



iShare Medical
HISP Practices Statement
July 3, 2026

Introduction

1.1 Overview

This document is the iShare Medical HISP Practices Statement (HPS) that states the policies and practices of iShare Medical Health Information Services Provider (HISP) as it performs secure encrypted exchange of electronic medical records and other healthcare related transactions compliant with DirectTrust HISP Policy.

This DirectTrust HP follows the general structure of the Internet Engineering Task Force (IETF) Internet X.509 Public Key Infrastructure (PKI) Certificate Policy and Certification Practices Framework ([RFC 3647](#)). This HISP Practices Statement diverges from that framework where required to include additional unique aspects of HISP operations and Direct messaging for the secure transport of health information over the Internet.

1.1.1 Relationship between this DirectTrust HP and a Corresponding HPS

This HPS documents a summary of how iShare Medical complies with HISP Policy (HP).

1.1.2 Relationship between this DirectTrust HP and the DirectTrust CP

As a HISP, iShare Medical creates Direct Addresses. These addresses are bound to the digital identity of the entity as well as two key pairs, each pair bound to an X.509 Certificate, one of which is for encryption/decryption of the data and the other of which is used for the digital signature of the transaction. The DirectTrust Certificate Policy (CP) describes policies that the Certificate Authority must adhere to relating to issuance and management of X.509 certificates for use in Direct messaging applications. These policies and practices flow to iShare Medical when creating, maintaining, and protecting the Direct Addresses.

1.1.3 Relationship between this DirectTrust HP and the DirectTrust Accreditation program

iShare Medical is a DirectTrust Accredited Trust Anchor HISP that complies with HP. This document explains how iShare Medical complies with these requirements; however, this attestation is not a substitute for Accreditation. Accreditation involves an intensive review and audit of HISP policies, procedures, and practices.

1.2 Document Name and Identification

This DirectTrust HP is assigned a unique object identifier (OID). The DirectTrust set of policy OIDs are registered under an arc of its assigned organizational identifier as registered in the ISO/ITU OID Registry.

iShare Medical complies with DirectTrust HP Version 2.0.3 which supersedes all previous HP versions.

1.3 PKI Participant

The following are roles relevant to the administration and operation of the Public Key Infrastructure (PKI) within which a conforming HISP operates to provide Direct messaging services.

1.3.1 PKI Authorities

1.3.1.1 DirectTrust

DirectTrust is a non-profit, competitively neutral, self-regulatory entity operated by and for participants in the Direct community. DirectTrust has developed and maintains a security and trust framework and operates as a policy authority responsible for this HP and for the DirectTrust CP, related policy and practice statements, and for overseeing the conformance of HISP practices with this HP through the DirectTrust HISP Accreditation program. DirectTrust is also a standards development organization and, since 2019, has acted as maintainer of the Applicability Statement for Secure Health Transport and the related documents.

1.3.1.2 Certification Authorities (CAs)

A certification authority (CA) in this context is an entity that signs certificate signing requests (CSRs) and issues public key X.509 certificates to Direct exchange or Direct Project organizational or individual Subscribers. Policies governing CA services are found in the DirectTrust CP. iShare Medical uses a third party DirectTrust Accredited CA for creation of its Certificates.

1.3.1.3 Registration Authorities (RAs)

Registration Authorities (RA) operate identity management systems (IdMs) and collect and verify Subscriber information on the Issuer CA's behalf. RAs collect and verify identity information from Direct Subscribers using procedures that implement the identity validation policies set forth in the DirectTrust CP. Policies governing RA services are found in the DirectTrust CP. iShare Medical uses a third party DirectTrust Accredited RA for identity proofing and identity verification.

1.3.2 End Users

An End User is a person or device that uses the iShare Medical HISP solution to support Direct Secure Messaging transactions and communications. End Users are not always the party identified in a Certificate, such as when Group Certificates are issued to an organization for use by its End Users. All End Users are Subscribers of Direct X.509 Certificates, as defined in the DirectTrust Certificate Policy, but not all Subscribers are End Users. iShare Medical issues Direct Addresses to entities and individuals such as providers, payers, devices, and business associates of covered entities that have a HIPAA compliant right to create, read, update, or share medical records.

1.3.3 Health Information Services Providers (HISPs)

iShare Medical is a DirectTrust Accredited Trust Anchor HISP that provides Secure Direct Messaging services to and from known identity proofed Direct Addresses (electronic endpoints point to the real identity of the owner) in accordance with the Direct Project Applicability Statement (i.e. provides “Direct Services”). iShare Medical holds and manages the PKI private keys with the Direct Digital Certificate on behalf of the Subscriber. Private Keys are created using a Hardware Security Module (HSM) and are stored, encrypted by a wrapping key that resides only on the HSM and a duplicate of the HSM, on servers in iShare’s datacenter environment. Direct Message signing and decryption operations are performed on an HSM. Further, the primary HSM and its duplicate are in geographically distinct datacenters.

1.3.3.1 HISP Boundary Considerations

The “HISP boundary” defines the iShare Medical HISP in order to specify the clear logical and/or physical borders where the HISP ends and other organizational functions and responsibilities begin. The following items are a list of functions that are under iShare Medical’s control and are subject to the HISP Policy:

- Perform Security/Trust Agent (STA) functions (decrypt inbound messages, validate counterparty signature including message digest, ensure outbound messages are properly signed, encrypt outbound messages, send/receive MDNs to confirm receipt or final delivery of message) [section 6.9.4]
- Perform trust management functions such as maintaining trust anchor store and trust policy enablement [section 6.9.3]
- Perform Certificate discovery functions [section 6.9.4]
- Provide S/MIME inbound and outbound interfaces [section 6.9.4] to receive messages sent to End User Direct Addresses and transmit messages sent from End User Direct Addresses
- Provide HISP-side of edge protocol connection including webmail or integration interfaces, or internal API or data sharing repository for unified software with integrated HISP [section 6.7.1]
- Maintain End User private key store for decryption of inbound messages [section 6.2]
- Perform End User authentication (but can be tiered on authentication by EHR technology or dependent application) [section 6.7.1]
- Maintain integrity of security and trust framework, includes review of security logs.
- Maintain privacy of electronic Protected Health Information (ePHI) [section 6.7.1, 6.9.2]
- Perform HISP Information Systems Security Officer (ISSO) functions [section 6.2]
- Maintain End User signing private key store, and/or provide interface for Hardware- based signing keys held by End User

- Provision Direct Addresses
- Generate End User private keys [section 6.1.1]
- Operate SMTP inbound or outbound server
- Operate POP/IMAP server
- Operate DNS servers hosting End User certificates for discovery
- Maintain End User message queues and/or mailboxes
- Provide Tools or interfaces to create a message and include attachments
- Provide End User technical support
- Operate Provider Directory

1.3.4 Counterparties

A Counterparty is either an end entity that either:

- i) receives a Direct message sent by an iShare Medical HISP's End User, or
- ii) sends a Direct message to an iShare Medical End User.

If an iShare Medical HISP's End User is the sender of a Direct message, then the recipient is the Counterparty. If an iShare Medical HISP's End User is the recipient of a Direct message, then the sender is the Counterparty. A Counterparty uses the public key in an End User's X.509 certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the End User.

1.3.5 Counterparty HISP

A Counterparty HISP is the entity providing HISP services to a Counterparty. The Counterparty HISP may be a different HISP than that used by the End User.

1.3.6 Intermediate System

An Intermediate System is a healthcare application or other system outside the HISP boundary that communicates using the iShare Medical HISP to send and receive Direct Messages on behalf of its End Users via the iShare Medical RESTful Application Program Interface (API).

An Intermediate System may communicate directly with a HISP or two or more Intermediate Systems may form a chain of communication between the End User and the HISP. The Intermediate System communicates with a HISP or another Intermediate System to send and/or receive Direct messages on behalf of End Users using an edge protocol supported by both systems. Some examples of Intermediate Systems include Electronic Health Record (EHR) technologies, Personal Health Record (PHR) technologies, and Patient Portal systems.

When a single application includes components both inside and outside the HISP Boundary, such as an EHR technology with an integrated HISP, the portion of the application outside the HISP Boundary is an Intermediate System.

1.3.7 Affiliated Organization

An Affiliated Organization is an entity that authorizes organizational affiliation with the Subscriber of a Certificate (note that this definition is from DirectTrust Certificate Policy, v2.1).

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The primary anticipated use for a DirectTrust Community X.509 certificate is in the exchange of electronic messages grounded in the specifications of the Direct Project. This includes S/MIME message signature verification and S/MIME message encryption. A iShare Medical HISP uses Certificates issued under the DirectTrust CP only for purposes permitted by the DirectTrust CP.

1.4.2 Prohibited Certificate Uses

The iShare Medical HISP does not use Certificates and private keys issued under the DirectTrust CP for any purpose prohibited by the DirectTrust CP.

1.5 Policy Administration

1.5.1 Organization Administering the Document

iShare Medical
107 West 63rd Street, Suite 248
Kansas City, Missouri 64113

1.5.2 Contact Person

Lind M. Van Horn, Owner/CEO
iShare Medical
107 West 63rd Street, Suite 248
Kansas City, Missouri 64113

Phone: 816.249.2555
email: info@isharemedical.com
web: [https:// www.sharemedical.com](https://www.sharemedical.com)

1.5.3 Person Determining HISP Practices Statement Suitability for the Policy

A HPS states how iShare Medical implements the policies required by this HISP Policy. iShare Medical approves the content of this HPS and its compliance with DirectTrust HISP Policy.

iShare Medical is a DirectTrust Accredited Trust Anchor HISP and has been since 2015. This means that iShare Medical has successfully completed the DirectTrust Accreditation program and deemed to be Accredited. This attestation is asserted by the following.

Lind M. Van Horn, Owner/CEO
iShare Medical
107 West 63rd Street, Suite 248
Kansas City, Missouri 64113

Phone: 816.249.2555
email: info@isharemedical.com
web: [https:// www.sharemedical.com](https://www.sharemedical.com)

1.5.4 HISP Practices Statement Approval Procedures

This HPS can be updated at any time. The HPS is reviewed at least annually.

1.6 Definitions and Acronyms

1.6.1 Acronyms

Acronym	Meaning
API	Application Programming Interface
ASTP	Assistant Security for Technology Policy
CA	Certification Authority
CP	Certificate Policy
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DNS	Domain Name Server
EHR	Electronic Health Record
HISP	Health Information Services Provider or Health Information Service
HPS	HISP Practices Statement
ID	Identity
IETF	Internet Engineering Task Force
ISO/ITU	International Organization for Standardization/International Telecommunication Union
ISSO	Information Systems Security Officer
LDAP	Lightweight Directory Access Protocol
MDN	Message Delivery Notification
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
ONC	Office of the National Coordinator for Health Information Technology

PHI	Protected Health Information
PKI	Public Key Infrastructure
RA	Registration Authority
RESTful	Representational State Transfer
RFC	Request for Comments
S/MIME	Secure Multipurpose Internet Mail Extensions

1.6.2 Definitions

Term	Definition
Accreditation	Accreditation of a HISP through the program operated by DirectTrust.
Applicability Statement	The Applicability Statement for Secure Health Transport, Version 1.2, dated August 3, 2015, or any subsequent version, published by DirectTrust.
Application Programming Interface	Specifies how software components should interact via a programmatic service contract between one or more components.
Business Associate	An entity meeting the definition of a business associate under HIPAA at 45 CFR 160.103.
Certificate	A digital representation of information which at least: (1) identifies the Certification Authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the Certification Authority.
Certification Authority	An authority trusted by one or more users to create and assign
Certificate Policy	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during Certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital Certificates.
Certificate Practice Statement	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing Certificates and providing access to them, in accordance with specific requirements typically provided in a Certificate Policy.
Certificate Revocation List	A list maintained by a Certification Authority identifying the Certificates that it has issued that are revoked prior to their stated expiration date.
Confidential	Has the meaning set forth in § 9.3.1.

Information	
Counterparty	The end entity on the other side of a Direct transaction with an
Counterparty HISP	The HISP used by a Counterparty. This may be a different HISP
Covered Entity	An entity meeting the definition of a covered entity under HIPAA at 45 CFR § 160.103.
Delivery Notification IG	Unless otherwise stated, means the then current version of the Implementation Guide for Delivery Notification in
Direct Message	An electronic mail message digitally signed and encrypted according to the requirements of the Applicability Statement.
Direct Project	An initiative from the Office of the National Coordinator (ONC) for Health Information Technology that created a set of standards and services that, with a policy framework, enables simple, routed, scalable, and secure message transport over the Internet between known participants.
DirectTrust CP	The current versions of the DirectTrust Certificate Policy, as further defined in § 1.1.2.
Distinguished Name	A term that describes the identifying name in a Certificate, which becomes part of the Certificate itself.
Electronic PHI	Has the meaning given to <i>Electronic Protected Health Information</i> under 45 C.F.R. § 160.103 of HIPAA.
End User	An end entity that uses a HISP's Direct Services. An End User
Group Certificates	A Certificate where use of the corresponding Private Key is shared by multiple entities/End Users.
HIPAA	The Health Insurance Portability and Accountability Act of 1996, as amended.
HISP	A provider of Direct messaging Security/Trust Agent services to Subscribers.
HISP Policy	A policy document, written by DirectTrust, defining the requirements to conform to Direct Message standards and industry privacy and security best practices.
HISP Practices Statement	One or more documents written by a HISP to demonstrate how the HISP meets the requirements of this HISP Policy, including both technical and organizational
Intermediate System	A system outside the HISP boundary that communicates with a HISP or another Intermediate System to send and/or receive Direct messages on behalf of End Users using an edge protocol supported by both systems. See § 1.2.6
Internet Engineering Task	A standards development organization responsible for the

Force	creation and maintenance of many Internet-related
Information Systems Security Officer (ISSO)	An individual responsible for establishing and maintaining the enterprise vision, strategy and program as it relates to Information Systems Security, to ensure information assets are adequately protected.
Private Key	Means either (i) the key of an asymmetric key pair used to create a digital signature, or (ii) the key of an asymmetric key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	Means either (i) the key of an asymmetric key pair used to validate a digital signature, or (ii) the key of an asymmetric key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital Certificate.
Public Key Infrastructure	A set of policies, processes, server platforms, software and workstations used for the purpose of administering Certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key
Registration Authority	The entity responsible for identification and authentication of Certificate subjects.
Relying Party	A person or entity that has received information that includes a Certificate and a digital signature verifiable with reference to a public key listed in the Certificate and is in a position to rely on them.
Required Elements	Those elements of this HP that SHALL appear in the Accreditation criteria.
Secret Key	The cryptographic key only known by the hardware security module and used to wrap/encrypt Subscriber Private Keys prior to storage as well as decryption of those Private Keys during processing of Direct messages
Subscriber	A person or entity that: (1) is the subject named or identified in a Certificate issued to that entity, (2) holds, directly or through its designated HISP, a private key that corresponds to the public key listed in the Certificate, and (3) does not itself issue Certificates to another party.
Subscriber Agreement	Subscriber Agreement means the set of agreements entered into between iShare Medical and a Subscriber under which iShare Medical agrees to provide Subscriber with HISP services.
Trust Anchor	See Trust Anchor Certificate.
Trust Anchor Certificate	A Certificate identifying a trusted issuer of Certificates.

Trust Anchor Store	A repository holding a collection of Trust Anchors.
Trust Bundle Distribution IG	Unless otherwise stated, means the then current version of the Implementation Guide for Direct Project Trust Bundle
Trusted Roles	Has the meaning set forth in § 5.2.1.
Workforce	Employees, volunteers, trainees, and other persons whose

2 Publication and Repository Responsibilities

2.1 Repositories

iShare Medical manages certificates on behalf of its Subscribers for Direct Messaging in a repository of certificates available for discovery via DNS.

2.1.1 Repository Obligations

Subscriber certificates for Direct Messaging managed by iShare Medical on behalf of its End Users are available for discovery 24 hours a day, 7 days a week.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate status

The iShare Medical HISP End User Certificates are discoverable by DirectTrust Accredited HISPs via DNS.

2.2.2 Publication of CA Information

iShare Medical uses a third party DirectTrust Accredited CA that is fully compliant with the DirectTrust CP.

2.2.3 Interoperability

iShare Medical's Certificates are issued by a third party that is DirectTrust Accredited CA and is fully compliant with the DirectTrust CP.

2.3 Frequency of Publication

Each certificate in iShare Medical's repository is available continuously, 24 hours a day, 7 days a week from the time of its publication until it is removed after expiration or revocation.

2.4 Access Controls on Repositories

Certificates in iShare Medical's repository are published for discovery via DNS. The repository resides on servers in iShare Medical's HIPAA compliant datacenter. Management of the certificates in the repository, including addition of certificates to and removal of certificates from the repository, is only available to authorized members of iShare Medical's workforce who must authenticate to the tools designed for this purpose.

3 Identification and Authentication

This section pertains only to naming rules and identity validation for initial certificate issuance, and identification and authentication for re-key and revocation requests for existing certificates. Subsequent identification and authentication of End Users and Intermediate Systems in order to use existing keys for signing or decryption of Direct messages are discussed in Sections 6.7.2 and 6.7.3.

3.1 Naming

No stipulation beyond conformance with the DirectTrust CP.

3.2 Initial Identity Validation

No stipulation beyond conformance with the DirectTrust CP.

3.3 Identification and Authentication for Re-key Requests

No stipulation beyond conformance with the DirectTrust CP.

3.4 Identification and Authentication for Revocation Request

No stipulation beyond conformance with the DirectTrust CP.

4 Certificate Life-Cycle

4.1 Application

No stipulation beyond conformance with the DirectTrust CP.

4.2 Certificate Application Processing

No stipulation beyond conformance with the DirectTrust CP.

4.3 Issuance

No stipulation beyond conformance with the DirectTrust CP.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

No stipulation beyond conformance with the DirectTrust CP.

4.4.2 Publication of the Certificate by the HISP

iShare Medical publishes End User certificate in its repository, discoverable via DNS, as required in section 2.2.1.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

iShare Medical conforms to DirectTrust CP. Private Keys are created using a Hardware Security Module (HSM) and are stored, encrypted by a wrapping key that resides only on the HSM and a duplicate of the HSM, on servers in iShare's datacenter environment. Direct Message signing and decryption operations are performed on an HSM. Further, the primary HSM, and its duplicate are in geographically distinct datacenters.

The iShare Medical HISP trust anchor Certificate is available to Relying Parties for download from the DirectTrust website found here:

<https://bundles.directtrust.org/bundles/accreditedCommunity.p7b>,

as required by the Trust Bundle Distribution IG.

4.5.2 Relying Party Public Key and Certificate Usage

When using Counterparty certificates in the context of sending or receiving a Direct message, a conforming iShare Medical HISP processes the corresponding status information as follows:

If a certificate in the Counterparty certificate chain to be validated lists a CRL distribution point and the HISP obtains status information to confirm that the certificate has not been revoked before the certificate is trusted.

1. If the status information is available, either from newly retrieved data or from a non-stale cached version, and the CRL or OSCP status does not indicate the certificate is revoked, then the iShare Medical HISP will trust the certificate chain so long as all other trust requirements are met.
2. If the status information is available and the certificate is marked as revoked, then the iShare Medical HISP will mark the certificate chain as untrusted.

3. If the status information is not available due to network or other failure, then the HISP mark the certificate chain as not trusted.

iShare Medical requires each incoming signed message intended for an End User to contain at least one trusted and valid Certificate prior to sending a message disposition notification (MDN) back to the Counterparty and further processing the message. If there is not at least one valid Certificate, then the message is marked as untrusted and iShare Medical will not process the message nor send a MDN back to the Counterparty.

4.6 Certificate Renewal

iShare Medical requests Certificate renewals, with new public/private key pairs created in a Hardware Security Module, prior to the Certification expiration dates. This helps ensure the continuity of interoperability as the Direct Address does not change and relying parties continue operations as normal without requiring any action on their part regarding the Certificate renewal.

4.7 Certificate Re-Key

No stipulation beyond conformance with the DirectTrust CP.

4.8 Modification

No stipulation beyond conformance with the DirectTrust CP.

4.9 Certificate Revocation and Suspension

iShare Medical reserves the right to revoke an End User Certificate for any reason. If iShare Medical suspects that a private key has been compromised or other suspicious activity, iShare Medical may inactivate the account rendering it unusable until an investigation has been made. If a determination has been made that a compromise has occurred then iShare Medical will revoke the Certificate. Depending on the circumstances of the incident, a determination will be made whether another Certificate will be issued to the End User or if their iShare Medical HISP services are also to be revoked.

4.10 Certificate Status Services

iShare Medical uses CRL to determine the status of a Counterparty certificate.

4.11 End of Subscription

At the termination of the Subscription to iShare Medical HISP services, iShare Medical revokes all Certificates managed by iShare Medical on behalf of the Subscriber. Additionally, all accounts accessible to End Users authorized to use Certificates on behalf of the Subscriber are disabled or removed.

4.12 Key Escrow and Recovery

iShare Medical does not escrow Certificates.

4.12.1 Key Escrow and Recovery Policy and Practices

iShare Medical does not escrow Certificates.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

iShare Medical does not provide this service.

5 Facility Management and Operations Controls

5.1 Physical Controls

iShare Medical is:

- DirectTrust Accredited for Privacy and Security
- DirectTrust Accredited Health Information Services Provider (HISP)
- DirectTrust Accredited Trust Anchor Bundle

iShare Medical has engaged LightEdge for its two data centers operations. LightEdge is a Tier 3 data center meaning that for every piece of equipment deployed there is at least one additional piece of equipment ready(N+1). This includes server, networks, UPS, backup generators, components for power, cooling, and multiple independent paths for power, and concurrent maintainability. Further, Tier 3 data centers have 99.982% up time or a maximum down time of 1.6 hours per year. LightEdge has the following Certifications and Credentials that are pertinent to iShare Medical:

- HITRUST CSF Certified
- HIPAA schellman Attestation and Compliance Services
- ISO 14001 Environmental Management Systems
- ISO 20000-1 Information Service Management System
- ISO 22301 Business Continuity Management Systems
- ISO 27001 Information Security, Cybersecurity, and Data Protection
- ISO 27701 Privacy Information Management System (PIMS)
- NIST 800-53 schellman Attestation and Compliance Services
- SOC 1 Type 2
- SOC 2 Type 2
- SOC 3 Type 3

5.1.1 Site Location and Construction

The primary data center is located 160 feet underground in a former limestone mine. The walls are thick limestone which are impenetrable by wireless communications. The data center has its a private parking lot with a gated entrance. All doors in and out of the data center and locked and require identity, authentication, authorization prior to access.

5.1.2 Physical Access

The data center has policies and procedures for provision, controlling, and monitoring of physical access to the data center and facilities. Visitors are required to show a valid government ID which is scanned into a computer log, and the ID is retained until the person exists. Visitors are escorted at all times by data center personnel.

Doors require badge access including mutli-factor, biometric scanners, and personal identification. Surveillance cameras are located throughout the facility. Entrance to the systems are protected by a man trap entrance where the door entered must be locked before the next door will open.

5.1.3 Power and Air Conditioning

The data center is equipped with dedicated air conditioning units are configured to notify data center personal in the event of predefined temperature and humidity levels exceeded.

Electricity is supplied by two substations. Production systems are connected to uninterruptible power supply (UPS) systems that are configured to provide temporary electricity in the event of a power outage. In addition, the data center are connected to dedicated power generator that provide electricity during long-term power outages. UPS systems are inspected and maintained semi-annually and generators are inspected and maintained annually.

5.1.4 Water Exposures

Data center equipment is mounted on evaluated racks to facilitate cooling and to protect from flooding.

5.1.5 Fire Prevention and Protection

Data centers are protected by fire detection systems, audible and visual fire alarms, fire extinguishers and either dry-pip water sprinkler or gaseous / chemical fire suppressions. Fire prevention and protection systems are monitored 24/7/365 and are inspected and maintained annually.

5.1.6 Media Storage

All hardware and media is tracked and documented as to its receipts, removal, re-use, and destruction. All backups of data are stored on disk at the data centers. iShare Medical Prohibits storage of protected health information (PHI) and personally identifiable information (PHI) outside of the data centers. All confidential information, including electronic PHI and PHI, is properly removed from electronic hardware and media before such media is made available for re-use. Upon final disposition of hardware and media containing PHI and PII, all electronic media and hardware is destroyed or disposed of such that it is rendered unreadable.

Further, all destruction of information contained on electronic media and hardware is done in accordance with iShare Medical's record retention policies.

5.1.7 Waste Disposal

See 5.1.6 for the destruction and removal of hardware and media containing PHI or PHI

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. iShare Medical performs pre-employment screening of all employees. Further, employees and contractors are required to participate in ongoing training including training annual training on the four rules of HIPAA Privacy Rule, Security Rule, Breach Notification Rule, and Enforcements Rule and iShare Medical's Policies compliance with these rules.

There are 5 roles defined by DirectTrust Policy and HIPAA that are related to the operation, administration, and management and implemented by iShare Medical they are:

Administration and Operations:

1. Administrator
2. Information Systems Security Officer (ISSO)
3. Operator – authorized to perform system backup and recovery.

Compliance and Support:

4. iShare Medical Security Officer
5. iShare Medical Privacy Officer

5.2.1.1 Administrator

The administrator role is responsible for:

- Installation, configuration, and maintenance of the HISP
- Establishing and maintaining HISP system accounts

5.2.1.2 Information Systems Security Officer

The Information Systems Security Officer is responsible for:

- Configuring End User profiles or templates
- Generating, installing and backing up End User keys
- Managing End User access to private keys stored by HISP

- Managing HISP-wide trust decisions, e.g. addition or deletion of trust anchors, trust bundles, or policy enforcement rules, if applicable

5.2.1.3 Operator

The operator role is responsible for the routine operation of the HISP equipment and operations such as system backups and recovery or changing recording media.

5.2.1.4 iShare Medical Security Officer

The iShare Medical Security Officer is responsible for implementing and enforcing the Security Policies and Procedures, communicating with iShare Medical's workforce members and contractors regarding HIPAA security issues, and educating iShare Medical's workforce members and contractors regarding HIPAA and the Security Policies and Procedures.

5.2.1.5 iShare Medical Privacy Officer

The iShare Medical Privacy Officer is responsible for implementing and enforcing the Privacy Policies and Procedures, communicating with iShare Medical's workforce members and contractors regarding HIPAA privacy issues, and educating iShare Medical's workforce members and contractors regarding HIPAA and the Privacy Policies and Procedures.

5.2.2 Number of Persons Required Per Task

No stipulation.

5.2.3 Identification and Authentication for Each Role

Each role is assigned the proper rights and privileges in order to perform their job responsibilities. These roles are bound to their identity.

5.2.4 Separation of Roles

No stipulation.

5.2.5 Access to Electronic PHI

iShare Medical restricts the number of workforce members that have access to the data centers containing PHI and PII to a maximum of three workforce members that are required to adhere to iShare Medical's minimally necessary policies in accordance with HIPAA.

5.2.6 Use of Cloud Service Providers

iShare Medical does not use a CSP (Cloud Services Provider).

iShare Medical operates in a secure Private Cloud in a Tier 3 data center. For privacy and security reasons, iShare Medical does not support on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

iShare Medical performs pre-employment screening on all employees.

5.3.2 Background Check Procedures

No stipulation.

5.3.3 Training Requirements

Employees and contactors are required to participate in ongoing training including training annual training on the four rules of HIPAA Privacy Rule, Security Rule, Breach Notification Rule, and Enforcements Rule and iShare Medical's Policies compliance with these rules.

5.3.4 Retraining Frequency and Requirements

Annually.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

iShare Medical Sanctions policies have the following steps:

1. investigation and determine of the incident,
2. assessment of severity,
3. determination of the level of sanction, and
4. implementation of the sanction.

5.3.7 Independent Contractor Requirements

Independent Contractors of iShare Medical are required to sign a Business Associate Contractor Agreement and, in some cases, also are asked to sign a confidentiality and non-disclosure agreement.

5.3.7.1 Business Associates of HISP

iShare Medical most commonly provided service is HISP services to a Business Associate of a Covered Entity or Business Associate Subcontractor. LightEdge is a Business Associate Sub-

contractor to iShare Medical providing fully managed data center operations at two data center locations.

5.3.8 Documentation Supplied to Personnel

Workforce members are provided with access to the iShare Medical Privacy Manual, iShare Medical Privacy Manual Documentation, and access to online training on HIPAA. Further, workforce members are provided with one-to-one training when assigned a new task. Often these training sessions are recorded for reference and review.

5.4 Audit Logging Procedures

Audit log files are generated for all events occurring within the HISP boundary that relate to the security of the HISP. All security audit logs, both electronic and non-electronic, are retained and are made available during compliance audits. Note that most logs are automated electronic logs.

5.4.1 Types of Events Recorded

At a minimum, each audit record includes the following (either recorded automatically or manually for each auditable event):

- The type of event
- The date and time the event occurred
- A success or failure indicator, where appropriate
- The identity of the entity and/or operator (of the HISP) that caused the event

The security events captured by iShare Medical HISP are listed in the table below.

SECURITY AUDIT
• Any changes to the audit parameters, e.g. audit frequency, type of event audited • Any attempt to delete or modify the audit logs
AUTHENTICATION TO HISP STA SYSTEMS
• Successful and unsuccessful attempts to assume a role • The value of maximum number of authentication attempts is changed • Maximum number of unsuccessful authentication attempts reached during user login
LOCAL DATA ENTRY
• All security-relevant data that is entered in the system
REMOTE DATA ENTRY

• All security-relevant messages that are received by the system
DATA EXPORT AND OUTPUT • All successful and unsuccessful requests for confidential and security-relevant information
KEY GENERATION • Issue Certificate • Revoke Certificate • Access Certificate
PRIVATE KEY LOAD AND STORAGE • All access to certificate subject Private Keys retained within the HISP for key recovery purposes
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE • Any change to the trusted public keys, including additions and deletions
SECRET KEY STORAGE • The creation of secret keys used for authentication
PRIVATE AND SECRET KEY EXPORT • The export of private and secret keys (keys used for a single session or message are excluded)
HISP CONFIGURATION • Any security-relevant changes to the configuration of a HISP system component
ACCOUNT ADMINISTRATION • Roles and users are added or deleted • The access control privileges of a user account or a role are modified
TRUST MANAGEMENT PROFILES • All changes to End User trust management profile, including policy enforcement rules, enabling or disabling trust anchors or trust bundles.
TIME STAMPING • A third-party time stamp is obtained (local system time stamps are excluded).

MISCELLANEOUS • Appointment of an individual to a Trusted Role • Installation of an Operating System • Installation of a HISP Application • Installation of Hardware Security Modules • System Startup • Logon attempts to PKI Application • Attempts to set passwords • Attempts to modify passwords • Backup of the internal HISP database • Restoration from backup of the internal HISP database • All certificate compromise notification requests • Zeroizing Hardware Security Modules • Re-key of a HISP system component
CONFIGURATION CHANGES • Hardware • Software • Operating System • Patches
PHYSICAL ACCESS / SITE SECURITY • Known or suspected violations of physical security • ANOMALIES • System crashes and hardware failures • Software error conditions • Software check integrity failures • Network attacks (suspected or confirmed) • Equipment failure • Violations of the HP or HPS • Resetting Operating System clock

5.4.2 Frequency of Processing Log

iShare employs open-source tools, OSSEC, AuditD, and ClamAV to monitor activity on, for Host Intrusion Detection, and to protect against malware on iShare's systems that alert the Security Officers or his or her designee to suspected or known security incidents. OSSEC is configured to send alerts via email to the Security Officer for events above a predetermined OSSEC alert level. An appropriate review and mitigations are conducted for such alerts. The ClamAV software antivirus database is configured to update at least once per day. Further iShare Security Officer or designee monitors additional system log files for potential security incidents.

Audit logs capture:

- Login attempts, both successful and failed attempts
- Changes to account privileges
- Unauthorized function calls
- Elevation of privileges
- CRUD of security and audit parameters
- System shutdown/restart
- System errors
- CRUD of files in monitored directories

5.4.3 Retention Period for Audit Logs

OSSEC and AuditD logs are retained for at least 30 days.

5.4.4 Protection of Audit Logs

Access to audit logs are restricted to users with access to the datacenter VMs, which is a maximum of three iShare workforce members.

5.4.5 Audit Log Backup Procedures

Security Audit logs are included in the nightly full image backups of the VMs automatically conducted by the datacenter backup processes.

5.4.6 Audit Collection System (internal vs. external)

All security audit processes are invoked at HISP startup and cease only at shutdown. In the event of a failure of a security audit component, iShare accesses the issue and endeavors to recover the failed components in a timely manner. If such a recovery cannot be accomplished in a timely manner, iShare shuts down external customer access to its systems in order to continue assessment and planning and response and to ensure minimal injury to customer data. After recovery from such an incident, iShare monitors the security logs and system activity carefully until satisfied the incident is resolved.

Assessment of what is considered “timely” is at the discretion of the ISSO and the owner/CEO of iShare Medical.

5.4.7 Notification to Event-Causing Subject

The subject is not notified of the audit event.

5.4.8 Vulnerability Assessments

iShare Medical has engaged its HITRUST Certified data center to perform data center management, security, and operational tasks such as Private Cloud, Private Cloud Data Protection, Cloud Monitoring, Managed Firewalls, Managed Security, Managed Backup and Disaster Recovery. Risk assessments are performed at least annually but can be performed more often based on the threat level, to identify and evaluate risks that threaten the ability of iShare Medical to conduct business operations.

Risk assessment review major changes in business environment, threat and/or vulnerability landscape or control effectiveness. Each risk is evaluated for likelihood and impact to people, property, and business, and assigned a risk rating, existing controls that mitigate measures that are considered in the risk score. A risk treatment plan is used to evaluate the residual risk score and determine if there is any additional need for mitigation or if the residual risk can be accepted

In addition, iShare has also engaged with an independent third party to conduct periodic Cyber Hygiene scans of iShare Medical's public facing interfaces to test for vulnerabilities. The frequency with which scans are performed depends upon the frequency and severity of vulnerabilities found during previous scans and threat level. These assessments are performed at least once per week but can be performed multiple times per day if the threat level is high. Assessment reports are monitored by iShare Medical's ISSO. If a potential vulnerability is found, a ticket is created with iShare Medical's data center for investigation and resolution.

Further, the data center and iShare Medical operations maintain firewalls, runs continuous intrusion detection, anti-virus and malware detection software. The goal is to detect, prevent, and find security risks and mitigate the risk.

5.5 Records Archival

5.5.1 Types of Events Archived

The following items are examples are items which iShare Medical archives:

1. Any Accreditation of the HISP,
2. HP and HPS versions,
3. Contractual obligations and other agreements concerning the operation of the HISP, notably BAAs,
4. Certificate signing and revocation requests,
5. Any documentation related to the receipt or acceptance of a certificate or token,
6. End User Agreements,
7. Compliance auditor reports
8. Access to Private Keys for key recovery purposes,
9. Appointment of an individual to a trusted role,

iShare Medical Policies and Procedure specify that iShare Medical is to document the following items when these events occur; however, none of these events have occurred:

1. Destruction of a cryptographic module,
2. Certificate compromise notifications,
3. Remedial action taken as a result of violations of physical security
4. Violations of the HP or HPS.
5. Security or Privacy Sanctions
6. Breach notifications

5.5.2 Retention Period for Archive

No stipulation.

5.5.3 Protection of Archive

No stipulation.

5.5.4 Archive Backup Procedures

No stipulation.

5.5.5 Requirements for Time-Stamping of Records

No stipulation.

5.5.6 Archive Collection System (Internal vs. External)

No stipulation.

5.5.7 Procedures to Obtain & Verify Archive Information

No stipulation.

5.6 Key Changeover

No stipulation beyond conformance with the DirectTrust CP.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

iShare Medical performs annual testing and review of incident response including planning, testing, and training. This review includes a review and analysis of incident response plan: incident investigation, internal communications, external communications, business continuity, disaster recovery, and customer impact analysis.

iShare Medical's has policies and procedures for potential security incidents, including investigate of the incident, determination if a security event occurred, assessment of severity, determination if a breach has occurred of PHI, and if so, quantification of the breach, review of Business Associates Agreement regarding required notifications to Covered Entities/Subscribers, identification of the parties to be notified in consideration of applicable state and federal law, and Business Associates Agreement, and remediation of the event. Further, this policy provides guidelines for documentation of the event.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

iShare Medical performs daily full image backups of the three servers, web server, database server, and app server at the iShare Medical primary data center. Full image backups create a copy of the operating system and all its data including the system state and configurations making recovery of the exact system faster. Each day upon completion, a copy of each of these three backup files are sent via an IPSec tunnel to the backup data center that is located approximately 200 miles away from the primary data center. This means that there are two copies of the three servers, one copy at the primary data center and another copy at the backup data center.

In addition, iShare Medical has Hardware Security Modules (HSMs) deployed at both data centers which are used for wrapping and unwrapping primary keys. Both HSMs employ the same wrapping key, enabling them to decrypt and sign messages with the same customer's private keys.

In the unlikely event that data becomes corrupted, iShare Medical can recover from the full image backups of the three servers. If the private keys on the HSM(s) at one of the datacenters become corrupted, iShare Medical can flip a switch and be fully operational using the backup HSM(s).

5.7.3 Entity Private Key Compromise Procedures

iShare Medical reserves the right to revoke an End User Certificate for any reason. If iShare Medical suspects that a private key has been compromised or other suspicious activity, iShare Medical may inactivate the account rendering it unusable until an investigation has been made. If a determination has been made that a compromise has occurred, then iShare Medical will revoke the Certificate. Depending on the circumstances of the incident, a determination will be made whether another Certificate will be issued to the End User or if their iShare Medical HISP services are also to be revoked.

5.7.4 Business Continuity Capabilities after a Disaster

iShare Medical Business Continuity and Disaster Recovery is a core component of our operational strategy. This is way we have chosen our HITRUST Certified Tier 3 data centers. Our Tier 3 data centers have N+1 redundancy. This means that for every piece of equipment that is at least one additional piece of equipment, that is idle and ready to be deployed in production. Tier 3 data centers also have a maximum of 1.6 hours of planned downtime per year.

iShare Medical operates two geographically diverse (200 miles apart) data centers (see 5.7.2 for a description of our backup and recovery ability). In most cases, iShare Medical can have a restore of our systems at the backup data center fully operational in less than 24 hours. Plus, failure of an HSM that we use for wrapping private keys can be operational with a flip of a switch.

5.8 HISP Termination

No stipulation.

5.9 Backup of Electronic PHI

iShare Medical's backups are full image copies of the systems. This includes all PHI and Direct Messages sent or received to or from iShare Medical HISP. For more information about iShare Medical's backups see section 5.7.2.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

As a HISP, iShare Medical creates Direct Addresses and generates two key pairs. These addresses are bound to the digital identity of the entity as well as two key pairs, each pair bound to an X.509 Certificate, one of which is for encryption/decryption of the data and the other of which is used for the digital signature of the transaction. The DirectTrust Certificate Policy (CP) describes policies that the Certificate Authority must adhere to for issuance and management of X.509 certificates for use in Direct messaging applications. These policies and practices flow to iShare Medical when creating, maintaining, and protecting the Direct Addresses. Private Keys are created using a Hardware Security Module (HSM) and are stored, encrypted by a wrapping key that resides only on the HSM and a duplicate of the HSM, on servers in iShare's datacenter environment. The HSM is used for wrapping and unwrapping the private keys.

6.1.2 Private Key Delivery to Subscriber

iShare Medical does not deliver private keys to the Subscriber. Instead, private keys are kept by iShare Medical and stored wrapped (encrypted) on systems in iShare's datacenter environment. They are only unwrapped for the purpose of decrypting an inbound message or applying a digital signature inside an HSM.

6.1.3 Public Key Delivery to Certificate Issuer

Public Keys are delivered via a Certificate Signing Request (CSR) to the Certificate Authority using a secure channel including a username/password combination plus a client certificate.

6.1.4 Public Key Delivery to Relying Parties

6.1.4.1 HISP Trust Anchor Delivery

The iShare Medical is a DirectTrust Accredited Trust Anchor HISP. iShare Medical's Trust Anchor Certificate is available to Relying Parties for download from the DirectTrust website found here:

<https://bundles.directtrust.org/bundles/accreditedCommunity.p7b>.

Certificates signed by iShare's Trust Anchor, which is included in this bundle, are published via DNS on a server in iShare Medical's datacenter as required by the Trust Bundle Distribution IG.

6.1.4.2 End User Subscriber Public Key Delivery

Subscriber Public Keys are delivered within the Certificates and made available for discovery through DNS as specified in the Certificate Discovery IG.

6.1.5 Key Sizes

iShare Medical utilized a minimum of 2048-bit RSA Key with Secure Hash Algorithm version 2 (SHA-256) for all Subscriber Certificate Keys.

6.1.6 Public Key Parameters Generation and Quality Checking

iShare Medical generates the Public Key parameters in accordance with Digital Signatures specified in FIPS 186-2.

iShare Medical perform quality checking in accordance with Digital Signatures specified in FIPS 186-2.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

iShare Medical issues Certificates in compliance with DirectTrust Certificate Policy 2.0 or later. iShare Medical issues two key pairs, one for digital signature of outbound messages and the other for encryption/decryption of inbound messages. Certificates assert a single key usage bit of either:

- digitalSignature
- keyEnchipherment

iShare Medical issues Key Usage Purposes asserted in the key usage field of extended key usage extension bit of emailProtection in conformance with DirectTrust CP 2.0. iShare Medical does not issue Certificates that assert the non-repudiation bit. iShare Medical enforces key usages when using certificates for Subscribers to whom iShare Medical holds the private key.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

HISPs that manage private keys SHALL perform specific risk assessment and risk mitigation to ensure that the private keys have the strongest protection from unauthorized use.

A conforming HISP SHALL identify at least one Information Systems Security Officer (ISSO) or equivalent, who will be responsible for ensuring adequate protection of cryptographic keys held on behalf of End

Users, and also for tracking and recording exactly who has access to said keys at any given point.

A HISP ISSO SHALL perform these responsibilities, including any delegation of the tracking and recording obligations to its customers, in accordance with the DirectTrust CP.

6.2.1 Cryptographic Module Standards and Controls

iShare Medical employs Hardware Security Modules (HSMs) for the creation of public/private key pairs and for decryption of inbound and signing of outbound messages using those keys. The HSMs include a primary HSM and a backup HSM that are in geographically distinct datacenters.

6.2.2 Private Key (n out of m) Multi-person Control

Does not apply. iShare Medical does not allow multi-person control.

6.2.3 Private Key Escrow

Does not apply. iShare Medical does not Escrow Private Keys.

6.2.4 Private Key Backup

Private Keys are created using a Hardware Security Module (HSM) and are stored, encrypted by a wrapping key that resides only on the HSM and a duplicate of the HSM, on servers in iShare's datacenter environment. Direct Message signing and decryption operations are performed on an HSM. Further, the primary HSM, and its duplicate are in geographically distinct datacenters.

The wrapped keys are backed up during the nightly backups of systems in the datacenter. In the event of failure of the primary HSM, iShare Medical can flip a switch and be fully operational using the backup HSM.

6.2.5 Private Key Archival

Not applicable.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Private Keys are generated using an HSM. Keys are wrapped with an AES-128 secret key and stored as files and in a database on servers in iShare's datacenter environment. Private Keys can only be used by unwrapping the key using the HSM and decrypting them using the secret AES-128 key. Private Keys are always wrapped and unwrapped using the HSM and are therefore never exposed in an unencrypted state outside of an HSM.

6.2.7 Private Key Storage on Cryptographic Module

Private Keys are always wrapped and unwrapped using the AES-128 secret key on an HSM and are therefore never exposed in an unencrypted state outside of an HSM. Wrapped keys are stored as files on a server and in a database in iShare's datacenter environment; however, they are useless without the HSM and AES-128 secret key.

6.2.8 Method of Activating Private Keys

iShare Medical is the custodian of the private keys of their Subscribers. iShare Medical activates the Subscribers Private key such that it can be used.

6.2.9 Methods of Deactivating Private Keys

Only iShare Medical can activate and deactivate Private Keys. This is done by removing the wrapped private key from its location in the file system and from the database.

6.2.10 Method of Destroying Private Keys

Private Keys are destroyed upon termination of the Subscribers Services or when a Private Key becomes compromised. This is done by removing the wrapped private key from its location in the file system and from the database.

6.2.11 Cryptographic Module Rating

No stipulation beyond conformance with the DirectTrust CP.

6.3 Other Aspects of Key Management

6.3.1 Public Key Archival

Public Keys are backed up as a part of the daily back up process see section 5.7.2.

6.3.2 Certificate Operational Periods/Key Usage Periods

iShare Medical issues Certificates for one year from the date of issuance. Certificates for active customers are renewed once per year with new private/public key pairs. In the event that a private key is potentially compromised, the corresponding subscriber certificates are renewed by re-keying with a new set of public/private key pairs. In this case, the resulting certificates are valid until the next expiration time of the certificates they replace.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

No stipulation beyond conformance with the DirectTrust CP.

6.4.2 Activation Data Protection

No stipulation beyond conformance with the DirectTrust CP.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

1. Before a person becomes a workforce member at iShare Medical with access to systems in the datacenter, where PHI resides, they first undergo a background check performed by a qualified partner for this purpose.
2. Each workforce member with remote access to the systems in the datacenter must gain this access via a VPN connection that requires two factors of authentication including a username/password combination plus a second factor of authentication, which is entered via a cell phone app after the username/password combination is successfully submitted.
3. As there are only three such users who have such access, all of them require root level access to the systems in the datacenter as each must potentially serve in a role as a replacement/substitute for the others.
4. Actions taken by such users are logged in audit records accessible by AuditD and OSSEC.
5. Workforce members who have such access must abide by iShare Medical's Workstation Policy which requires users to ensure that unattended systems are locked so that the screen is not displayed and a password is required to unlock the screen, that any monitor or display screen is protected from viewing by unauthorized individuals among other protections.

6. Workforce members who have such access must abide by iShare Medical's Prohibition on Storage of PHI policy which prohibits downloading or storage of PHI on any device or medium outside of the datacenter.
7. Workforce members who have such access must abide by iShare Medical's Wireless Policy which requires that any WiFi connection used for internet access while connecting via VPN must require a password that is compliant with iShare Medical's Password Policy and must be configured to use WPA2 or newer protocol with AES or higher encryption.
8. Workforce members who have such access must abide by iShare Medical's Protection Against Malicious Software policy, which requires workstations to be protected by approved anti-malware/antivirus software.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life-Cycle Security Controls

The requirements of Section 6.6.1 – 6.6.3 apply only to systems controlled by the HISP.

6.6.1 System Development Controls

Per iShare Medical's Software Development Lifecycle policy (SDLC), iShare primarily employs an Agile model for software development.

Furthermore, iShare participates in DirectTrust's annual Greenlight testing with other HISPs in the Accredited Trust Anchor Bundle (ATA). iShare always achieves 100% interoperability with its ATAB partners during this testing.

6.6.2 Security Management Controls

Hardware system changes are addressed by iShare Medical's datacenter. Beyond that, changes to systems at the virtual and software level are subject to iShare Medical's policies for SDLC, patch management, audit logging, risk assessment, incident response, and emergency response. Software modifications are primarily guided by the Agile SDLS method and require planning, testing, tweaking ins a development and testing environment, then approval before deployment into the production environment.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

iShare Medical's firewall blocks suspicious traffic and also blocks all traffic identified as being from outside the USA.

iShare Medical's Prohibition on Storage policy prohibits workforce members from storing PHI on any device or media outside this datacenter.

iShare Medical's Workstation policy requires workforce members to ensure that unattended systems are locked so that the screen is not displayed, and a password is required to unlock the screen, that any monitor or display screen is protected from viewing by unauthorized individuals among other protections.

iShare Medical's Wireless Policy requires that any WiFi connection used by workforce members for internet access while connecting via VPN must require a password that is compliant with iShare Medical's Password Policy and must be configured to use WPA2 or newer protocol with AES or higher encryption.

iShare Medical's Protection Against Malicious Software policy requires workstations used by workforce members to be protected by approved anti-malware/antivirus software.

6.7.1 End User Data Storage and Edge Protocols

iShare Medical's enterprise firewall blocks suspicious traffic. All incoming traffic goes through the firewall that includes advance intrusion detection, prevention, and monitoring:

- Address spoofing
- Fragmentation of packets
- Pattern evasion
- Coordinated attack threat
- Network intrusion detection system (NIDS)
- Host intrusion detection (HIDS)
- Signature-based intrusion detection system (SIDS)
- Anomaly-based intrusion detection system (AIDS)
- Perimeter intrusion detection systems (PIDS)
- Virtual machine-based intrusion system (VMIDS)
- Stack-based intrusion detections system (SBIDS)

iShare Medical employs the services of a datacenter where data is stored at rest using 256 bit AES encryption.

iShare Medical offers a web user interface to access Direct Messaging accounts. The web site is protected via TLS 1.2. Each user is required to have his or her own login. Login requires a username/password plus a second factor of authentication consisting of a randomly generated single use token sent to a user's cell phone that is valid for approximately 60 seconds.

Direct Messages received using this tool are encrypted using RSA 2048 bit public keys. The inbound messages are decrypted using a private key that is imported and unwrapped within a

Hardware Security Module (HSM). Outbound messages are signed using a private key, also unwrapped within the HSM, where the digital signature is attached before the message is sent.

A conforming HISP SHALL ensure the security of the messages processed by the HISP supports adherence to the standard HIPAA privacy rules defined at 45 CFR Part 160 and Subparts A and E of Part 164.

iShare Medical also offers a RESTful API for Direct Messaging. Calls made to this API are also encrypted via TLS and require username/password plus a client certificate for Mutual TLS. The client certificate is bound to an RSA 2048 bit public/private key pair. Direct Messages sent or received use the same encryption methods and HSMs as for the web user interface described above.

6.7.2 Authentication of End Users

End users authenticate for sending, receiving, viewing Direct Messages via the web UI or the API as described in the section 6.7.1. In the case of the Web UI, the website is accessed via https (TLS) and in the case of the API, as indicated above, a client certificate for Mutual TLS is required.

6.7.3 Authentication of Intermediate Systems

An intermediate system may access iShare Medical's API for Direct Messaging via authentication by submission of a username/password combination plus a client certificate for Mutual TLS as described in previous sections.

6.7.4 Access Controls (Internal Access)

No stipulation.

6.8 Time Stamping

iShare Medical's servers are configured to synchronize their clocks with NTP time servers operated by NIST.

6.9 Direct Messaging Operations

6.9.1 CA and RA Services

iShare Medical uses a DirectTrust Accredited Registration Authority for identity proofing and a Authority DirectTrust Accredited Certification Authority for certificate creation DirectTrust accredited HISP Services.

6.9.2 End User/Subscriber Agreements

Subscribers who are Covered Entities or Business Associates of Cover Entities are required to agree to the following:

- iShare Medical HISP Agreement
- iShare Medical Directory Data Sharing Agreement
- Business Associates Agreement or Business Associates Subcontractors Agreement

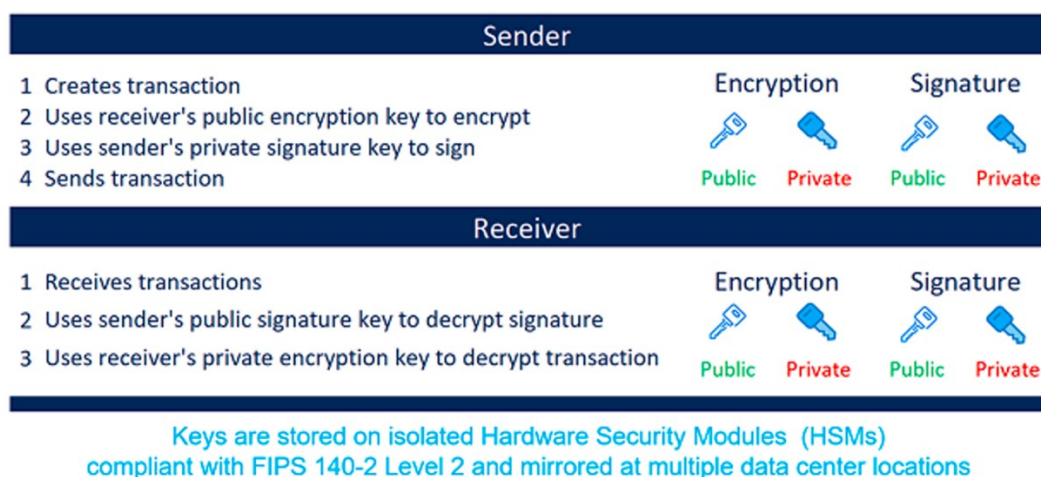
6.9.3 Trust Management

iShare Medical DirectTrust Accredited Trust Anchor HISP providing Secure Direct Messaging services to patients, providers, payers, and devices. There are three components to Direct Messaging:

- RA (Registration Authority)– perform digital identity proofing of the End User of Subscriber at NIST 800-63-2 IAL2
- CA (Certificate Authority) – create two key pairs, each pair is bound to an X.509 Certificate, one key pair is for encryption/decryption of the data and the other key pair is digital signature of the transaction. The Certificates are issued under the HISP’s Accredited Trust Anchor.
- HISP (Health Information Services Provider) – creates the Direct Address that is bound to the End Users or Subscribers real identity and also bound to two single use X.509 Certificates. The Direct Address also contains metadata about the End User or Subscriber. Each key pair has a Public Key and a Private Key. It is the role of the HISP to protect the Private Key while also using it for secure encrypted exchange of protect health information and personally identifiable informaiton. iShare Medical protects the Private Keys by wrapping them using a Hardware Security Module (HSM) that can only be unwrapped using a secret wrapping key. The wrapping key exists only on the primary HSM and on a duplicate of the primary HSM in a geographically distinct location.

At the time of exchange, the sending HISP interrogates the sender’s Direct Address Certificates to confirm the identity of the sender and to ensure they chain to a valid root certificate in the Accredited Trust Anchor Bundle (ATAB). Then, the receiver’s encryption Certfcate is also checked to see if it chains to a trusted root certificate in the ATAB. If both the sender and receiver are trusted, the HISP uses the receiver’s public key to encrypt the transaction and sender’s private key to sign the transaction and sends the message. The receiving entity’s HISP uses the sender’s public key to decrypt the signature and uses receiver’s the private key to decrypt the transaction (see diagram below).

How Public Key Infrastructure (PKI) Works



It is not possible to spoof or spam a Direct Message because the sender and receiver are always known.

6.9.4 Direct Messaging Protocols

iShare Medical performs digital identity, certificate generation, creation of the Direct Address bound to the digital identity, authentication, authorization, encryption and decryption of messages Secure Direct Messaging utilizing SMTP transport protocol as specified in the Applicability Statement for Direct Secure Health Transport.

iShare Medical supports both DNS and LDAP methods for discovery of electronic endpoint as specified in the S&I Framework Certificate Discovery for Direct Project Implementation Guide dated January 9, 2012, or any subsequent version to securely route message from the senders Direct Address to the recipients Direct Address.

6.9.4.1 Message Disposition Notifications (MDNs)

iShare Medical has implemented a response mechanism for final delivery notification in accordance with Delivery Notification IG.

When HISP receives an incoming Direct message invoking the final delivery notification request mechanism, the respond to the sender with either a Dispatched MDN or failure notification in accordance with the Delivery Notification IG.

In cases where the HISP is responsible for providing final message storage for the recipient, then a positive delivery notification as defined by the Delivery Notification IG is issued upon delivery to the recipient's inbox. If the HISP delivers received messages to an intermediate system, then a positive delivery notification is issued upon successful handoff of the message to the intermediate system, as defined by the HISP APIs. A positive delivery notification is not a "read receipt" and does not imply that the message was opened, viewed, or acted upon by the recipient.

iShare Medical HISP will not delay the transmission of Processed MDNs in response to incoming Direct messages. Once a receiving iShare Medical HISP has successfully decrypted a message, verified trust and message integrity, a Processed MDN is transmitted promptly to indicate to the sender that iShare Medical HISP has received the message and is taking responsibility to attempt delivery to a recipient or endpoint serviced by the HISP. If such delivery attempt subsequently fails, the HISP SHOULD transmit a failure notification to the sender.

If one-way trust is enabled for sending or receiving Direct messages with a Counterparty, iShare Medical allows for receipt and/or transmission of corresponding message disposition notifications in accordance with the Applicability Statement and, when applicable, the Delivery Notification IG.

iShare Medical has established time-out intervals for receipt of expected message disposition notifications from Counterparty HISPs and provides failure notifications when those time-out intervals have been exceeded. The time-out interval is one hour for receipt of routine Processed MDNs and one hour for receipt of Dispatched MDNs.

When a HISP sends a message without a request for final delivery notification, it is possible that the HISP will receive a delayed failure notification message after receiving a routine Processed MDN from the Counterparty HISP. There is no time limit on when such a delayed failure notification may be sent. Determination of how delayed failure notifications are handled is a matter of local HISP policy.

6.9.4.2 Message Wrapping

When sending a message on behalf of the End User, iShare Medical HISP wraps the Unwrapped Direct messages in order to protect the outer, non-content-related message header fields by wrapping the message as specified in Section 3.1 of the “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification,” RFC 5751, published by the Internet Engineering Task Force and be able to accept and process incoming messages wrapped in this manner.

The iShare Medical HISP validates the sender and recipient information for an incoming message and generates a wrapped message by including the full message submitted by or constructed on behalf of the End User in a message/rfc822 wrapper with the signer and encryption Certificates used.

The iShare Medical HISP uses the same non-content-related message header fields in both the outer headers and the wrapped headers for consistency and suppress the “Subject” header field in the outer message to mitigate against inadvertent exposure to PHI, and does not allow blind copy or copy recipients to improve reconciliation of the SMTP envelope data with protected headers by all Counterparties.

When receiving a message on behalf of an End User, iShare Medical allows incoming messages that use not wrapped messages in the interest of supporting interoperability with older systems. When receiving a wrapped message on behalf of an End User, it can be assumed that the intent was to provide header protection. iShare Medical validates that sender and recipient information for an incoming message is consistent with the protected headers within the message/rfc822 wrapper and with the signer and encryption certificates used. consistencies are found relating to sender and recipient information.

iShare Medical processes any message disposition notification requests included in the wrapped headers. Message disposition notifications sent in response to a wrapped message contains a set the value of Original-Message-ID field of the outgoing message disposition report to the value of the Message-ID field within the protected inner headers if this value is different from the outer Message-ID.

6.9.4.3 Case Sensitivity

For incoming messages, iShare Medical HISP treats the Direct addresses that it services in a case-insensitive manner. When address certificates are used, a conforming HISP SHALL treat Subject Alternative Name/rfc822 Name entries in a case-insensitive manner when validating the binding between a Direct address and the rfc822Name. The domain part of any Direct address and any dnsName included in a domain-bound certificate SHALL always be treated in a case- insensitive manner.

6.9.4.4 Message Canonicalization

iShare Medical prepares the message content for signing in accordance with Section 3.1 of RFC 5751. This preparation includes conversion of all leaf parts of the MIME content to canonical form as detailed in Section 3.1.1 of RFC 5751 prior to computation of the message digest for the digital signature.

Before computing the message digest on an incoming message to validate a digital signature, a receiving iShare Medical will either (a) convert the received content to canonical form or (b) treat the received content as if it were properly canonicalized by the sender (i.e. perform no further canonicalization).

6.9.4.5 Delivery Status Notifications (DSNs)

iShare Medical facilitates the ability for the sending STA to correlate the original message with the receiving the STA as follows:

To enable the original sending STA to correlate a Delivery Status Notification (DSN) with the original message, a receiving STA that generates a DSN SHALL set a per-message extension field of X-Original-Message-ID with a value of the original RFC822 message ID. For compatibility with legacy systems, if the X-Original-Message-ID is not present in a received DSN,

a sending STA uses the value of the In-Reply-To field when available to correlate the DSN with the original message.

6.9.5 Directory Services

iShare Medical HISP provides the ability to look up provider Direct Addresses via the iShare Medical Directory. Subscribers are required to be a HISP customer and agree to the iShare Medical HISP Services Agreement, DirectTrust Data Sharing Agreement, and enter into a Business Associates or Business Associates Subcontractor Agreement. iShare Medical complies with the DirectTrust Aggregated Directory Sharing Policy Version 4.0 or later and the terms of the terms required to participate in the iShare Medical Directory are contained in Subscriber documents.

7 Certificate, CRL, and OCSP Profiles Format

7.1 Certificate Profile

iShare Medical HISP processed and use certificates issued in conformance with the certificate profiles defined in the DirectTrust CP.

7.1.1 Version Numbers

No stipulation beyond conformance with the DirectTrust CP.

7.1.2 Certificate Extensions

No stipulation beyond conformance with the DirectTrust CP.

7.1.3 Algorithm Object Identifiers

No stipulation beyond conformance with the DirectTrust CP.

7.1.4 Name Forms

No stipulation beyond conformance with the DirectTrust CP.

7.1.5 Name Constraints

No stipulation beyond conformance with the DirectTrust CP.

7.1.6 Certificate Policy Object Identifier

No stipulation beyond conformance with the DirectTrust CP.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

iShare Medical HISP process Certificates in accordance with section 6.9.3.

iShare Medical will reject Certificates in which an extension that it does not recognize or when a critical extension that contains information that it cannot process.

7.2 CRL Profile

iShare Medical HISP process processes CRLs in accordance with the CRL profile defined in DirectTrust CP 2.0.

7.2.1 Version Numbers

No stipulation beyond conformance with the DirectTrust CP.

7.2.2 CRL and CRL Entry Extensions

No stipulation beyond conformance with the DirectTrust CP.

7.3 OCSP Profile

No Stipulation.

8 Compliance Audits and Other Assessments

iShare Medical is audited by DirectTrust Audits every two years. iShare Medical first achieved DirectTrust Accreditation for Privacy and Security and as DirectTrust Accredited Trust Anchor on February 25, 2015.

DirectTrust Audits iShare Medical for Privacy and Security and HISP Accredited at least once every two years. DirectTrust Accreditation program to certify the compliance of HISPs. iShare Medical is DirectTrust Accredited for Privacy and Security and a DirectTrust Accredited Trust Anchor HISP which is published on the DirectTrust website at:

<https://accreditation.directtrust.org/accreditation-full>

iShare Medical has not other audits or assessment to report.

iShare Medical's data center LightEdge, has participated in many assessments including the following Certifications and Credentials that are pertinent to iShare Medical:

- HITRUST CSF Certified
- HIPAA schellman Attestation and Compliance Services
- ISO 14001 Environmental Management Systems
- ISO 20000-1 Information Service Management System
- ISO 22301 Business Continuity Management Systems
- ISO 27001 Information Security, Cybersecurity, and Data Protection
- ISO 27701 Privacy Information Management System (PIMS)
- NIST 800-53 schellman Attestation and Compliance Services
- SOC 1 Type 2
- SOC 2 Type 2
- SOC 3 Type 3

8.1 Frequency and Circumstances of Assessment

None to report.

8.2 Identity/Qualifications of Assessor

None to report.

8.3 Assessor's Relationship to Assessed Entity

None to report.

8.4 Topics Covered by Assessment

None to report.

8.5 Actions Taken as a Result of Deficiency

None to report.

8.6 Communication of Results

None to report.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance/Renewal Fees

Fees payable by Subscribers are specified in the iShare Medical HISP Agreement.

9.1.2 Certificate Access Fees

Fees payable by Subscribers are specified in the iShare Medical HISP Agreement.

9.1.3 Revocation or Status Information Access Fee

No stipulation.

9.1.4 Fees for other Services

iShare Medical does not charge a Counterparty HISP a fee to exchange a Direct message on behalf of an End User.

9.1.5 Refund Policy

iShare Medical does not issue refunds related to iShare Medical HISP Subscriptions.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

iShare Medical maintains Cyber Liability Insurance, the limits vary based on the category. For Technology and Services Liability, the limits of liability are 1,000,000 per claim and in aggregate. Subscribers are encouraged to carry liability insurance.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance/Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

As used herein, the term "Confidential Information" with respect to iShare includes information which relates to iShare Medical's operations, which may or may not be in writing and may or may not be labeled "Confidential". Such information includes, but is not limited to, technical and non-technical information relating to iShare Medical's proprietary concepts and ideas, whether or not patentable, copyrights and trade secrets, plans, existing or contemplated products and services, software, research and development, data models, algorithms, illustrations, drawings, processes, devices, techniques, data and formulas, financial data, revenues, expenses, profits, pricing policies, marketing plans, customers and clients, leads, audit logs, policies and procedures related to this HPC, audit reports and related material, data center audit reports and data, business relationships, current or future business plans and models, compilations of data; marketing and organizational strategies and plans, and any information concerning the business affairs and methods of the parties which is not readily available to the public, regardless of whether such information is designated as confidential information at the time of its disclosure.

iShare Medical will not disclose, copy, distribute, sell, license, reproduce or otherwise make available Confidential Information of others without their permission or as required by laws, regulations, or other legal authority, or by this HPC Policy.

It is understood and agreed that Confidential Information is not deemed to include (a) information which is now or subsequently becomes part of the public domain through no action or fault of the disclosing party, or (b) information which was already known by the other party prior to the effective date of this HPC.

9.3.2 Information not within the scope of Confidential Information

It is understood and agreed that Confidential Information is not deemed to include (a) information which is now or subsequently becomes part of the public domain through no action or fault of the disclosing party, or (b) information which was already known by the other party prior to the effective date of this HPC.

9.3.3 Responsibility to Protect Confidential Information

All employees and contactors sign a Confidentiality and Non-Disclosure Agreement that clearly defined confidential information and its uses, iShare Medical's Proprietary and Intellectual Rights, and Property.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

iShare Medical protect private information, including PHI and PII in accordance with its policies and procedures contained in the iShare Medical HIPAA Privacy Manual and iShare Medical HIPAA Security Manual. iShare Medical Policies and Procedures are not publicly available.

9.4.2 Information Treated as Private

Information included in certificates is not deemed private.

9.4.4 Responsibility to Protect Private Information

iShare Medical securely stores all PHI, PII, and other medical information in its data centers. All data is encrypted at rest and in flight. Private Keys for Direct Messaging are created using a Hardware Security Module (HSM) and are stored, encrypted by a wrapping key that resides only on the HSM and a duplicate of the HSM, on servers in iShare's datacenter environment. Direct Message signing and decryption operations are performed on an HSM. Further, the primary HSM, and its duplicate are in geographically distinct datacenters.

9.4.5 Notice and Consent to Use Private Information

iShare Medical complies with HIPAA and will not disclose private information unless exempt, required by law, regulation or court order and in compliance with HIPAA. iShare Medical complies with applicable laws, regulations, court orders, Business Associates Agreements and/or Business Associates Subcontract Agreements regarding the notification of parties involved.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

iShare Medical complies with HIPAA and will not disclose private information unless exempt, required by law, regulation or court order and in compliance with HIPAA. iShare Medical complies with applicable laws, regulations, court orders, Business Associates Agreements and/or Business Associates Subcontract Agreements regarding the notification of parties involved.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

iShare Medical will not knowingly violate the intellectual property rights held by others.

9.6 Representations and Warranties

9.6.1 HISP Representations and Warranties

iShare Medical is provided as is and as available. No warranties are being made, express or implied. iShare Medical further assumes no responsibility or liability for any errors or omissions in the content of the information transported by iShare Medical HISP. This includes completeness, accuracy, usefulness, or timeliness of services or data.

iShare Medical is not responsible for or liable for (i) any inaccuracies of data or other information that are provided by third parties to iShare Medical for inclusion in the iShare Medical Direct Messaging content and iShare Medical Directory or (ii) any errors (e.g., typographical mistakes) by the Subscriber. Further, in no event will iShare Medical be liable for any special, indirect, incidental or consequential damages in connection with or related to the services provided hereunder. Liability of iShare Medical for claims related to this Agreement, whether in contract, tort or otherwise, will not exceed the Fees paid by the Subscriber for the services to which the claims relate.

9.6.2 CA/RA Representations and Warranties

iShare Medical uses a DirectTrust Accredited RA/CA to perform its RA and CA functions.

9.6.3 End User Representations and Warranties

Each End User represents and warrants to iShare Medical that they will:

1. Protect its Private Keys and their activation codes from compromise (including if employing a HISP who uses secure processes against potential compromise),
2. Provide accurate and complete information and communication to the HISP,
3. Confirm the accuracy of certificate data prior to using the certificate,
4. Promptly cease using a certificate and notify the HISP, CA, and/or RA if (i) any information that was submitted to the Issuer CA or is included in certificate changes or becomes misleading or (ii) there is any actual or suspected misuse or compromise of the Private Key or any password associated with the certificate or HISP account,
5. Use the certificate only for authorized and legal purposes, consistent with the relevant CPS and Subscriber Agreement, (including only installing device certificates on servers accessible at the domain listed in the certificate), and
6. Promptly cease using the certificate and related Private Key after the certificate's expiration.
7. Further, End Users that are also a Subscriber agrees to comply, when applicable, with the iShare Medical Health Information Services Provider Agreement, Provider Directory Data Sharing Agreement, Business Associates Agreement, and Business Associates Subcontractor Agreement.

9.6.4 Counterparty Representations and Warranties

Counterparty represents and warrants that they agree to the same representations and warranties as Subscribers in accordance with section 9.6.3.

9.6.5 Representations and Warranties of Affiliated Organizations

Affiliated Organizations represent and warrant that they agree to the same representations and warranties as Subscribers in accordance with section 9.6.3.

9.6.6 Representations and Warranties of Other Participants

Affiliated Organizations represent and warrant that they agree to the same representations and warranties as Subscribers in accordance with section 9.6.3.

9.7 Disclaimers of Warranties

iShare Medical is provided as is and as available. No warranties are being made, express or implied. iShare Medical further assumes no responsibility or liability for any errors or omissions in the content of the information transported by iShare Medical HISP. This includes completeness, accuracy, usefulness, or timeliness of services or data.

9.8 Limitations of Liabilities

iShare Medical is not responsible for or liable for (i) any inaccuracies of data or other information that are provided by third parties to iShare Medical for inclusion in the iShare Medical Direct Messaging content and iShare Medical Directory or (ii) any errors (e.g., typographical mistakes) by the Subscriber. Further, in no event will iShare Medical be liable for any special, indirect, incidental or consequential damages in connection with or related to the services provided hereunder. Liability of iShare Medical for claims related to this Agreement, whether in contract, tort or otherwise, will not exceed the Fees paid by the Subscriber for the services to which the claims relate.

9.9 Indemnities

Subscribers, End Users, Affiliates, Counter Parties, other Parties will indemnify and defend iShare Medical and its officers, directors, managers, members, employees and representatives against all claims and damages, including expenses and reasonable attorneys' fees ("**Claim**") to the extent arising out of its use or disclosure of protected health information hereunder.

In no event will iShare Medical be liable for any special, indirect, incidental or consequential damages in connection with or related to the Services. Liability of iShare Medical for claims related to this Agreement, whether in contract, tort or otherwise, will not exceed the fees paid by the Subscriber for the Services to which the claims relate.

iShare Medical is not responsible for or liable for (i) any inaccuracies of data or other information that are provided by third parties to iShare Medical for inclusion in the iShare Medical Direct Messaging content and iShare Medical Directory or (ii) any errors (e.g., typographical mistakes) by the Subscriber. Further, in no event will iShare Medical be liable for any special, indirect, incidental or consequential damages in connection with or related to the services provided hereunder. Liability of iShare Medical for claims related to this Agreement, whether in contract, tort or otherwise, will not exceed the Fees paid by the Subscriber for the services to which the claims relate.

9.10 Term and Termination

9.10.1 Term

This Policy becomes effective immediately upon publication. This HPC Policy has no specified term and is subject to Change and Termination in accordance with this HPC Policy document in section 1.5.4.

9.10.2 Termination

This HPC Policy is subject to Termination in accordance with this HPC Policy document in section 1.5.4.

9.10.3 Effect of Termination and Survival

The requirements of this Policy remain in effect until terminated by iShare Medical.

9.11 Individual Notices and Communications with Participants

Individual notices and communications with PKI Participants are conducted in a professional and reasonable manner based on the reason for such notice and/or communication.

9.12 Amendments

9.12.1 Procedure for Amendment

This HPC may be amended in accordance with this HPC policy document in section 1.5.4. All amendments are to be agreed upon and communicated in writing.

9.12.2 Notification Mechanism and Period

No stipulation.

9.12.3 Circumstances Under Which OID Must be Changed

No stipulation.

9.13 Dispute Resolution Provisions

This HPC shall be construed and governed by the laws of the State of Missouri. Any action or claim arising from, under or pursuant to this Agreement shall be brought in the courts, state or federal, within Kansas City, Missouri, and the parties expressly waive the right to bring any legal action or claims in any other courts. The parties to this Agreement hereby consent to venue in any state or federal court within Kansas City, Missouri for all purposes in connection with any action or proceeding commenced between the parties hereto in connection with or arising from this Agreement.

9.14 Governing Law

This HPC shall be construed and governed by the laws of the State of Missouri. Any action or claim arising from, under or pursuant to this Agreement shall be brought in the courts, state or federal, within Kansas City, Missouri, and the parties expressly waive the right to bring any legal action or claims in any other courts. The parties to this Agreement hereby consent to venue in any state or federal court within Kansas City, Missouri for all purposes in connection with any action or proceeding commenced between the parties hereto in connection with or arising from this Agreement.

9.15 Compliance with Applicable Law

This HPC shall be construed and governed by the laws of the State of Missouri. Any action or claim arising from, under or pursuant to this Agreement shall be brought in the courts, state or federal, within Kansas City, Missouri, and the parties expressly waive the right to bring any legal action or claims in any other courts. The parties to this Agreement hereby consent to venue in any state or federal court within Kansas City, Missouri for all purposes in connection with any action or proceeding commenced between the parties hereto in connection with or arising from this Agreement.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This HPS is the entire agreement and supersedes all prior HPC agreements.

9.16.2 Assignment

iShare Medical reserves the right to, at its sole discretion, assign this agreement with or without notice or consent.

9.16.3 Severability

In the event that any provision of this HPC hereof is found invalid, unlawful, or unenforceable, the remainder of this HPC Policy shall remain valid and enforceable according to its terms.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

Failure of iShare Medical to perform its obligations under this HPC will not subject iShare Medical to any liability if such failure is caused by acts of God, legal restrictions, transportation conditions, materials shortages, supplier delays, riot, sabotage, communication losses or interruptions, embargo, strikes or any other cause beyond the reasonable control of iShare Medical. Such an occurrence or interruption shall not constitute a breach of this HPC or vest in any right of damage, cancellation or rescission. iShare Medical will resume the performance of its obligations as soon as practicable after the force majeure event has ceased.

9.17 Other Provisions

No stipulation.