HITRUST

6175 Main Street
Suite 400
Frisco, TX 75034

Letter of HITRUST Risk-based, 2-year (r2) Certification

October 18, 2024

ImpediMed, Inc.
5900 Pasteur Court
Suite 125
Carlsbad, California 92008-7334

HITRUST has developed the HITRUST CSF, a certifiable security and privacy framework which incorporates information protection requirements based on input from leading organizations. HITRUST identified a subset of the HITRUST CSF requirements that an organization must meet to be HITRUST Risk-based, 2-year (r2) Certified for a defined assessment scope. ImpediMed, Inc. ("the Organization") has chosen to perform a HITRUST CSF v9.6.2 r2 validated assessment utilizing a HITRUST Authorized External Assessor Organization ("External Assessor").

Scope

The following platforms of the Organization were included within the scope of this assessment ("Scope") which included a review of the referenced facilities and supporting infrastructure for the applicable information protection requirements:

Platforms:

- Microsoft Office365 residing at Microsoft Data Center
- MySOZO SaaS Application residing at Amazon Web Services

Facilities:

- Amazon Web Services (APAC) (Data Center) managed by Amazon Web Services located in Sydney, Australia
- Amazon Web Services (EU) (Data Center) managed by Amazon Web Services located in Dublin, Ireland
- Amazon Web Services (US) (Data Center) managed by Amazon Web Services located in Ashburn, Virginia, United States of America
- Microsoft Data Center (Data Center) managed by Microsoft located in Redmond, Washington, United States of America

Certification

The Organization has met the criteria specified as part of the HITRUST Assurance Program to obtain a HITRUST r2 validated assessment report with certification ("Certification") for the

Scope. Certification is awarded based on each domain's average maturity score meeting a minimum score. Within each domain the maturity scores for each requirement statement were validated by an External Assessor and the assessment was subjected to quality assurance procedures performed by HITRUST.

The Certification for the Scope is valid for a period of two years from the date of this letter assuming the following occurs. If any of these criteria are not met, HITRUST will perform an investigation to determine ongoing validity of the certification and reserves the right to revoke the Organization's certification.

- No security events resulting in unauthorized access to the assessed environment or data housed therein, including any data security breaches occurring within or affecting the assessed environment reportable to a federal or state agency by law or regulation

- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the HITRUST r2 certification criteria specified as part of the HITRUST Assurance Program.

Users of this letter can contact HITRUST customer support (*support@hitrustalliance.net)* for questions on using this letter.

The Organization's Assertions

Management of the Organization has provided the following assertions to HITRUST:

- The Organization has acknowledged that, as members of management, they are responsible for the information protection controls implemented as required by the HITRUST.

- The Organization has implemented the information protection controls as described within their assessment.

- The Organization maintains the information security management program via monitoring, review, and periodic re-assessments of the information protection controls.

- The Organization has responded honestly, accurately, and completely to inquiries made throughout the assessment process and certification lifecycle.

- The Organization has provided the External Assessor with accurate and complete records and necessary documentation related to the information protection controls included within the scope of its assessment.

- The Organization has disclosed all design and operating deficiencies in its information protection controls of which is it aware throughout the assessment process, including those where it believes the cost of corrective action may exceed the benefits.

- No events or transactions have occurred or are pending that would have an effect on the assessment that was performed and used as a basis by HITRUST for issuing the report.

- There have been no communications from regulatory agencies concerning noncompliance with or deficiencies regarding the information protection controls that are included within the Scope of this assessment.

External Assessor Responsibilities

External Assessors are authorized by HITRUST based upon a thorough vetting process to demonstrate their ability to perform HITRUST CSF assessments, and individual practitioners are required to maintain appropriate credentials based upon their role on HITRUST assessments. In HITRUST r2 validated assessments the External Assessor is responsible for:

- Reviewing and gaining a detailed understanding of the information provided by the Organization.

- Performing sufficient procedures to validate the control maturity scores provided by the Organization.

- Meeting all HITRUST Assessment criteria described within the HITRUST Assessment Handbook.

HITRUST Responsibilities

HITRUST is responsible for maintenance of the HITRUST CSF and HITRUST Assurance Program against which the Organization and an External Assessor completed this assessment.

HITRUST performed a quality assurance review of this assessment to support that the control maturity scores were consistent with the results of testing performed by the External Assessor. HITRUST's quality assurance review incorporated a risk-based approach to substantiate the External Assessor's procedures were performed in accordance with the requirements of the HITRUST Assurance Program.

A full HITRUST Validated Assessment Report has also been issued by HITRUST which can also be requested from the organization listed above directly. Additional information on the HITRUST Assurance Program can be found at the HITRUST website (*https://hitrustalliance.net).*

Limitations of Assurance

The HITRUST Assurance Program is intended to gather and report information in an efficient and effective manner. The assessment is not a substitute for a comprehensive risk management program but is a critical data point in risk analysis. The assessment should also not be a substitute for management oversight and decision-making but, again, leveraged as a key input.

HITRUST

HITRUST

Enclosures (2):

- Assessment Context
- Scope of Systems in the Assessment

Assessment Context

About the HITRUST r2 Assessment and Certification

The HITRUST r2 assessment provides the highest level of information protection and compliance assurance. It is the most comprehensive and robust HITRUST certification, and can be optionally tailored to include coverage for additional authoritative sources such as HIPAA, the NIST Cybersecurity Framework, and GDPR.

The HITRUST r2 assessment is an evolving, threat-adaptive assessment with an accompanying certification. HITRUST r2 assessments leverage threat intelligence data and best practice controls to deliver an assessment that addresses relevant practices and active cyber threats. To do this, HITRUST continually evaluates cybersecurity controls to identify those relevant to mitigating known risks using cyber threat intelligence data from leading threat intelligence providers. Therefore, the HITRUST r2 includes controls that exclusively address emerging cyber threats actively being targeted today.

Assessment Approach

An *Authorized HITRUST External Assessor Organization* (the "External Assessor") performed validation procedures to measure the control maturity of the HITRUST CSF requirements and corresponding evaluative elements included in this assessment for the scope of the assessment. These validation procedures were designed by the External Assessor based upon the assessment's scope in observance of HITRUST's CSF Assurance Program Requirements and consisted of inquiry with key personnel, inspection of evidence (e.g. access lists, logs, configuration, sample items, policies, procedures, diagrams), on-site or virtual observations, (optionally) utilization of the work of others (as described elsewhere in this report), and (optionally) reperformance of controls.

Each requirement in the HITRUST CSF contains one or more evaluative elements. For example, requirement 0322.09u2Organizational.12, which reads "Media is encrypted when onsite unless physical security can be guaranteed, and always when offsite.", contains the following two evaluative elements: "1. The organization restricts the use of writable, removable media in organizational systems" and "2. The organization restricts the use of personally owned, removable media in organizational systems". The implementation and operation of all evaluative elements associated with applicable HITRUST CSF requirements included in the assessment was evaluated by the External Assessor in reaching an implementation score.

Implementation Score	Description	Points Awarded
Not compliant- (NC)	Very few if any of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment. Rough numeric equivalent of 0% (point estimate) or 0% to 10% (interval estimate).	0
Somewhat complaint (SC)	Some of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 25% (point estimate) or 11% to 32% (interval estimate).	25
Partially compliant (PC)	About half of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 50% (point estimate) or 33% to 65% (interval estimate).	50
Mostly compliant (MC)	Many but not all of the evaluative elements in HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 75% (point estimate) or 66% to 89% (interval estimate).	75
Fully compliant (FC)	Most if not all of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 100% (point estimate) or 90% to 100% (interval estimate).	100

Risk Factors

The assessed entity completed the following tailoring questionnaire to derive this assessment's customized set of HITRUST CSF requirements based on organizational, geographical, technical, and regulatory risk factors.

Assessment Type	
HITRUST Risk-based, 2-year (r2) Security Assessment	
General Risk Factors	
Organization Type	Service Provider (Non-IT)
Entity Type	Healthcare - Business Associate
Geographic Risk Factors	

Geographic Scope of Operations Considered	Multi-State
Organizational Risk Factors	
Number of Records that are currently held	Less than 10 Million Records
Technical Risk Factors	
Is the system(s) accessible from the Internet?	Yes
Is the scoped system(s) (on-premise or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)?	Yes
Does the system(s) transmit or receive data with a third-party?	Yes
Is the system(s) publicly positioned?	No - The SOZO System is not publicly positioned. It is only accessible by Clinicians and authorized personnel at the customer facilities.
Number of interfaces to other systems	Fewer than 25
Number of users of the system(s)	Fewer than 500
Number of transactions per day	Fewer than 6,750
Does the scoped environment allow dial-up/dial-in capabilities (i.e., functional analog modems)?	No - Dial-up/Dial-in capabilities are restricted and equipment is not present.
Is scoped information sent and/or received via fax machine (i.e., an actual machine, excluding efax or scan to email)?	No - Fax capabilities are restricted and equipment is not present.
Do any of the organization's personnel travel to locations the organization deems to be of significant risk?	No - High Risk locations are not a part of ImpediMed's consumer base, and we do not offer services to these high-risk locations.
Are hardware tokens used as an authentication method within the scoped environment?	No - Hardware tokens are not utilized.
Does the organization allow personally owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)?	No - BYOD Devices are restricted from accessing the in-scope environment.
Are wireless access points in place at any of the organization's in-scope facilities?	No - Wireless Access Points are not utilized for the in-scope environment.
Does the organization use any part of the scoped systems, system components, or system services to sell goods and/or services?	No - Scoped environments are not utilized for eCommerce.
Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES)?	No - Electronic Signatures are not utilized in the context of in-scope services.

Is scoped information sent by the organization using courier services, internal mail services, or external mail services (e.g., USPS)?	No - Physical Mail services are not utilized for the in-scope services of MySOZO/SOZO.
Is any aspect of the scoped environment hosted on the cloud?	Yes
Does the system allow users to access the scoped environment from an external network that is not controlled by the organization?	Yes
Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component?	Yes
Compliance Factors (Optional)	
HIPAA Security Rule	

Scope of the Assessment

Company Background

ImpediMed is the world leader in the development and distribution of medical devices employing Bio-impedance Spectroscopy (BIS) technologies for use in the non-invasive clinical assessment and monitoring of fluid status. ImpediMed's primary product range consists of a number of medical devices that aid surgeons, oncologists, therapists and radiation oncologists in the clinical assessment of patients for the potential onset of secondary lymphoedema. Pre-operative clinical assessment in cancer survivors, before the onset of symptoms, may prevent the condition from becoming a lifelong management issue and thus improve the quality of life of the cancer survivor. ImpediMed had the first medical device with an FDA clearance in the United States to aid health care professionals in the clinical assessment of secondary lymphoedema of the arm and leg in female and male cancer patients.

In-scope Platforms

The following tables describe the platforms that were included in the scope of this assessment.

Microsoft Office365	
Description	Microsoft Office365 is a cloud platform utilized for Internal User management, Email services, Logging, Document Storage, and Productivity Applications.
Application(s)	Office365 Suite, SharePoint, Outlook, Microsoft Security and Compliance Center
Database Type(s)	Azure SQL
Operating System(s)	N/A "“ Microsoft Office365 is a cloud-based SaaS provider.
Residing Facilities	Microsoft Data Center

MySOZO SaaS Application	
Description	The Primary system in scope is the SOZO Medical Device's MySOZO SaaS Application. MySOZO Web Application is hosted on AWS physical infrastructure. The SOZO Device connects to the MySOZO Web Application utilizing the SOZO Tablet Application which comes pre-installed on the SOZO Tablet. MySOZO utilizes a "Server-less" platform. It is supported by a group of services provided by AWS. The AWS services supporting the MySOZO Web Application include CloudFront, AWS Shield, CloudWatch, AWS KMS, AWS Cognito, AWS IAM, AWS VPC, AWS Lambda, AWS CloudTrail, S3, and Aurora Database. The MySOZO Web Application is the storage and processing location of the measurements/data recorded by the SOZO Device. End-Users (Clinicians and Customer Administrators) can access the MySOZO Web Portal to create patients, review patient history, run historical assessment reports, user management, configure security settings and run audit reports for their tenant. ePHI is stored on the MySOZO Web Application including: Patient Name, MRN, D.O.B, Weight, Height, Sex, Measurement Data, Phone (optional) and address (optional).
Application(s)	AWS CloudFront, AWS Shield, CloudWatch, AWS KMS, AWS Cognito, AWS IAM, AWS VPC, AWS Lambda, AWS CloudTrail, S3, and Aurora Database. Node.Js, SQL
Database Type(s)	RDS
Operating System(s)	AWS Microservice based platform
Residing Facilities	Amazon Web Services (US)

In-scope Facilities

The following table presents the facilities that were included in the scope of this assessment.

Facility Name	Type of Facility	Third-party Managed?	Third-party Provider	City	State	Country
Amazon Web Services (US)	Data Center	Yes	Amazon Web Services	Ashburn	Virginia	United States of America

Facility Name	Type of Facility	Third-party Managed?	Third-party Provider	City	State	Country
Microsoft Data Center	Data Center	Yes	Microsoft	Redmond	Washington	United States of America
Amazon Web Services (APAC)	Data Center	Yes	Amazon Web Services	Sydney		Australia
Amazon Web Services (EU)	Data Center	Yes	Amazon Web Services	Dublin		Ireland

Services Outsourced

The following table presents the outsourced services relevant to the scope of this assessment. The "Consideration in this Assessment" column of this table specifies the method utilized for each service provider relevant to the scope of this r2 assessment. HITRUST requires the inclusive method must be used on HITRUST r2 validated assessments. Under the Inclusive method, HITRUST CSF requirements performed by the service provider are included within the scope of the assessment and addressed through full or partial inheritance, reliance on third-party assurance reports, and/or direct testing by the External Assessor.

Third-party Provider	Relevant Service(s) Provided	Consideration in this Assessment
Amazon Web Services	Impedimed's MySOZO SaaS Application is hosted on AWS infrastructure in a "Server-less" platform architecture. AWS services utilized for the MySOZO Web Application include CloudFront, AWS Shield, CloudWatch, AWS KMS, AWS Cognito, AWS IAM, AWS VPC, AWS Lambda, AWS CloudTrail, S3, and Aurora Database. As the infrastructure provider, AWS holds responsibilities for physical security, environmental safeguards, hardware maintenance, data center redundancy, and disaster recovery infrastructure testing across global availability zones. AWS is also responsible for hardware-level encryption, network-level protection (DDoS mitigation via AWS Shield), and platform integrity.	Included

Third-party Provider	Relevant Service(s) Provided	Consideration in this Assessment
Microsoft	Microsoft provides a cloud-based platform for internal productivity, user management, and data storage. Office 365 services utilized include Exchange Online, SharePoint, Outlook, Microsoft Security and Compliance Center. Microsoft Azure is utilized for Identity Services and logging. As the cloud provider, Microsoft holds responsibilities for physical security, environmental safeguards, hardware maintenance, and redundancy within its global data centers. Microsoft ensures the availability of core platform services, including disaster recovery testing, fault-tolerant infrastructure, and data redundancy across multiple Azure regions and Office 365 availability zones. Microsoft is also responsible for platform-level encryption for data at rest and in transit and integrated tools to protect against network threats, such as DDoS attacks.	Included