iShare®
MEDICAL
INNOVATING THE FUTURE OF HEALTHCARE

HISP Practice Statement
Updated March 1, 2021

Contents

iShare Medical
HISP Practice Statement
Updated October 4, 2020

About iShare Medical

iShare Medical is:

- DirectTrust Accredited Health Information Services Provider (HISP)
- EHNAC Accredited for HIPAA Privacy and Security
- EHNAC Accredited as a Trusted Network Accreditation Program Qualified Health Information Network (TNAP-QHIN).

iShare Medical uses the Direct Standard™ is method of data exchange protocol used by iShare Medical to securely and seamlessly share medical information throughout the US Healthcare System.

iShare Medical is a DirectTrust Accredited Trust Anchor, member of the DirectTrust Accredited Trust Anchor Bundle, and a DirectTrust Network Services Provider.

DirectTrust

DirectTrust is a non-profit that has established a trust framework for secure encrypted sharing of medical information across a nationwide trust network. Participating organizations undergo extensive Accreditation process that includes compliance with HIPAA and DirectTrust Policies.

DirectTrust Accredited Health Information Services Providers (HISP) can participate as a Trust Anchor in the DirectTrust Network referred to as the DirectTrust Accredited Trust Anchor Bundle (ATAB) or DirectTrust Network Services Provider.

DirectTrust also operates the DirectTrust Standards is an ANSI standards development organization for the following three standards:

- Direct Standard™
- Trusted Instant Messaging Plus Standard
- Notifications Standard

iShare Medical is a DirectTrust Accredited Trust Anchor, member of the DirectTrust Accredited Trust Anchor Bundle, and a DirectTrust Network Services Provider and participates in all three DirectTrust Standards Development Consensus Bodies.

EHNAC

The Electronic Healthcare Network Accreditation Commission (EHNAC) is a non-profit accreditation body designed to improve transactional quality, operational efficiency and data security in healthcare.

iShare Medical is EHNAC Accredited for HIPAA Privacy and Security and EHNAC Accredited as a Trusted Network Accreditation Program Qualified Health Information Network (TNAP-QHIN).

Registration Authority (RA)

iShare Medical has contracted with DigiCert, an Accredited Registration Authority (RA), to perform Registration Authority services for the iShare HISP. DigiCert is compliant with the DirectTrust X.509 Certificate Policy. Two-factor authentication is utilized to access DigiCert. Access to DigiCert is restricted to the Information System Security Officer (ISSO)

Certificate Authority (CA)

iShare Medical has contracted with DigiCert, an Accredited Certificate Authority (CA), to perform Certificate Authority services for the iShare HISP. DigiCert is compliant with the DirectTrust X.509 Certificate Policy. Two-factor authentication is utilized to access DigiCert. Access to DigiCert is restricted to the Information System Security Officer (ISSO)

Direct Addresses

iShare Medical has contracted with DigiCert to authenticate iShare Medical's customers. Individual or Organizational Level Direct addresses are issued at Level of Assurance 3 (LoA3). The certificates issued by DigiCert are bound to cryptographic keys that provide reliability an assurance of the verified identity.

The DirectTrust Accredited Trust Anchor Bundle (ATAB) operates at NIST Special Publication 800-63-2 Level of Assurance LoA3:

> "Level 3 – Level 3 provides multi-factor remote network authentication. At least two authentication factors are required. At this level, identity proofing procedures require verification of identifying materials and information. Level 3 authentication is based on proof of possession of the allowed types of tokens through a cryptographic protocol. Multi-factor Software Cryptographic Tokens are allowed at Level 3. Level 3 also permits any of the token methods of Level 4. Level 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token against compromise by the protocol threats for all threats at Level 2 as well as verifier impersonation attacks. Various types of tokens may be used as described in Section 6.
>
> Authentication requires that the Claimant prove, through a secure authentication protocol, that he or she controls the token. The Claimant unlocks the token with a password or biometric, or uses a secure multi-token authentication protocol to establish two-factor authentication (through proof of possession of a physical or software token in combination with some memorized secret knowledge). Long-term shared authentication secrets, if used, are never revealed to any party except the Claimant and Verifiers operated directly by the CSP; however, session (temporary) shared secrets may be provided to independent Verifiers by the CSP. In addition to Level 2 requirements, assertions are protected against repudiation by the Verifier."

iShare Medical accepts certificates at LoA3 or higher levels of assurance from DirectTrust Accredited Trust Anchors in the DirectTrust Accredited Trust Anchor Bundle.

iShare HISP Responsibilities

As a HISP, iShare Medical:

- Has designated one employee to act as the Information Systems Security Officer (ISSO) plus one employee, the Privacy Officer, to act as the ISSO in the event that the ISSO is unavailable for this role
- Has designated one employee as the Security Officer
- Has designated one employee as the Privacy Officer
- Assigns domain and address level for Direct Accounts
- Manages the identity and credentials of iShare customers (Subscribers)
- Stores and maintains digital certificates and associated private keys on a FIPS-140-2 Level 2 Hardware Security Module
- Associates certificates with DNS or LDAP entries
- Abides by the Accredited Trust Anchor Standard Operating Procedures
- Has published a HISP Practice Statement (SPS) for DirectTrust accreditation as a HISP
- Performs Security / Trust Agent (STA) functions for decryption of inbound messages, validation of counterparty signature, ensure outbound messages are properly signed, encrypt outbound messages, send/receive MDNs and confirm receipt of messages
- Performs trust management functions such as maintaining trust anchor store and trust policy enablement including Hardware-based signing of keys held by End Users via a FIPS-140-2 Level 2 compliant Hardware Security Module (HSM) device
- Performs Certificate discovery functions
- Provides S/MIME inbound and outbound interfaces to send to End User Direct Addresses and transmit messages from End User Direct Addresses
- Provides HISP-side of edge protocol connection including a web app and RESTful API for HISP services
- Provides Direct Address discovery including web app and RESTful API for Directory services
- Performs End User authentication
- Maintains integrity of security and trust framework, including review of security logs
- Maintains privacy of Protect Health Information

Counterparties and Intermediate Systems

A Counterparty is either an end entity that receives a Direct message sent by the HISP's End User, or end entity that sends a Direct message to the HISP's End User. iShare Medical software uses 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.

An Intermediate System is a healthcare application that communicates with a HISP on behalf of End Users such as an Electronic Health Records (EHR) or Personal Health Record (PHR). The End User of the Intermediate system is issued the X.509 certificate based upon their entity type in accordance with DirectTrust Policies such as Covered Entity or Patient. iShare Medical requires that developers of Intermediate systems sign the iShare Medical Developers Agreement for RESTful API for HISP Services prior to access to Documentation for the RESTFUL API for HISP Services. Further, all Developers are required to sign an Appropriate Business Associate Agreement or Business Associate Subcontractor Agreement. Further, all End Users of the Intermediate System must be issued a DirectTrust Compliant certificate. Intermediate Systems assume all liability for security, privacy and breach notification once the PHI is downloaded from the iShare Medical secure system.

iShare Medical uses the End User's X.509 certificate to verify the integrity of a digitally signed message, to identify the creator of the message and/or to establish secure communications with the End User.

Digital Certificates and Private Key Management

Digital certificates and wrapped (encrypted) private keys are managed via Direct Project Java implementation and stored the iShare Isolated App Server in iShare's environment at the LightEdge data center. Private Keys are assigned by the Information System Security Officer (ISSO) to the certificate at either the organizational or individual level. Private keys are generated inside of a FIPS-140-2 Level 2 compliant Hardware Security Module (HSM), wrapped with a wrapping key that is stored in side of the HSM, and stored wrapped on the app server.

Administrative access to the iShare Isolated App Server is restricted and protected by a firewall. Two-factor authentication is required for administrative access to the iShare Isolated App Server. Such access requires a PIN and a randomized 6 digit token as the two factors of authentication. The token is valid for 30 seconds, after which another token is generated. Mutual TLS is used for API authentication including username, password, and token. The iShare data center is staffed and monitored 24 / 7 / 365 by the technical staff. Ports are actively monitored. Vulnerability scans are run daily.

The HSMs are mirrored between two data centers, one located in Kansas City, Missouri and another located three and a half hours north of Kansas City in Altoona, Iowa (a suburb of Des Moines). iShare Medical can fail-over between HSMs located in geographically separated locations.

Encryption and Decryption

Per the Direct Standard™, transportation of data is encrypted. The wrapping key for decrypting the private keys for the purpose, in turn, of decrypting inbound Direct Messages is stored on FIPS-140-2 Level 2 compliant Hardware Security Modules (HSMs). In order to decrypt a Direct Message, the appropriate key is the opened inside of the HSM and unwrapped by the wrapping key inside of the HSM. The decryption of the message occurs inside of the HSM. Furthermore, encryption of outbound messages also occurs inside of the HSM. Private keys are NOT stored unencrypted outside of the HSM. Encryption and decryption of messages does NOT occur outside of the HSM.

HISP Services for Covered Entities

iShare Medical has entered into a business associate agreement with covered entities or business associates sub-contract agreement to provide HISP services.

iShare Medical Complies With HIPAA Privacy Rule

iShare Medical complies with the HIPAA Privacy Rule. iShare Medical's privacy policies are documented in the iShare Medical Privacy Policy Manual. iShare Medical is EHNAC Accredited for HIPAA Privacy and Security

iShare Complies With HIPAA Security Rule

iShare Medical complies with the HIPAA Security Rule. iShare Medical's security policies are documented in the iShare Medical Security Policy Manual. iShare Medical is EHNAC Accredited for HIPAA Privacy and Security

Compliance With DirectTrust HISP Policy and Trusted Exchange

DirectTrust is a framework built on a set of standards and policies. iShare Medical agrees to comply with the DirectTrust HISP Policy Statement as published at www.directtrust.org. iShare Medical is a DirectTrust Accredited Health Information Services Provider (HISP), member of the DirectTrust Accredited Trust Anchor Bundle (ATAB), and a DirectTrust Network Services Provider.

iShare Medical performs bi-directional exchange of medical data with DirectTrust Accredited Health Information Services Providers who are member of the Accreditation Trust Anchor Bundle.

DirectTrust Accredited Health Information Services Providers in the Accreditation Trust Anchor Bundle that do violate the DirectTrust Polices will be "blacklisted" and reported to the DirectTrust organization. "Blacklisted" means that iShare Medical will mark the HISP as not trust worthy and will no longer exchange data with the HISP. A "Blacklisted" HISP may be removed from the "Blacklist" upon providing compelling evidence that the HISP is now complying with the DirectTrust Policies.

Authentication User Log-in and Time Out

Each iShare Medical customer or end user has access to one and only one account based on their role. This is enforced in part through the use of two factor authentication which occurs with each log in. The two factors are user name and password and randomly generated single use pin that is texted to the users' cell phone and valid for approximately one minute or in the case of the API via Mutual TLS Token. Users are automatically logged off for inactivity for a period of 15 minutes.

Amendments to this Statement

iShare Medical reserves the right to amend the HISP Practice Statement as needed.

iShare Medical Trademark

iShare Medical® is a federally registered trademark of iShare Medical, LLC.

iShare Medical LLC

iShare Medical is a limited liability company whose corporate headquarters are located at:

iShare Medical LLC
6320 Brookside Plaza, Suite 248
Kansas City, Missouri 64113

Prepared By

This document was prepared by iShare Medical President / CEO Linda Van Horn, MBA and by iShare Medical ISSO and Sr. Database Architect, Michael Mall, BS.