Direct: Implementation Guidelines to Assure Security and Interoperability
May, 2013

Purpose of these Guidelines

ONC is releasing these guidelines— an update of prior programmatic guidance issued for the State HIE Program— to provide recommended policies and practices for health information service providers (HISPs), trust communities and accrediting bodies, such as DirectTrust. Adoption of these policies and practices will give providers and other stakeholders' confidence that Direct is being implemented in a way that will support vendor to vendor exchange and interoperability. The document reflects consensus reached at the Direct Scalable Trust Forum convened by ONC in November, 2012. For more background, please see Appendix A at the end of this document.

ONC believes that adoption of these consensus policies and practices by voluntary accreditation programs and trust communities and widespread HISP participation in those programs, such as DirectTrust, will enable providers to easily and securely exchange patient health information using Direct irrespective of organizational and vendor boundaries to meet Stage 2 Meaningful Use exchange requirements and overall care coordination needs.

ONC strongly encourages HISPs providing Direct services to providers and hospitals for Meaningful Use Stage 2, as well as ONC grantees and their HISP partners, to conform to these policies and practices and participate in accreditation programs and/or trust communities that adopt them.

Application of the Guidelines

In using this guidance, HISPs and associated accreditation bodies and trust communities should keep in mind that the fundamental trust basis for Direct exchange is between the initiating sender and the final receiver of information (not between HISPs). A common set of policies will let HISPs automatically recognize each others' certificates and provide confidence that information will be securely routed to the right recipient, but a provider will ultimately still need to decide to send/receive information to/from another party for patient care or for other reasons allowable under the Health Insurance Portability and Accountability Act (HIPAA).

It should also be noted that these policies and practices are recommended to support provider to provider exchange. Providers will also need to be able to exchange information with patients and their HISPs, regardless of whether those patient-facing HISPs follow these specific policies. A separate "Blue Button" certificate anchor bundle has been developed for that purpose.

ONC also recognizes two related but distinct roles in enabling Direct exchange (which are covered separately by this guidance, though a single entity may perform both roles):

1. Security and Trust Agents (STAs) (which is software that may be operated by a healthcare entity, or—most commonly—by a 3rd party entity known as a Health Information Service Provider or HISP) facilitate Direct exchange services.

2. Registration Authorities (RA) establish the identity of certificate subjects and Certificate Authorities (CA) issue certificates. The functions of an RA and a CA in a given implementation may be performed by a single entity or by multiple entities.

Recommended STA/HISP Guidelines

All STAs/HISPs[1] should:

1. Conform to all of the requirements specified in the Applicability Statement for Secure Health Transport v1.1 and (if implementing) the XDR and XDM for Direct Messaging v1.0 specifications.

2. Determine whether they are business associates (BAs) and hold themselves to the provisions of the HIPAA Security Rule, as amended by the HITECH Act, that are applicable to BAs.

3. Have contractually binding legal agreements with their clients (who send and receive Individually Identifiable Health Information [IIHI] using Direct), including all terms and conditions required in a Business Associate Agreement (BAA).

4. Demonstrate (through either availability of a written security audit report or formal accreditation provided by an established, independent third-party entity) conformance with industry standard practices related to meeting privacy and security regulations in terms of both technical performance and business processes. In particular:

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

    - HISPs that manage trust anchors on behalf of their customers -- should have well defined, publicly available policies that permit customers and other parties to evaluate the certificate issuance policies of those trust anchors.

5. Minimize data collection, use, retention and disclosure to that minimally required to meet the level of service required of the HISP. To the extent that HISPs support multiple functions with different requirements for data use, they must separate those functions such that more extensive data use or disclosure is not required for use of more basic (Direct) exchange services.

6. Issue Direct addresses only to organizations and/or individuals[2] that have had their identity verified according to NIST Level of Assurance 3 requirements, at a minimum, through in-person or remote options.

7. Follow Federal Bridge Certification Authority (FBCA) Basic (or equivalent) policies and practices for all certificate issuance and management matters beyond identity verification.

---

1 Many different entities will serve in STA and HISP roles as Meaningful Use Stage 2 is implemented. Guidelines for STAs/HISPs apply to the wide variety of implementation approaches, including EHR vendors serving as HISPs and provider organizations serving as STAs

2 The term "individual" in the context of these guidelines refers to health care-related professionals and is not meant to include patients.

8. Only facilitate the exchange of Direct messages that utilize Direct addresses and digital certificates which *at least* meet the requirements below in the Recommended RA/CA Guidelines section. In particular, Direct certificates must:

    - Conform to the requirements set forth in Applicability Statement for Secure Health Transport v1.1. Direct certificates are used only for transport and not for identity verification or non-repudiation.

    - Have been issued to a health care related organization or more granular component of an organization (e.g., department, individual). One certificate issued to a HISP to use on behalf of all participants in the HISP does *not* meet this criterion.

9. Authenticate and encrypt all edge protocol communications that enable 'last mile' exchange between end-users' systems and an STA/HISP's Direct infrastructure by using SSL/TLS or similar industry standard.

10. Provide users with mechanisms to directly establish trust with another user (e.g., store the public key) to enable ad-hoc messaging even if the respective HISPs have not "white listed" each other.

11. Support the Implementation Guide for Direct Project Trust Bundle Distribution v1.0, which provides a common and automated mechanism for exchanging trust anchors between HISPs.

In addition to the security and trust measures listed above, we recommend that HISPs also implement the following guidelines to enhance interoperability:

12. Implement the XDR and XDM for Direct Messaging v1.0 specifications in order to support Direct-ready EHR vendor implementations using this deployment pattern.

13. Implement the specifications in the Implementation Guide for Delivery Notification in Direct v1.0 in order to support use cases that require greater message delivery assurance.

Recommended Registration Authority and Certificate Authority Guidelines

1. Specifically with respect to identity validation, RAs, CAs and any other entities performing RA functions should ensure that representatives of organizations that are being issued certificates and individuals that are using HISP services are identity proofed at the NIST Level 3 of Assurance (as specified in NIST SP 800-63-1, dated December 2011). The identity of the applicant must be established no earlier than 30 days prior to the initial certificate issuance or use of HISP services.

    - For individual end-users: identity is established by in-person or remote proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities (such as a notary public).

- For in-person proofing[3]: possession of verified current primary Government Picture ID that contains Applicant's picture and either address of record or nationality of record (e.g., driver's license or passport).

- For remote proofing: possession of a valid Government ID (e.g., a driver's license or Passport) number and a financial or utility account number (e.g., checking account, savings account, utility account, loan or credit card) confirmed via record checks of both numbers.

- All credentials must be unexpired.

- For organizations: Identity is established by 1) verifying (per the individual end-user criteria listed above) the identity of the requesting representative (from the Information Systems Security Office or equivalent) of the organization and the representative's authorization to act in the name of the organization, and 2) verifying the organization's name and address, as well as documentation of the existence of the organization.

  - In addition to NIST/FBCA requirements, an organization participating in a HISP must be a HIPAA covered entity, a business associate of a HIPAA covered entity, or be a person or organization who is involved in health care related activities and who agrees to hold themselves to the same security requirements as provided in the HIPAA Security Rule.

2. CAs should either 1) be cross-certified to the Federal Bridge Certification Authority (FBCA) and issue FBCA Basic (or higher) cross-certified certificates or 2) adhere to policies and procedures equivalent to FBCA Basic for all matters related to certificate issuance and management.

   In particular, the CA should issue certificates that:

   - Do not have non-repudiation flag set

   - Conform to other requirements set forth in the Applicability Statement for Secure Health Transport v1.1

   Important: if a HISP/CA opts to not issue FBCA cross-certified certificates, health care providers using the certificates will likely be unable to engage in Direct exchange with Federal agencies. Additionally, Federal agencies may have specific implementation and use requirements to meet Federal security policies, such as higher assurance levels or separate certificates for encrypting and signing Direct messages for transport (separate certificates will be required for encryption and signing after 12/31/2015).

[3] A trust relationship between the Trusted Agent and the applicant, which is based on an in-person antecedent, may suffice as meeting the in-person identity proofing requirement. Clarification on the trust relationship between the Trusted Agent and the applicant, which is based on an in-person antecedent identity proofing event, can be found in the "FBCA Supplementary Antecedent, In-Person Definition" document.

Appendix A. Background

ONC has found that many Health Information Service Providers (HISPs) are deploying Direct in a way that proactively enables exchange within a given HISP's boundaries while not offering mechanisms or supporting policies that enable exchange with other HISPs. Such limitations effectively block providers using different HISPs from exchanging patient information. In effect, HISPs are creating "islands of automation using a common standard." This will hamper information following patients where they seek care—including across organizational and vendor boundaries—to support care coordination and Meaningful Use Stage 2 requirements.

The technical and policy challenges of exchange across HISPs were well-described in the report summarizing the results of the ONC-convened Direct Scalable Trust Forum[4]:

> *There are special privacy and security concerns when transporting health information, which is both sensitive and protected by law, due to an insecure network like the Internet. To effectively address these concerns, the Direct Project specification (hereon referred to as Direct) uses public key infrastructure (PKI)[5] to protect information exchanged via the Internet through X.509 digital certificates and public/private keys. This means that Direct users (organizations or individuals) cannot send or receive information to or from other Direct users until they have established trust. The process of establishing trust between users involves three basic steps:*
>
> 1. *Users must determine that they want to send information to and/or receive information from the other user.*
>
> 2. *Users must have a way to discover each other's public keys (per the Direct Project's Applicability Statement) so that messages and attachments can be decrypted.*
>
> 3. *Users must store each other's trust anchors for use in assuring the validity of each other's public keys prior to use. Trust anchors can be either the public keys associated with users or, more likely in today's implementations, the root certificates[6] associated with those public keys.*
>
> *From a technical perspective, this process can occur several different ways and is relatively simple when Direct users are subscribed to messaging services from the same*

[4] The full Direct Scalable Trust Report is available at http://www.healthit.gov/policy-researchers-implementers/health-information-exchange-governance

[5] PKI is 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 certificates.

[6] A root certificate is an X.509 certificate issued by a Root Certificate Authority and used to verify the digital signatures associated with all certificates issued by the HIDP. A root certificate is the top-most certificate of the tree structure of certificates, the private key of which is used to "sign" other certificates. A root certificate is a self-signed certificate that identifies the Root Certificate Authority.

service provider. However, when users do not share the same system there needs to be a mechanism for exchanging trust anchors and agreement on whatever set of policies are required as a precondition for that exchange. These policy and operational considerations are not addressed by Direct's technical specification and involve a variety of stakeholders (such as certificate authorities, registration authorities, service providers, technology vendors, health care organizations, etc.). To enable seamless point-to-point information sharing, implementers must collaborate on elements beyond the basic technical specification, including establishing consistent policies and practices on which all stakeholders agree.

To address these challenges, some HISPs have executed peer-to-peer legal agreements and then have exchanged and loaded trust anchors, giving their respective users a way to exchange Direct messages with each other. Unfortunately, such peer-to-peer legal agreements have proven to be expensive and time-consuming to implement and are cumbersome to monitor and enforce. They are not a realistic long-term basis for vendor to vendor exchange.