WEDI Healthcare Secure Messaging Workgroup

15 things to know about DIRECT messaging

DIRECT messaging is one type of secure messaging that is generally recognized as an effective secure encrypted communication mechanism for use in the point-to-point exchange of sensitive clinical and administrative data. This document provides an overview of Direct messaging from the perspective of the Direct Project and its efforts to establish an industry agreed upon standard protocol to allow exchange of information depending on user preference, across an organization, country and/or the world.

1. **What is Direct?**
   "Direct is a technical standard for exchanging health information between health care entities (e.g. primary care physicians, specialists, hospitals, clinical labs) in a trusted network. It is secure, easy-to-use, inexpensive, and approved for use by nationally recognized experts and organizations. Direct messaging functions like regular e-mail with additional security measures. Direct ensures that messages are only accessible to the intended recipient, per the privacy and security regulations of the Health Insurance Portability and Accountability Act (HIPAA)". Access the Direct Basics: Q&A for Providers on HealthIT.gov for more information.

2. **What was the Direct Project?**
   The Direct Project was a public-private sector initiative sponsored and run by the Office of the National Coordinator (ONC) whose aim was to create a simple, secure, and open standard for transport of messages and attachments between health care participants over the Internet, regardless of end-user technology.

   At its core, the Direct Project was started in an effort to provide simpler methods to encourage health information exchange. The method chosen was discussed and approved through consensus within the Direct project and became the underlying basis for future Direct efforts (including DirectTrust). This is known as Direct email, which is a concept predicated on the use of a common email standard (SMTP) with additional security mechanisms.

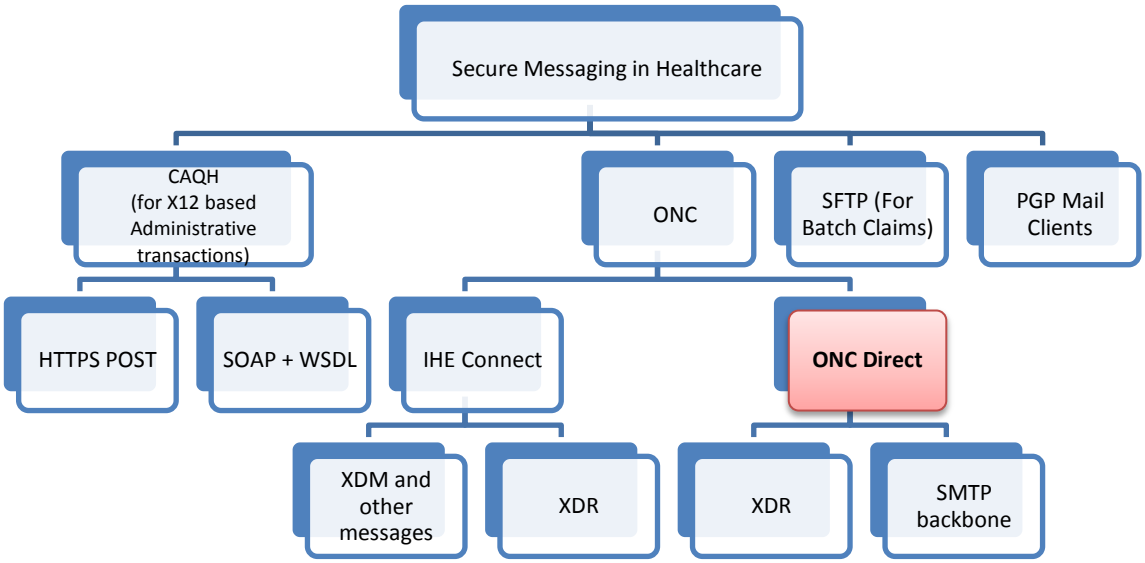
   The objectives of the Direct Project include defining:
   - Terminology used in secure messaging, including the communications and security standards implemented.
   - Terminology surrounding the Direct Project
   - Terminology associated with Direct Trust

3. **What is a Direct Address?**
   The Direct standard requires the use of a Direct address. A Direct address is similar to a typical email address which can be issued to an individual, organization or machine but is different because a Direct Address serves as a *secure* messaging system that provides for identity management and message encryption to enable the secure sending and receiving of personal health information and other sensitive communication exchange. Typical email accounts, do not encrypt messages and the identify management process that includes

simply a log in with a password does not provide enough security to confirm the identity of the sender and receiver.

4. **Is Direct messaging required for Meaningful Use Stage 2?**
   Direct exchange is not the only way that providers can meet the health information exchange requirements of Stage 2 Meaningful Use, SOAP-based optional transport standard capability is also permitted. However, since all certified EHR technology must enable use of Direct exchange, Direct may be the easiest messaging solution to deploy. Visit http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html for more information regarding Stage 2 Meaningful Use requirements.

5. **What is the difference/similarity between Direct and Secure Messaging encrypted transport standards?**
   Secure messaging is a web-based message system for managing and exchanging encrypted, messages that may contain sensitive information with a variety of stakeholders, such as physicians and other providers, payers, nurses, members and others. ONC Direct protocol is one type of secure messaging. ONC Direct protocols are required under Meaningful Use definitions driving EMR certification necessary to qualify for federal reimbursement under HITECH EMR incentive programs. It currently requires support for SMIME/SMTP and permits the deployment of XDR/SOAP (an IHE construct promoted under the interoperability enablement investments made by ONC to support Web Services deployments of connected EMR's).



6. **How do I sign up and obtain a Direct Address?**
   Direct addresses can be obtained from current vendors in which you have a relationship. For example, EMR vendors, Health Information Exchanges, Health Information Service Providers

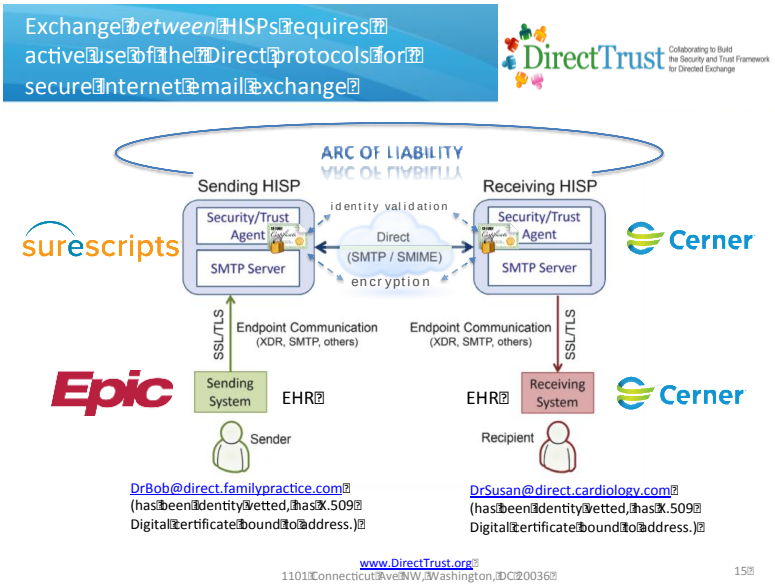
(HISPs) that provide DIRECT capability are good sources to request a DIRECT address. See Certified Health IT Product List for certified EMR's, State Health Information Exchanges at Health IT and EHNAC-DirectTrust Direct Trusted Agent Accreditation Program (DTAAP) listing for entities that provide DIRECT capability.

7. How can I use my Direct Address?

According to HealthIT.gov, "the Direct standard uses strong security to protect communications (just like trusted internet interactions with financial institutions, online retailers, and other secured websites)". For this reason, "certain steps may need to be taken to start exchanging information with a message recipient to ensure that they are a trusted connection. There are a few important points to note on establishing trust with message recipients:

1. Based on the sender's system or the message recipient's system, the sender may be required to indicate their wish to send and/or receive information from the other message recipient.
2. Depending on the EHR and/or HISP the sender and receiver are using, assistance from their vendor to establish this trusted relationship will be needed.
3. Some work between the two vendors may be required in order to communicate. If you have questions about communicating with another recipient, check with the EHR vendor or Direct HISP as a first point of contact."

Access the Direct Basics: Q&A for Providers on HealthIT.gov for more information.



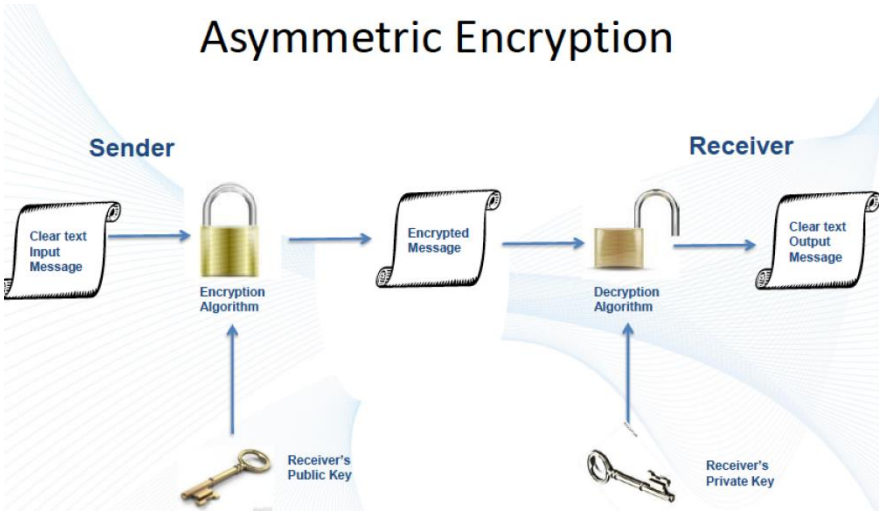
As noted in the figure above:

1. An EHR can be a HISP for its customers (and patients)
2. An EHR can partner with a single full service HISP.
3. An EHR can configure connections (SOAP XDR) to allow customers to choose a HISP, in which case an EHR vendor might have relationships with multiple HISPs.

8. How do I find out someone's Direct Address?

Manually reaching out to an intended receiver is always a good choice. Otherwise, vendors or HISPs may offer a provider directory, which contain Direct addresses.

9. **What do I need to know about direct security mechanisms?**
   There are several key terms used to explain the implementation of Direct security mechanisms (specifically the cryptography used to secure a message). These terms include:
   - Key: A secret number used to lock (encrypt) or unlock (decrypt) information
   - Algorithm: A mathematical procedure that is fed with a key to encrypt or decrypt information
   - Hash: A mathematical procedure that turns a message into a small number that is unique to that message
   - Symmetric: The same key is used to encrypt and decrypt information. This is traditional cryptography.
   - Asymmetric: One key encrypts information and different key decrypts information. Also called Public Key Cryptography. The concept of asymmetric encryption is shown in the figure below:



REQUEST SOURCE

10. **What are the roles and responsibility of parties that support secure Direct communications and business transactions??**
    The following representatives working together ensure the identity of the sender and the receiver to increase the trust of the communication exchange.

    Certificate Authority (CA) (a.k.a. Certification Authority)
    - Issues digital certificates
    - Revokes digital certificates and maintains a Certificate Revocation List (CRL)
    - May manage a directory of issued certificates
    - Bound by a Certification Practice Statement (CPS)

    Registration Authority (RA)
    - Identity proofs certificate applicants
    - Generates certificate signing requests (CSRs) for the Certificate Authority

- Not necessarily an employee of the Certificate Authority

Subscriber: (the subject of the certificate)
- Often generates key pairs
- Must report compromised private keys

Relying party: the entity that is relying on the authenticity and validity of certificates for establishing trust

11. What is a digital signature or certificate?

A digital signature is a fixed length hash of a document, that is encrypted with a private key, then typically sent with the original document and the sender's public key (contained in a digital certificate). This method allows you to verify the authorship and integrity of the message.

12. What does a digital certificate in a private key infrastructure (PKI) contain?

- Subject's name (person or machine)
- Subject's organization
- Subjects' public key
- Validity dates
- The signature of a trusted third party (The certificate authority)
- Other information such as the CA's policy, acceptable key usage, location of the CA's CRL, and so on
- X.509 is the digital certificate standard

13. What are some of the rules surrounding use of private key infrastructure PKI in Direct?

- Direct allows for the use of Organizational Identity Certificates as well as traditional Individual Identity Certificates
- Direct Supports using Domain Name Service (DNS) records to store certificates as well as traditional Lightweight Directory Access Protocol (LDAP) directories. With Direct, a Health Information Service Providers (HISP) or Registration Authorities (RA) will typically generate the end entity key pairs and Certificate Signing Requests (CSRs).

14. What is DTAAP accreditation, and how does an entity become an accredited HISP, CA, and/or RA?

On April 4, 2013, ONC announced the awarding of a Cooperative Agreement to DirectTrust, under the Exemplar HIE Governance Program. A major goal of this award was to advance DirectTrust's partnership with EHNAC for the promulgation and launch of a national accreditation program for HISPs, CAs and RAs to create a network of "scalable trust" so that relying parties in Direct would not need to engage in further one-off contracts and arrangements.

The EHNAC-DirectTrust HISP, CA, or RA Accreditation Program:
- Validates the technical, security, trust, and business practice conformance of Trust Agents involved in Direct.
- Assures HISP-to-HISP interoperability among accredited Trust Agents and other Direct participants.

- Facilitates security, interoperability and trust among Direct exchange participants; fosters public confidence; and otherwise promotes the adoption and success of Directed exchange through the promotion of policies and best practices for security and trust, consistent with state and federal law, for the purpose of improving the quality of health care through secure electronic exchange of health information. DirectTrust has developed and is continuing to develop specific standards and policies for Directed exchange Trust Agents, which enjoy widespread recognition in the Directed exchange community.
- Reduces risk to PHI and operations through the demonstration of a risk management program with effective controls that appropriately minimize threats.
- Prepares your organization for implementing secure communications in support of Meaningful Use requirements by ONC including secure, scalable, standards-based ways for participants to send authenticated, encrypted health information directly to known, trusted recipients over the internet.

To begin the application process for the Direct Trusted Agent Accreditation Program (DTAAP), please complete the pre-application form through EHNAC's Web Site at https://www.ehnac.org/pre-application-form/. Program criteria are located on the criteria page at https://www.ehnac.org/program-criteria/.

15. Where can I go for more information regarding Direct?

- Direct Boot Camp 1.0
  http://wiki.directproject.org/ONC+Direct+Boot+Camp
- Direct Boot Camp 2.0
  http://wiki.directproject.org/ONC+Direct+Boot+Camp+2.0
- Direct Project Wiki
  http://wiki.directproject.org
- Direct Scalable Trust Forum Summary of Findings
  http://www.healthit.gov/sites/default/files/direct-scalable-trust-forum-summary-of-findings-report.pdf
- Direct Implementation Guidelines to Assure Security and Interoperability
  http://www.healthit.gov/sites/default/files/direct_implementation_guidelines_to_assure_se curity_and_interoperability.pdf
- Direct Project Implementation Geographies Workgroup – regular meetings of communities and vendors that are implementing or have implemented Direct
  http://wiki.directproject.org/Implementation+Geographies
- Direct Project Reference Implementation Workgroup – Java and C# open source reference implementations of Direct Project specifications
  http://wiki.directproject.org/Reference+Implementation+Workgroup
- Direct Basics: Q&A for Providers on HealthIT.gov
  http://www.healthit.gov/sites/default/files/directbasicsforprovidersqa_05092014.pdf
- Implementation Guide for Direct Project Trust Bundle Distribution v1.0
  http://wiki.directproject.org/file/view/Implementation+Guide+for+Direct+Project+Trust+Bundle+Distribution+v1.0.pdf
- Meaningful Use
  http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html