Implementation Guidelines for State HIE Grantees on
Direct Infrastructure & Security/Trust Measures for Interoperability

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."

To address these challenges, some HISPs have begun using DURSA-like agreements to enable providers using different HISPs to exchange Direct messages. Once an agreement is executed, HISPs allow their respective users to seamlessly exchange messages. Unfortunately, such peer-to-peer legal agreements are expensive and time-consuming to implement and are cumbersome to monitor and enforce. They are not a realistic long-term basis for scalable trust.

Ultimately, it is hoped that Nationwide Health Information Network (NwHIN) Governance, by providing common rules of the road and a voluntary validation process, can alleviate the perceived need for peer-to-peer legal agreements among and between HISPs. In the meantime, grantees have asked for common policies that can be immediately adopted across the more than 40 states that are implementing Direct in order to:

- Give providers and other stakeholders confidence that Direct is being implemented according to specifications and will support widespread exchange and interoperability
- Encourage consistent standards of practice among HISPs to support confidence and interoperability
- Enable the development of trust communities across HISPs, including at the regional or state level

This document outlines recommended policies and practices for grantees implementing Direct. Grantees should encourage their HISP partners to conform to these common policies and practices and establish interoperability with other HISPs using them.

In using this guidance, grantees should keep two considerations in mind:

1. The fundamental trust basis for directed exchange is between the initiating sender and the final receiver (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).
2. This guidance is offered to support grantees' Direct implementations that are being deployed now and over the next few months. The specific policies and standards may need to be adjusted to mirror the requirements of NwHIN Governance once they are established through regulation.

The State HIE program recognizes two related but distinct roles in enabling directed exchange (which are covered separately by this guidance, though a single entity may perform both roles):

1. Security and Trust Agents (STAs) (also known as Health Information Service Provider or HISPs) facilitate Direct exchange services.

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

Recommended STA/HISP Guidelines

All STAs/HISPs should:

1. Conform to all of the requirements specified in the Applicability Statement for Secure Health Transport and (if implementing) the XDR and XDM for Direct Messaging specifications. In addition, STAs/HISPs should implement the Certificate Discovery for Direct Project Implementation Guide (which is anticipated to be included in a revised version of the Direct Project's Applicability Statement soon).

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 more basic (Direct) exchange models.

6. Only facilitate Direct messages that utilize digital certificates which:
    - Have been cross certified to the Federal Bridge Certification Authority (FBCA)
    - Conform to 'medium' level of identity assurance for the selected certificate type
    - Do not have non-repudiation flag set
    - Conform to other requirements set forth in Applicability Statement for Secure Health Transport

- 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.

7. 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.

8. 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.

9. Enable the XDR and XDM for Direct Messaging specifications in order to support Direct-ready EHR vendor implementations using this deployment pattern.

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 individuals and organizations are identity proofed at the medium assurance level (as specified in FBCA X.509 Certificate Policy for the Federal Bridge Certification Authority Dec. 9, 2011). The identity of the applicant must be established no earlier than 30 days prior to the initial certificate issuance.

    - For individual end-users: identity is established by in-person 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) using federal government-issued photo ID, a REAL ID Act compliant photo ID or two non-federal IDs, one of which is a photo ID (e.g., Non-REAL ID Act compliant Drivers License). All credentials must be unexpired. 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

    - For organizations: As set out in the FBCA Certificate Policy, identity is established by a representative of the organization (from the Information Systems Security Office or equivalent) providing the organization name, address, and documentation of the existence of the organization. In addition to verifying this information, the RA must verify the authenticity of the requesting representative (at the medium level of assurance) and the representative's authorization to act in the name of the organization to control of the organization's group certificate private key.

In addition to the FBCA requirements listed above:

- 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 be cross-certified to the Federal Bridge Certification Authority (FBCA) and issue/utilize a certificate policy (CP) and certificate practice statement (CPS) that conforms to FBCA cross-certified requirements.

In particular, the CA should issue certificates that:

- Are cross certified to the Federal Bridge Certification Authority (FBCA)
- Conform to identity assurance criteria as listed above in #1
- Do not have non-repudiation flag set
- Conform to other requirements set forth in Applicability Statement for Secure Health Transport

Note: the RA/CA guidelines and requirements listed above are intended to apply to health care-related organizations and individual providers (i.e., those transferring others' health information), ***not*** *consumers / patients (i.e., those transferring their own health information).*