further information in regard to administrative and technical controls implemented by ImpediMed can be found in PM-129 SOZO Security Overview.

23.0 DATA RETENTION, DISPOSAL AND PATIENT RIGHT OF ERASURE

ImpediMed adheres to regional regulatory requirements for Data retention and Disposal such as HIPAA 45 CFR164.316 (b)(1)(2). Data stored by MySOZO is retained and disposed in accordance with ImpediMed Retention and Data Destruction policies and procedures. ImpediMed data destruction and sanitation policies adhere to NIST 800-88 guidelines.

ImpediMed and the Customer have a shared responsibility to ensure a patient/subject's right of erasure, also known as the "right to be forgotten". Following a patient/subject's written or verbal request for erasure, the customer must contact ImpediMed no later than 30 days. ImpediMed authorized support staff shall sanitize and dispose of patient/subject's data in accordance with NIST guidelines.

24.0 BREACH REPORTING

ImpediMed adheres to HIPAA's breach notification requirements found in 45 CFR Subpart D, which in turn adheres to the breach requirements of many other regional regulatory bodies. Immediate mitigation steps are taken to limit the extent of the breach. Both an Investigation and a Security Risk Analysis are launched to determine the root cause, as well identify areas in which ImpediMed can implement stronger technical and administrative controls to protect the Privacy and Security of sensitive data. Affected Business Associates and Covered entities are notified within 72 Hours. Notifications to the governing bodies adhere to their specific regional requirements. It is the Customer's responsibility to notify affected individuals following the discovery of a breach, as ImpediMed does not maintain a patient/subject relationship nor accesses contact information for patient/subjects for any purposes aside from technical support which must be authorized by the Covered Entity or Data Controller.

25.0 PRIVACY RISKS AND MITIGATIONS

Risk	Mitigation
Malicious Code	Malicious code may be found on servers, client computers, and network shared storage. To address these risks, the ImpediMed employs a suite of tools and systems to detect, remove, and block malicious code and to minimize the risk of network and user exposure. Software is designed in adherence with OWASP Principles, including coding techniques used to prevent execution of malicious code.
Hackers	To address this risk, ImpediMed implements a defense-in-depth strategy including firewalls, intrusion prevention systems and system security monitoring.
Unauthorized Access to Data (Logical and Physical Access)	To address these risks, access to information is based on the least privilege security model in which authorized administrators and users are given the smallest amount of system and data access that is necessary to accomplish their authorized tasks. Each new network user receives the most restrictive set of privileges and network access, and additional privileges and access must be authorized when appropriate. Access to ImpediMed systems is controlled, logged and monitored.
Misconfigured information asset	To address this risk, ImpediMed has deployed a strict design control program to approve and

Risk	Mitigation
	document all configuration changes made to ImpediMed software and systems.
Unapproved Sensitive PII storage	To address this risk, ImpediMed policy states that ePHI may only be stored on approved storage media, fulfilling encryption, data security and access control requirements.
Lost or misplaced backup media	To address this risk, ImpediMed encrypts all data backups, rendering misplaced backup media unreadable.
Information loss through IT asset decommissioning	To address this risk, all IT asset hard drives are sanitized before reuse or destroyed before disposal, in accordance with ImpediMed policies and procedures.
Personally Owned IT Equipment	To address this risk, no personally owned devices are allowed to access systems with PII information. Technical controls are in place to prevent and monitor access attempts.
Unapproved Sensitive PII transmission	To address this risk, ImpediMed policy requires approval prior to transmission of sensitive PII. Technical controls are in place to ensure encryption of data in transit. ImpediMed policy requires transmission of data to adhere to approved data transmission methods.

26.0 PRIVACY IMPACT ASSESSMENT CONCLUSION

ImpediMed has complied with all local regulations (HIPAA and HITech Act included) and best practices to ensure that any data that it has access to, stores or transmits, has been shared using best practice principles, is processed in an openly disclosed manner for a reasonable purpose and the data is protected for confidentiality, integrity and availability.

ImpediMed will seek to re-assess and rectify due to any new information becoming available, be this due to local requirements, changes to the SOZO system or changes to local & territorial legislation and best practice.

27.0 APPENDICES / ATTACHMENTS

Appendix A – SOZO Cloud Data
Appendix B - Regulations and Guidance Documents Considered within this report
Appendix C - Expert Determination of De-identification report

APPENDIX A – MYSOZO DATA

The data stored on the MySOZO Database may include the following, note, some of the data fields are intended for future revisions of the SW and may not actually be shared at the time of document release):

Data	Description	Data Type
Assessment Type	Type of assessment used for the measurement taken (Fluid Analysis, Tissue Analysis, L-Dex)	Operational Data
Date of measurement	Date of measurement	Personally Identifiable Information
Good/Bad result flag	Measurement quality accepted as good or marked as bad.	Operational Data
Device Serial Number	SOZO device unique serial number	Operational Data
Firmware Version	SOZO device firmware version	Operational Data
Calibration Date	SOZO device calibration date	Operational Data
SOZOapp Version	SOZOapp software version	Operational Data
SOZO Cloud Lambda Version	SOZO Cloud Lambda Version (Server-side application version)	Operational Data
Pseudonymized ID of Measurement subject	Non-subject identifying identifier (not linkable to identity). Allows numbers of measurement taken against a given subject with no knowledge of who the subject is.	Anonymous Identifier - Cannot be used by ImpediMed to re-identify subject.
Clinic Name (Facility Name)	The name of the clinic where the subject was taken. To ascertain ownership of data.	Operational Data
Facility ID	Facility ID number used to identify Clinic.	Operational Data
Clinic Address (Facility Address)	Facility Address used for operational purposes. Includes Address, State, City, Postal Code	Operational Data
Clinic Time Zone	Time Zone of the Clinic/Facility	Operational Data
Clinic Administrator and Clinician email address	The email address of the clinic administrator.	Operational Data
Clinician Administrator and Clinician Name	Clinician and Administrator's First and Last Name	Personally Identifiable Information

Data	Description	Data Type
Clinician Administrator and Clinician User ID/Credentials	Credentials utilized to access the MySOZO Web Portal	Operational Data
Patient Name	Subject Full Name	Personally Identifiable Information
Patient Email Address	Subjects Email address (optional)	Personally Identifiable Information
Patient Phone Number	Subjects Email address (optional)	Personally Identifiable Information
Medical Record Number (MRN)	A number assigned to a Subject for identification purposes	Personally Identifiable Information
Height	Subject Height	Non–patient identifying measurement data
Age	Subject Age at point of measurement recorded as year only (no day/month) for patients below 89 years of age. Patients 89 years and older are identified as such with no associated year.	Non–patient identifying measurement data
Subject Birth date	Birth date of Subject	Personally Identifiable Information
Gender	Subject Birth Sex	Non–patient identifying measurement data
Weight	Subject Weight	Non–patient identifying measurement data
Frequency	Frequency used to capture raw data	Non–patient identifying measurement data
Result ID	ID assigned to a single measurement	Non–patient identifying measurement data
Right Body R	Resistance of right body at a specific frequency	Non–patient identifying measurement data
Right Body Xc	Reactance of right body at a specific frequency	Non–patient identifying measurement data
Right Body Z	Impedance of right body at a specific frequency	Non–patient identifying measurement data
Right Body Phi	The angle in degrees for right body calculated for every frequency in combination with R and Xc	Non–patient identifying measurement data
Left Body R	Resistance of left body at a specific frequency	Non–patient identifying measurement data
Left Body Xc	Reactance of left body at a specific frequency	Non–patient identifying measurement data
Data	Description	Data Type

Left Body Z	Impedance of left body at a specific frequency	Non–patient identifying measurement data
Left Body Phi	The angle in degrees for left body calculated for every frequency in combination with R and Xc	Non–patient identifying measurement data
Right Arm R	Resistance of right arm at a specific frequency	Non–patient identifying measurement data
Right Arm Xc	Reactance of right arm at a specific frequency	Non–patient identifying measurement data
Right Arm Z	Impedance of right arm at a specific frequency	Non–patient identifying measurement data
Right Leg R	Resistance of right leg at a specific frequency	Non–patient identifying measurement data
Right Arm Phi	The angle in degrees for right arm calculated for every frequency in combination with R and Xc	Non–patient identifying measurement data
Right Leg Xc	Reactance of right leg at a specific frequency	Non–patient identifying measurement data
Right Leg Z	Impedance of right leg at a specific frequency	Non–patient identifying measurement data
Right Leg Phi	The angle in degrees for right leg calculated for every frequency in combination with R and Xc	Non–patient identifying measurement data
Left Arm R	Resistance of left arm at a specific frequency	Non–patient identifying measurement data
Left Arm Xc	Reactance of left arm at a specific frequency	Non–patient identifying measurement data
Left Arm Z	Impedance of left arm at a specific frequency	Non–patient identifying measurement data
Left Arm Phi	The angle in degrees for left arm calculated for every frequency in combination with R and Xc	Non–patient identifying measurement data
Left Leg R	Resistance of left leg at a specific frequency	Non–patient identifying measurement data
Left Leg Xc	Reactance of left leg at a specific frequency	Non–patient identifying measurement data
Left LegZ	Impedance of left leg at a specific frequency	Non–patient identifying measurement data

Data	Description	Data Type
Left Leg Phi	The angle in degrees for left leg calculated for every frequency in combination with R and Xc	Non–patient identifying measurement data
(Body) Element Selection	Used to enable Lymphedema measurement calculations	Non–patient identifying measurement data
Risk Side Selection	Used to enable Lymphedema measurement calculations	Non–patient identifying measurement data
Limb Dominance Selection	Used to enable Lymphedema measurement calculations	Non–patient identifying measurement data
Baseline L-dex	Used to enable baseline in trending	Non–patient identifying measurement data
Baseline Bilateral Right L-dex	Used to enable baseline in trending	Non–patient identifying measurement data
Baseline Bilateral Left L-dex	Used to enable baseline in trending	Non–patient identifying measurement data
Baseline ECF	Used to enable baseline in trending	Non–patient identifying measurement data
Baseline Hy-dex	Used to enable baseline in trending	Non–patient identifying measurement data
Baseline FFM	Used to enable baseline in trending	Non–patient identifying measurement data
L-Dex	Calculated measurement	Non–patient identifying measurement data
Z0	Z0 Calculation	Non–patient identifying measurement data
Whole BMR	Calculated result	Non–patient identifying measurement data
Whole BMI	Calculated result	Non–patient identifying measurement data
Whole Hy-dex	Calculated result	Non–patient identifying measurement data
Measurement Hy-dex Offset	Calculated result	Non–patient identifying measurement data
Whole Right RZero	Calculated result	Non–patient identifying measurement data
Whole Right RInf	Calculated result	Non–patient identifying measurement data
Whole Right SEE	Calculated result	Non–patient identifying measurement data
Data	Description	Data Type

WholeRightMetricProtein	Calculated result	Non–patient identifying measurement data
WholeRightMetricMinerals	Calculated result	Non–patient identifying measurement data
WholeRightMetricSMM	Calculated result	Non–patient identifying measurement data
WholeRightMetricECM	Calculated result	Non–patient identifying measurement data
WholeRightMetricBCM	Calculated result	Non–patient identifying measurement data
WholeRightMetricTBW	Calculated result	Non–patient identifying measurement data
WholeRightMetricECF	Calculated result	Non–patient identifying measurement data
WholeRightMetricICF	Calculated result	Non–patient identifying measurement data
WholeRightMetricFFM	Calculated result	Non–patient identifying measurement data
WholeRightMetricFM	Calculated result	Non–patient identifying measurement data
WholeRightR50	Whole Right R50 measurement	Non–patient identifying measurement data
WholeRightXC50	Whole Right XC50 measurement	Non–patient identifying measurement data
WholeRightPhi50	Whole Right Phi50 measurement	Non–patient identifying measurement data
WholeLeftRZero	Whole Left R0	Non–patient identifying measurement data
WholeLeftRInf	Whole left RInf	Non–patient identifying measurement data
WholeLeftSEE	Calculated result	Non–patient identifying measurement data
WholeLeftMetricProtein	Calculated result	Non–patient identifying measurement data
WholeLeftMetricMinerals	Calculated result	Non–patient identifying measurement data
WholeLeftMetricSMM	Calculated result	Non–patient identifying measurement data

Data	Description	Data Type
WholeLeftMetricECM	Calculated result	Non–patient identifying measurement data
WholeLeftMetricBCM	Calculated result	Non–patient identifying measurement data
WholeLeftMetricTBW	Calculated result	Non–patient identifying measurement data
WholeLeftMetricECF	Calculated result	Non–patient identifying measurement data
WholeLeftMetricICF	Calculated result	Non–patient identifying measurement data
WholeLeftMetricFFM	Calculated result	Non–patient identifying measurement data
WholeLeftMetricFM	Calculated result	Non–patient identifying measurement data
WholeLeftR50	Whole Left R50	Non–patient identifying measurement data
WholeLeftXC50	Whole Left XC50	Non–patient identifying measurement data
WholeLeftPhi50	Whole Left Phi50	Non–patient identifying measurement data
RightArmRZero	Right Arm R0	Non–patient identifying measurement data
RightArmRInf	Right Arm RInf	Non–patient identifying measurement data
RightArmSEE	Calculated Result	Non–patient identifying measurement data
RightArmMetricTBW	Calculated Result	Non–patient identifying measurement data
RightArmMetricECF	Calculated Result	Non–patient identifying measurement data
RightArmMetricICF	Calculated Result	Non–patient identifying measurement data
RightArmMetricFFM	Calculated Result	Non–patient identifying measurement data
RightArmR50	Right Arm R50	Non–patient identifying measurement data
RightArmXC50	Right Arm XC50	Non–patient identifying measurement data

Data	Description	Data Type
RightArmPhi50	Right Arm Xc50	Non–patient identifying measurement data
RightLegRZero	Right Leg R0	Non–patient identifying measurement data
RightLegRInf	Right Leg RInfinity	Non–patient identifying measurement data
RightLegSEE	Right Leg SEE	Non–patient identifying measurement data
RightLegMetricTBW	Calculated result	Non–patient identifying measurement data
RightLegMetricECF	Calculated result	Non–patient identifying measurement data
RightLegMetricICF	Calculated result	Non–patient identifying measurement data
RightLegMetricFFM	Calculated result	Non–patient identifying measurement data
RightLegR50	Right Leg R50	Non–patient identifying measurement data
RightLegXC50	Right Leg XC50	Non–patient identifying measurement data
RightLegPhi50	Right Leg Phi50	Non–patient identifying measurement data
LeftArmRZero	Left Arm R0	Non–patient identifying measurement data
LeftArmRInf	Left Arm RInf	Non–patient identifying measurement data
LeftArmSEE	Left Arm SEE	Non–patient identifying measurement data
LeftArmMetricTBW	Calculated Result	Non–patient identifying measurement data
LeftArmMetricECF	Calculated Result	Non–patient identifying measurement data
LeftArmMetricICF	Calculated Result	Non–patient identifying measurement data
LeftArmMetricFFM	Calculated Result	Non–patient identifying measurement data
LeftArmR50	LeftArmR50	Non–patient identifying measurement data

Data	Description	Data Type
LeftArmXC50	LeftArmXC50	Non–patient identifying measurement data
LeftArmPhi50	LeftArmPhi50	Non–patient identifying measurement data
LeftLegRZero	LeftLegRZero	Non–patient identifying measurement data
LeftLegRInf	LeftLegRInf	Non–patient identifying measurement data
LeftLegSEE	LeftLegSEE	Non–patient identifying measurement data
LeftLegMetricTBW	Calculated Result	Non–patient identifying measurement data
LeftLegMetricECF	Calculated Result	Non–patient identifying measurement data
LeftLegMetricICF	Calculated Result	Non–patient identifying measurement data
LeftLegMetricFFM	Calculated Result	Non–patient identifying measurement data
LeftLegR50	LeftLegR50	Non–patient identifying measurement data
LeftLegXC50	LeftLegXC50	Non–patient identifying measurement data
LeftLegPhi50	LeftLegPhi50	Non–patient identifying measurement data
TrunkRightRZero	TrunkRightRZero	Non–patient identifying measurement data
TrunkRightRInf	TrunkRightRInf	Non–patient identifying measurement data
TrunkRightSEE	TrunkRightSEE	Non–patient identifying measurement data
TrunkRightMetricTBW	Calculated Result	Non–patient identifying measurement data
TrunkRightMetricECF	Calculated Result	Non–patient identifying measurement data
TrunkRightMetricICF	Calculated Result	Non–patient identifying measurement data
TrunkRightMetricFFM	Calculated Result	Non–patient identifying measurement data

Data	Description	Data Type
TrunkRightR50	TrunkRightR50	Non–patient identifying measurement data
TrunkRightXC50	TrunkRightXC50	Non–patient identifying measurement data
TrunkRightPhi50	TrunkRightPhi50	Non–patient identifying measurement data
TrunkLeftRZero	TrunkLeftRZero	Non–patient identifying measurement data
TrunkLeftRInf	TrunkLeftRInf	Non–patient identifying measurement data
TrunkLeftSEE	TrunkLeftSEE	Non–patient identifying measurement data
TrunkLeftMetricTBW	Calculated Result	Non–patient identifying measurement data
TrunkLeftMetricECF	Calculated Result	Non–patient identifying measurement data
TrunkLeftMetricICF	Calculated Result	Non–patient identifying measurement data
TrunkLeftMetricFFM	Calculated Result	Non–patient identifying measurement data
TrunkLeftR50	TrunkLeftR50	Non–patient identifying measurement data
TrunkLeftXC50	TrunkLeftXC50	Non–patient identifying measurement data
TrunkLeftPhi50	TrunkLeftPhi50	Non–patient identifying measurement data

APPENDIX B - REGULATIONS AND GUIDANCE DOCUMENTS CONSIDERED WITHIN THIS REPORT

UK

- ICO guidance documents (including those covering UK Data protection Act, Freedom of Information Act). https://ico.org.uk/for-organisations/guidance-index/
- The Data Protection Act. http://www.legislation.gov.uk/ukpga/1998/29/contents
- Statutory Instrument 417/2000- The Data Protection (Processing of Sensitive Personal Data) Order 2000. http://www.legislation.gov.uk/uksi/2000/417/contents/made
- Statutory Instrument 2905/2002- The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002. http://www.legislation.gov.uk/uksi/2002/2905/contents/made

EU

- Existing EU General Data Protection Directive (directive 95/46/EC on protection of individuals with regard to the processing of personal data and on the free movement of such data). http://eur-lex.europa.eu/legal content/en/ALL/?uri=CELEX:31995L0046
- Incoming EU General Data Protection Regulations (GDPR). http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

USA

- 45 CFR part 46. HHS Regulations for the Protection of Human Subjects. https://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/index.html
- 45 CFR parts 160 and 164. Health Insurance Portability and Accountability Act (HIPAA) Regulations for Standards for Privacy of Individually Identifiable Health Information. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html
- Guidance Fair Information Privacy Principles

APPENDIX C - EXPERT DETERMINATION OF DE-IDENTIFICATION REPORT

dEpid/dt Consulting, Inc.
Statistical De-Identification Privacy Solutions

August 15, 2018

Ms. Catherine Kingsford
Senior Vice President, Medical Affairs
ImpediMed Limited
5900 Pasteur Court
Carlsbad, CA 92008

Dear Ms. Kingsford:

As you know, ImpediMed Limited (ImpediMed) has engaged my services to conduct statistical disclosure review and analyses of ImpediMed's SOZOcloud data set (with data elements as described in Appendix A, the "Data") in order to: (1) determine whether this Data could be considered "statistically de-identified" under the Expert Determination method[1] found at Section 164.514 of the HIPAA privacy rule, promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA Privacy Rule");[2] and (2) identify any statistical disclosure control conditions or assumptions which would be necessary to support the foregoing.

I. *Overview.* It is my understanding, based on information provided to me by ImpediMed, that the SOZO system is a bioimpedance monitoring device that takes patient measurements and uses the collected impedance data to provide clinicians with fluid status information to aid in the assessment of various conditions. Data are collected at client hospitals and clinics using the SOZO system and are stored in the SOZOcloud, a cloud-based database managed by ImpediMed, which collects device operational data as well as patient and provider information. While a unique ID is assigned to each SOZO system unit, a SOZOhub may have multiple units feeding data into it. Furthermore, patients having measurements taken within a hospital facility may use any of the SOZO units to have data linked to their patient profiles.

This letter includes a summary of the results of my statistical disclosure review and analyses and my Expert Determination regarding the statistical de-identification of the SOZOcloud Data. You may share this letter with any interested parties, including for purposes of providing them with information on ImpediMed's HIPAA de-identification activities or informing them of ***my Expert Determination that the proposed Data complies with the statistical de-identification provisions in Section 164.514 of the HIPAA Privacy Rule***[1]. This letter will also serve as my verification to you that (i) I am an expert possessing substantial knowledge of the theoretical, statistical and

---

1 **The term "Expert Determination"** was first introduced by the Department of Health and Human Services Office of Civil Rights in their **November 26, 2012 document "***Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule***". The implementation** specifications for this method are found at 45 CFR Section 164.514 (b)(1)(i-ii), Prior to the use of this new term, de-identification achieved in compliance with the requirements of Section 164.514 (b)(1)(i-ii) was commonly referred to as **"statistical de-identification"**.

2 Section 164.514 (b)(1)(i-**ii) of the HIPAA Privacy Rule specifies that health information is not individually identifiable if "A** person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: (i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and (ii) Documents the methods and results of the analysis **that justify such determination;"**

scientific principles and methods of statistical disclosure control, (ii) I have considerable practical experience in the application of such statistical disclosure limitations, principles and methods,[3] and (iii) that the methodology utilized in connection with this review and analyses meets the requirements of Section 164.514(b)(1) of the HIPAA Privacy Rule.

II. *Review and Analyses*. For purposes of the review and analyses and my Expert Determination contained herein, I have examined the specifications for the Data and ImpediMed's proposed holding and use of the Data under the conditions of ImpediMed's *SOP-045 Data Access Policy Rev A* de-identification policies and procedures (Appendix B) and have conducted statistical disclosure analyses to determine the potential disclosure risks associated with the foregoing. The rationale and methodological approaches used for these analyses are consistent with the Department of Health and Human Services (HHS) guidance regarding the generally accepted statistical and scientific principles and methods[4,5] to be used for statistical de-identification in compliance with the Expert Determination Method at Section 164.514 (b)(1)(i-ii). Additionally, Appendix D included with this determination provides a detailed analysis and commentary on the **HHS's rationale for acceptable risks of re**-identification in de-identified data releases. This appendix provides a detailed schema for the approaches to statistical de-identification analyses supporting Expert Determination, which I routinely employ when conducting such analyses in order to address the various statistical de-**identification issues raised in HHS's available** Expert Determination de-identification guidance.[6]

As I have discussed with ImpediMed staff, although this Data is clearly amenable to statistical de-identification under the Expert Determination method, the Data could not be considered de-identified under the HIPAA Privacy Rule pursuant to the safe harbor de-identification provision. Although the Data does not contain the vast majority of the 18 types of data elements identified in

---

[3] Professionally, my experience conducting and managing statistical disclosure limitation operations and research has spanned more than two decades, involving activities in both the healthcare information industry and in academia. I have conducted educational training and made scientific presentations on statistical disclosure limitation to persons representing state and national healthcare organizations, commercial healthcare and healthcare information companies, federal agencies, and in academia. I also have authored several peer-reviewed publications and a book chapter on statistical disclosure assessment and control. Additionally, I have performed HIPAA compliant statistical de-identification analyses and implemented disclosure control methods for several healthcare and healthcare information organizations consistent with all requirements specified in Section 164.514 (b)(1)(i-ii) of the HIPAA Privacy Rule. Appendix C of this document provides my Curriculum Vitae, which provides details on these statistical de-identification activities.

[4] Statistical Policy Working Paper 22 - Report on Statistical Disclosure Limitation Methodology (http://www.fcsm.gov/working-papers/wp22.html) (prepared by the Subcommittee on Disclosure Limitation Methodology, Federal Committee on Statistical Methodology, Office of Management and Budget), (Citation from Federal Register, December 28, 2000, Section 164.514(a)–(c)—Deidentification General Approach (pages 82708-82712)

[5] Checklist on Disclosure Potential of Proposed Data Releases (http://www.fcsm.gov/docs/checklist_799.doc) (prepared by the Confidentiality and Data Access Committee, Federal Committee on Statistical Methodology, Office of Management and Budget), (Citation from Federal Register, December 28, 2000, Section 164.514(a)–(c)—Deidentification General Approach (pages 82708-82712)

[6] a) Federal Register, December 28, 2000, Section 164.514(a)–(c)—Deidentification General Approach (pages 82708-82712); b) Federal Register, April 14, 2002 (pages 53,232 – 53,238); c) Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (Dated as September 4, 2012, as first released on November 26, 2012). In addition to the de-identification regulations and HHS Office of Civil Rights (OCR) guidance provided in Appendices D of this document, a number of other very useful HHS NIH guidance documents related to HIPAA de-identification have been reviewed and taken into account in my analyses and assessment: d) Clinical Research and the HIPAA Privacy Rule. NIH Publication Number 04-5495 February, 2004. Available at: http://privacyruleandresearch.nih.gov/pdf/clin_research.pdf. e) Health Services Research and the HIPAA Privacy Rule NIH Publication Number 05-5308 May, 2005. Available at: http://privacyruleandresearch.nih.gov/pdf/HealthServicesResearchHIPAAPrivacyRule.pdf. f) Research Repositories, Databases, and the HIPAA Privacy Rule. NIH Publication Number 04-5489 January, 2004. Available at: http://privacyruleandresearch.nih.gov/pdf/research_repositories_final.pdf.

the safe harbor at Section 164.514(b)(2)(i)[7] **of the HIPAA Privacy Rule (the "**Safe Harbor Excluded List**"), the Data does include information on dates pertaining to an individual more** specific than year (such as date of measurement) which is a data element that must be removed to satisfy such safe harbor requirements.

Additionally, this Data contains information on various **"quasi-identifier"** characteristics (e.g. birth sex and age) of the individuals in the dataset. While these quasi-identifier characteristics are not designated for exclusion by the safe harbor specifications, they could provide additional linking variables which, when used in combination, can potentially increase the risk of re-identification for individuals in the dataset through linkage with other demographic characteristics often found in reasonably available external datasets and, thus, possibly creating re-identifying links to personal identifiers such as name, address**, or other "**directly **identifying"** data elements.[8]

To confirm the potential disclosure risks associated with the quasi-identifier variables included within the Data, I have performed statistical disclosure risk analyses to assess the statistical de-identification of this data, as required by the Expert Determination method at Section 164.514 (b)(1)(i-ii) of the HIPAA Privacy Rule. As indicated in Appendix D, the risk of re-identification for an individual in the Data is dependent on: 1) The probability that the individual is unique with regard to an identifying key in the Data; 2) The probability that the individual also is listed in an external data source to be used for record linkage; 3) The probability that the individual is unique in the external data source with respect to the same identifying key; and 4) The probability that the identifying keys in both data sources are identical, given the timing, accuracy and completeness of the data in both data sources.

---

[7] The Safe Harbor provision at **Section 164.514(b)(2)(i) of the HIPAA Privacy Rule provides that: "A covered entity may** determine that health information is not individually identifiable health information only if . . . The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed: (A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000; (C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses; (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger and voice prints; (Q) Full face photographic images and any comparable images; and (R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this **section."**

[8] Per the Limited Data Set provision found at 45 CFR §165.514(e)(2)(i-xvi) **"d**irect identifiers**" include**: (i) Names; (ii) Postal address information, other than town or city, State, and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses; (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; and (xvi) Full face photographic images and any comparable images.

Furthermore, I note that the inclusion of dates of measurement does not add in an appreciable way to the re-identification risks for the Data.[9] Therefore, my statistical disclosure analyses indicate that this information does not pose disclosure risks which could be considered greater **than the "very small" c**riteria required by Section 164.514(b)(1)(i-ii) of the HIPAA Privacy Rule.

Additionally, my statistical de-identification review also considered the risks posed by the inclusion of data on the names of clinics where the SOZOhub database is installed. Based on my existing knowledge of the catchment areas associated with hospitals and clinics for the set of quasi-identifiers included in this data, it is my professional opinion that this would not pose anything more than a very small risk.

Accordingly, based on my extensive experience with statistical disclosure controls for healthcare data, this Data can be considered de-identified under the Expert Determination method for statistical de-identification at Section 164.514(b)(1)(i-ii) of the HIPAA Privacy Rule, with some additional conditions limiting the conditions of the Data release as outlined in Part III of this letter. So long as the conditions described in Part III of this letter continue to be satisfied, future deliveries of Data will also be considered statistically de-identified under the Expert Determination method.[10]

It should be noted that this Expert Determination relates solely and exclusively to HIPAA de-identification requirements and not in any manner to any state or other law that might be applicable to the information and that could impose requirements, restrictions, etc. and as to which I give no advice. It is understood that ImpediMed separately relies upon its legal counsel for HIPAA and state and other law compliance generally, including in dealing with its covered entity and business associates and others.

III. *Conditions and Assumptions*. From the HIPAA guidance which I have reviewed in **Appendix D, HHS clearly indicates that "data use" or "restricted access" agreements provide one** means of providing disclosure control by limiting who has access to the Data and by exerting contractual restrictions on what may be done with the Data. Accordingly, data released only within an organization with well-developed privacy/security policies and procedures should be viewed as having low probabilities that re-identification would ever be attempted, while, for example, data to be released without condition on the Internet should be viewed as having a potentially unlimited set of anticipated recipients who would not face the same data intrusion restrictions. Therefore, the existence of appropriate policies along with the physical, technical and procedural safeguards assuring data security and privacy are important factors in the evaluation of the risk of re-identification by the anticipated data recipients. The analyses and conclusions contained herein are based upon the existence of certain conditions, and the assumption that such

---

[9] Based upon my professional expertise and consultation with other recognized experts in HIPAA statistical de-identification practice, particularly since the implementation of the HIPAA Privacy Rule in April 2003, date of service information from **external data sources is not considered "reasonably available information". This exception for dates of service is appropriat**e because data intruders will not generally be able to reliably find dates of service in external databases along with identifying information. Because of this, dates of service will typically pose only extremely minimal re-identification risks. This is in contrast to dates of birth and dates of death which should be considered matters of public record and, therefore, readily available external information.

[10] The HIPAA Privacy Rule clearly indicates that de-**identified information is not considered to be to be "individually identi**fiable **health information" under HIPAA and, therefore, is not subject to the HIPAA Privacy Rule restrictions on uses and disclosures** of protected health information (§ 164.502). Subject to any separate agreement between the parties, de-identified information may be used in any way, provided the de-identified information is not re-identified. 64 Fed. Reg. 59918, 59946 (Nov. 3, 1999) **("In this rule we are proposing that covered entities and their business partners be permitted to use protected health inform**ation to create de-identified health information. Covered entities would be permitted to further use and disclose such de-identified information in any way, provided that they do not disclose the key or other mechanism that would enable the information to be re-**identified, …")**

conditions will be maintained such that future releases of the Data are in compliance with the requirements for Expert Determination of statistical de-identification set forth in Section 164.514(b) of the HIPAA Privacy Rule. The continued existence of these conditions is necessary to assure a well-characterized set of conditions for the Data release and the anticipated recipients of the Data. Appendix B provides ImpediMed's *SOP-045 Data Access Policy Rev A* de-identification policies and procedures which includes key provisions that help to assure that the de-identified Data will not be re-identified. Because of this, the determination contained herein that the Data will continue to meet the standards for Expert Determination of statistical de-identification in the future is predicated on the continued existence of these provisions for data holding and use:

Key Provisions from ImpediMed's *SOP-045 Data Access Policy Rev A*

9. HIPAA COMPLIANCE

General statement: ImpediMed does, in the course of its business, collect de-identified data for the purpose of customer feedback, complaint investigation, and product enhancements. All ImpediMed employees are regularly trained on HIPAA requirements. Unless covered by a Business Associate Agreement with a Covered Entity, all ImpediMed de-identified data either falls within Safe Harbor requirements, or has been established as sufficiently de-identified through the Expert Determination process. Use and review of any de-identified data sets are covered by the requirements below:

9.1 **Compliance with Any Conditions of the HIPAA De-identification Expert Determination:** ImpediMed employees shall comply with any limits, qualifications, conditions, and/or restrictions as set forth in the Expert Determination document associated with the Expert Determination De-identified Data Sets (EDDDS).

9.2 **Prohibition of Re-identification Attempts**: ImpediMed employees may not (a) re-identify, or attempt to re-identify, or allow to be re-identified, any patient(s) or individual(s) who are the subjects of the de-identified data, or (b) re-identify, or attempt to re-identify, or allow to be re-identified, any relative(s), family or household member(s) of such patient(s) or individual(s).

9.3 **Prohibition of Additional Data Linkage, Unless HIPAA De-identification Status is Maintained:** ImpediMed employees may not link any other data elements to the de-identified data without obtaining a HIPAA Expert Determination that the data remains de-identified consistent with all of the conditions imposed by 45 CFR Part 164.514(b)(1).

Before proceeding with any form of additional data linkage, consult with the Chief Privacy Officer or their delegate and obtain their written approval. Be aware that additional data linkage may require a new Expert Determination assessment.

9.4 **Data Security/Privacy Policies, Procedures and Safeguards:**

Any ImpediMed employee seeking access to EDDDS must document the following in memorandum form prior to access being granted:

- Approval from employee management
- Justification explaining the need to access the data
- Explanation for what the data will be used for
- Control measures to ensure EDDDS continues to be held under ImpediMed control.
- Express statement that de-identified data sets will remain de-identified and not be used to re-identify in accordance with 45 CFR Part 164.514(b)(1).

A fully completed copy of any access requests will be maintained by the Chief Privacy Officer.

As confirmed by the letter signed by Shashi Tripathi, Chief Technology Officer (see Appendix B), it is also our understanding that this data will not be used by or disclosed to any parties outside of the ImpediMed work force. Therefore, the ongoing Expert Determination of the Data as meeting the requirements for statistically de-identified data assumes that ImpediMed will maintain and enforce such general agreements with the anticipated data recipients, as necessary for ImpediMed and their clients to comply with the foregoing conditions and assumptions.

Additionally, because of the contextual considerations that should be accounted for in an Expert Determination of re-identification risks, it is recommended that ImpediMed make an annual re-assessment as to whether there have been any substantive changes in: 1) the external data environment, 2) the regulatory definition for the Expert Determination method for statistical de-identification, 3) the availability of technologies that importantly facilitate the conduct of re-identification attacks, 4) the data elements contained in this Data stream, and 5) the de-identification policies, procedures and practices that are used to manage and control re-identification risks for this Data. Such annual assessments are important because they recognize the fact that de-identification status cannot be a static determination within a changing external **environment of "reasonably available" data which cou**ld be used in data intrusion attempts. Finally, so as to confirm that the conclusions of these de-identification determination analyses supporting these findings will still hold in the future and have not been altered by important changes in demographic characteristics that constitute the quasi-identifier variable sets, it is recommended that re-analysis for statistical disclosure risks be performed every three years, so long as the Data is still being used and released.

IV. *Conclusion*. So long as (a) the Data to be released is limited to only those data elements set forth in Appendix A; and (b) the general conditions and assumptions set forth in Part III hereof remain satisfied, it is my professional finding that the risk is very small that the Data to be released could be used, alone or in connection with other reasonably available information by the anticipated recipients, to identify an individual who is a subject of such data, and accordingly it is my opinion that the Data meets the requirements for Expert Determination of statistical de-identification as set forth in Section 164.514 of the HIPAA Privacy Rule, thereby satisfying the conditions set forth in Sections 164.514 (a)-(b)(1) of the HIPAA Privacy Rule.[11]

This Expert Determination remains effective until August 15, 2021, unless there are any substantive changes in the external data environment, changes in regulatory definition of Expert Determination of statistical de-identification, changes in the availability of technologies that importantly facilitate the conduct of re-identification attacks, changes in the data elements contained in this Data stream, or changes to the de-identification policies, procedures and

[11] For purpose of clarification and avoidance of doubt, the dEpid/dt Consulting provided services described in this determination letter should be understood to support only the HIPAA Expert Determination of De-identification provided above. Neither attention to, nor analysis with respect to any other law, including but not limited to federal law or the law of any state, territory, local, foreign, or other jurisdiction, was a part of these dEpid/dt Consulting services or implied by the HIPAA Expert Determination provided here.

practices that are used to manage and control re-identification risks for this Data in which case a new evaluation of statistical de-identification will be required. Continued annual reviews of these considerations will be a part of this ongoing Expert Determination de-identification process.

dEpid/dt Consulting Inc.,

By: 

Daniel C. Barth-Jones, M.P.H., Ph.D.
President, dEpid/dt Consulting, Inc.
and
Assistant Professor of Clinical Epidemiology
Department of Epidemiology
Mailman School of Public Health
Columbia University

cc: Reuben Lawson, Senior Director, Regulatory Affairs & Clinical