SOUTH DAKOTA

HealthLink

Exchanging information. Changing lives.

Direct Implementation Guide

For questions about these policies, contact the Executive Director of South Dakota Health Link (executive-director@sdhealthlink.org).

Revision Log

Date	Revision Type	Summary	Lead Author
January 9, 2023	Created		Lance Jahnig

Table of Contents

Direct Messaging Implementation

Direct Messaging is a simple, powerful solution that makes provider-to-provider communication across care communities as quick and easy as sending an email. With the confidence of knowing that protected health information stays protected. For more information about Direct see Appendix A below.

The following are the steps to implement Direct messaging with South Dakota Health Link (SDHL). The following need to be completed before the organization can begin the implementation.

1. Sign Participation Agreement with SDHL
2. Complete the Direct Certificates form, Information needed include:
    a. Organization information
    b. Organization contact information
    c. Signature
    d. One approved government-issued photo ID
    e. Notarized
3. Provide name to be used in the domain name of the address
4. XDR Connections will need to provide the endpoint and authentication certificate

Once the organization has completed all the above, the creation of the Direct address will begin. After the creation of the domain, training will be provided to create additional addresses if needed. The organization will be given access to the web portal for sending and receiving messages.

If using an XDR connection to the EMR/EHR for sending and receiving Direct messages, the SDHL endpoint and certificate will be provided. A call will be scheduled to complete the setup. After the call both the organization and SDHL will monitor to validate the connection is working correctly.

Appendix A - Direct Messaging Services*

***Applies only to those using SDHL Direct Messaging Services.**

Overview

SDHL has incorporated a set of rules to which a Health Information Service Provider (HISP) member would agree in order to be trusted by another HISP member within a privacy policy framework set by ONC. Note that a HISP member must agree to SDHL policies and agreements in order to be part of the HISP. Connectivity to other HISPs will only be done with other accredited DirectTrust members.

Definition

A Health Information Service Provider (HISP) is a role in a Direct message exchange that provides edge protocols, message formatting, security, and routing according to the Direct project specification. A HISP also provides trust-store management tools and services for members. The HISP member may be providers, payers, EHR vendors, PHR vendors, health information exchanges, and third-party entities.

Role

The Health Information Service Provider (HISP) shall provide services to a variety of organizations including providers, payers, EHR vendors, PHR vendors, health information exchanges, and other HISPs. The Direct Project developed a set of specifications to enable a secure, scalable, standards-based mechanism for universal transport and addressing that every HISP must follow. The consensus obtained during this process is expressed in the Applicability Statement for Secure Health Transport and includes (but is not limited to) use of X.509 certificates, S/MIME, MDNs, RFC5322 payload formatting, email-like endpoint addresses, and an SMTP backbone protocol. Consensus was also achieved within the XDR and XDM for Direct Messaging specification for use of XD metadata with XDR and XDM as well as conversion mechanisms for data traversing both XDR and SMTP.

Goal

The goal of Direct is to achieve universal information exchange and interoperability between HISPs within the confines of a trust model. As real-world pilot implementations of direct exchange have taken hold, a desire has been expressed for additional clarity and agreement in areas that go beyond the specifications listed above, in order to ensure that HISPs will be able to assess the trust-worthiness of other HISPs. Trust between HISPs is essential if direct addresses are to have confidence that their messages will be received consistently and reliably. Specifically, these areas include:

1. Security profile of HISP edge protocols.
    - Authentication and privacy mechanisms utilized up to the S/MIME.
    - Privacy (encryption) of data at rest.
2. Certificate discovery/directory mechanisms.
    - The Applicability Statement recommends Domain Name System (DNS) as one option for certificate discovery.
    - Specific qualifiers that either contribute to, or detract from, trust-worthiness of a HISP that uses DNS
3. Judging the trustworthiness of a Certificate Authority and Registration Authority associated with a HISP.
    - Certificate Policy and Certificate Practices Statements (including identity verification practices) – RFC 3647
    - WebTrust seal, ETSI certification, or FBCA cross-certification
    - HIT Policy Committee recommendations
    - Evaluation Criteria for Trust Anchors and Certification Authorities
4. Identity verification of patients versus providers.
5. Transparency and public disclosure requirements for HISPs.

HISP Policy

HISPs Serving Healthcare Organizations

It is the responsibility of the HISP member to provide intuitive tools and knowledge within a healthcare organization/individual that allows it to implement a trust policy consistent with security policies and within the capabilities of the Direct Project PKI architecture. To reap the benefits of secure but ubiquitous communication, healthcare organizations/individuals should codify trust by, possibly, adding trusted root certificates to its users' Direct Project trust stores. Healthcare organizations should not use the Direct Project PKI trust store to enforce business policies above and beyond those dealing with privacy and authentication of Direct Project messages.

A healthcare organization/individual that is a HIPAA covered entity will either provide HISP services within its network or execute a HIPAA Business Associate Agreement (BAA) with a third-party HISP. Either way, all PHI retention, use, disclosure, security, and access will follow HIPAA guidelines for a covered entity.

A healthcare organization/individual that is not a HIPAA covered entity will either provide HISP services within its network or execute a BAA with a third-party HISP that is materially equivalent to a HIPAA BAA. Either way all PHI retention, use, disclosure, security, and access will follow guidelines equivalent to those required of a HIPAA covered entity.

A Direct address contains a domain component that may be rooted at the HISP (e.g., OrganizationName@OrganizationName.sdhealthlink.net) or may be independent of the

HISP (e.g., Provider@OrganizationName.sdhealthlink.net). Should the user decide to switch to a different HISP, choosing the latter option allows them to do so without changing his Direct domain/address. HISPs should allow a provider to use their own domain (and certificate) if desired.

When a healthcare organization is issued an organizational Direct certificate, then HIPAA best practices should be followed by the healthcare organization in determining the appropriateness of assigning Direct addresses to its members (all of which will use the same Direct organizational certificate for S/MIME signature verification and encryption).

A HISP member should not use an organizational certificate to represent more than one distinct organization. A HISP member should not use an individual certificate to represent more than one distinct healthcare individual. For example, if a third-party HISP provides service to 20 distinct hospitals (legal entities), each hospital should be associated with a different organizational certificate.

Any HISP member who wishes to change their domain address may be subject to change fees or other costs associated with the change.

HIPAA and Legal Agreements

Because the HISP is a separate business organization from the sending and receiving organization, there are some functions that should be enforced through contract law, in addition to those enforced by Federal, State and local laws and regulations.

In many cases, HISPs may be required to have Business Associate Agreements (BAAs) with HIPAA Covered Entities. In cases where BAAs are not strictly required (for example, because the sender or receiver is not a Covered Entity), coverage under similar agreements is essential to provide the equivalent safeguards and protections provided under contractual law to those provided by BAAs for Business Associates of Covered Entities.

HIPAA provides legal safeguards and clear requirements for Individuals (patients/consumers) and Covered Entities, as defined in HIPAA. There are some participants that will desire to participate in directed exchange but will not meet the legal triggers for Covered Entity status. Including such participants in directed exchange without ensuring the same legal safeguards provided under HIPAA is problematic. HIPAA extends privacy safeguards and protections to apply to Business Associates of Covered Entities. Directed exchange of Personally Identifiable Information (PII) that involves intermediaries or third parties that are not Business Associates or covered by equivalent protections is likewise problematic, unless separate mutual contracts are in place to protect privacy, security and transparency. Because a model that requires mutual contracting is not operationally scalable, it is desirable to limit exchange to entities that have clear recognized responsibilities under HIPAA.

Exchange of data protected by strong encryption over the open Internet using pure routing functions (e.g., TCP/IP switching, SMTP servers handling encrypted data) generally does not need these levels of protection so long as the routing organizations do not have access to the decryption keys.

Directed exchange where participants have access to unencrypted data or could have access to unencrypted data (because they hold decryption keys for encrypted data) must involve Individuals, Covered Entities and Business Associates (using those terms as defined by HIPAA) OR organizations that have strong legally enforceable contractual obligations that provide equivalent protection for individuals to those provided by HIPAA.

By noting "equivalent protection," we recognize that the investigational powers and remedies available in contractual law do not equal those available to the Federal Government under HIPAA.

Information Security

The ability to protect PHI through strong information security is critical to establishing trust in directed messaging. There are well-established best practices in information security across multiple industry contexts that are available for HISPs to follow.

The HIPAA Security Rule establishes uniform national standards for information security. The security rule applies to Covered Entities, and, by extension to Business Associates; Meaningful Use also requires compliance to the HIPAA Security Rule. At a more detailed level, information security guidelines have been developed to protect cardholder data for financial transactions, in the PCI Data Security Standards (PCI-DSS); many of the detailed requirements for that purpose have broad applicability to health care as well.

Regardless of legal requirements, all HISPs will hold themselves to the provision of the HIPAA Security Rule, and, to the extent that it is relevant and consistent with the Security Rule, will follow the guidelines of PCI-DSS.

Some HISPs might maintain private keys as well as public certificates, and will use those private keys to manage trust on behalf of providers, provider organizations, or other participants in health information exchange. This implies a high degree of trust that must be protected with a high degree of security.

HISPs that manage private keys must perform specific risk assessment and risk mitigation to ensure that the private keys have a strong protection from unauthorized use. That risk assessment must address the risk of internal personnel or external attackers gaining unauthorized access either to the keys or to the health information functions for which the keys enforce trust. Some HISPs will manage trust anchors on behalf of their customers. This is a critical aspect of trust, and must be managed well to avoid compromise on strong assurance of identity.

HISPs that manage trust anchors on behalf of their customers must be an accredited DirectTrust member.

Transparency of Healthcare Information

Any HISP that manages, transforms or performs value-added services PHI has an obligation to make the extent of data use and other activities clear and transparent. Transparency initiatives should focus on both quality and cost. Empowering consumers to make health care decisions based on quality information should be a critical part of the discussion on health care transparency.

Health information transparency enhances the appropriate use and quality of healthcare, and it helps in cost management by enabling informed decision-making. HIT based on broadly accepted standards, allows patients, healthcare providers and health plans to share information securely, driving down costs by avoiding duplicate procedures and manual transactions.

HISP Direct Email Services

Using Direct will not require that providers implement software. Instead, the process for sending information is similar to sending e-mail today.

First a physician would contract with a HISP, such as SDHL that has decided to offer Direct as one of its exchange services. SDHL HISP would assign the physician a Direct e-mail address.

To use Direct, the physician would log into his or her HISP Direct gateway via the Internet and use his or her Direct e-mail address to send information to another provider who also has a Direct e-mail address. Information can only be sent to other providers using the Direct service.

Deployment Models

The deployment models associated with use of Direct Project specifications allow, under control of the sender and receiver, for the locus of encryption/decryption activities to take place either at the sender or receiver or with a separate party under an appropriate contractual relationship with the sender or receiver.

Preconditions

The sender and receiver have ensured that agents of the sender and receiver (for example, HIO, HISP, intermediary) are authorized to act as such and are authorized to handle protected health information according to law and policy.

Direct Messaging

Direct messaging is secured with appropriate level of encryption; HISP members must be approved to join the HISP and have a valid digital certificate in order to exchange messages within the HISP network.

DirectTrust

SDHL is a member of DirecTrust. DirectTrust is a vibrant and collaborative non-profit alliance of health IT and health care provider organizations who have joined forces to support secure, interoperable health information exchange via the Direct Message Protocols. SDHL will consider connections with HISPs outside our network who are also DirectTrust members.

HISP-to-HISP

All HISP-to-HISP connections will be made in accordance with DirectTrust policies and procedures available at www.directtrust.org. All HISP's connecting to South Dakota Health must be a DirectTrust member.

Certification Authority

SDHL uses Health Catalyst's HISP services. Digicert is Health Catalyst's Certificate Authority. The Cetificate Policy and Certificate Practice Statement are available on Digicert's site at https://www.digicert.com/legal-repository/. The DirectTrust Community X.509 Certificate Policy can be found on Digicert's site at https://www.directtrust.org/resources/compliance-and-key-policies. DirectTrust maintains a list of all the accredited HISP's and their Certificate Authority Certificate Policy at the following site https://directtrust.org/about-membership/member-list.

Registration Authority

Registration Authority Overview

Registration Authority (RA) is defined as an entity that is responsible for identification and authentication of certificate subjects. The RA function for their participants shall be conducted by SDHL HISP.

SDHL RA is responsible for ensuring the eligibility of a member with the accuracy and integrity of required information presented by the member.

The guidance contained in this document takes into consideration that joining members have met the common minimum requirements for RA services.

Registration Authority Requirements

SDHL HISP serves as a RA for their participants. RA is the entity that enters into an agreement with a Certification Authority (CA) to collect and verify each participant's identity and information to be entered into the public key certificate. The HISP RA performs its function in accordance with SDHL CA Policy and the Certificate Practice Statement (CPS), and any other relevant agreements or policy documents. Minimum activities that shall be conducted by the RA include:

1. In-person proofing
2. Verification and validation of identity documents
3. Enrollment and registration
4. Credential issuance
5. Credential usage
6. Credential revocation
7. Post issuance updates and additions
8. Credential re-issuance

The RA is responsible for the standards, training, oversight and audit of the RA entities operating at the direction of SDHL HISP. As such, the RA ensures that the approved Participant is in material compliance with SDHL policies and agreements at all times. The RA shall ensure that timely corrective action is taken to address any RA entities deficiency, including the termination or suspension of specific RA entity duties, when warranted.

Registration Authority Roles and Responsibilities

SDHL HISP serves as an RA for all HISPs joining the HISP community in order to allow simple, secure movement of health information between HISP participants.