NATIONAL
RURAL HEALTH
RESOURCE CENTER

Direct Guide

Direct Project Overview

The Direct Project is a set of standards, protocols and services that enable simple, secure electronic transport of health information (push messaging) between healthcare participants (e.g. providers, labs). The Direct Project will facilitate "direct" communication with a focus towards more advanced levels of interoperability than simple paper can provide. Direct focuses on transportation security mechanism for the content being exchanged, but does not specify the actual content itself.

Any two participants, organizations or communities without a central governance structure can implement the Direct Project standards and services. The Direct Project will coexist with other HIE services based on the existing Nationwide Health Information Network standards and services.

Applications

The Direct Project applications are similar to commonly available email applications, but provide encrypted messaging to ensure the safety and security of exchanged information. Just like email, the Direct Project requires the user to know the recipient's address. Most Direct Project applications do not include a system for searching and finding patient records or provider contacts (direct project addresses). Benefits of deploying a Direct Project application include nationwide communication, securely encrypted messages and attachments, cost-effective information exchange, and relatively simple implementation.

Minimum Requirements

The following are minimum requirements to participate in Direct exchange:

1) Known and trusted "Direct addresses" for the sender and the recipient: a Direct address is an identifier of the provider and location. This address is essentially an email address.
2) A digital certificate which associates (binds) the Direct address to a public key (often referred to as a "public certificate") and to a private key.

Sending a Direct message to another participant, the sender will require the recipient's Direct address and the recipient's public certificate; the receiver will receive the Direct message through his/her direct address and will decrypt with their private key. Other minimum requirements (encryption, trust verification, and other privacy and security mechanisms) can be provided by Health Information Service Providers (HISPs) or product vendors.

Vendor Solutions

Many EHR vendors offer information exchange modules to support exchange of information amongst providers with the same EHR solution. A limited number of vendors offer solutions for exchange between multiple EHR vendors. Exchange between EHR solutions ranges from natively available Direct Project applications (built directly into EHR solutions by the vendor) to complete interoperability resulting from vendor-to-vendor interfaces.

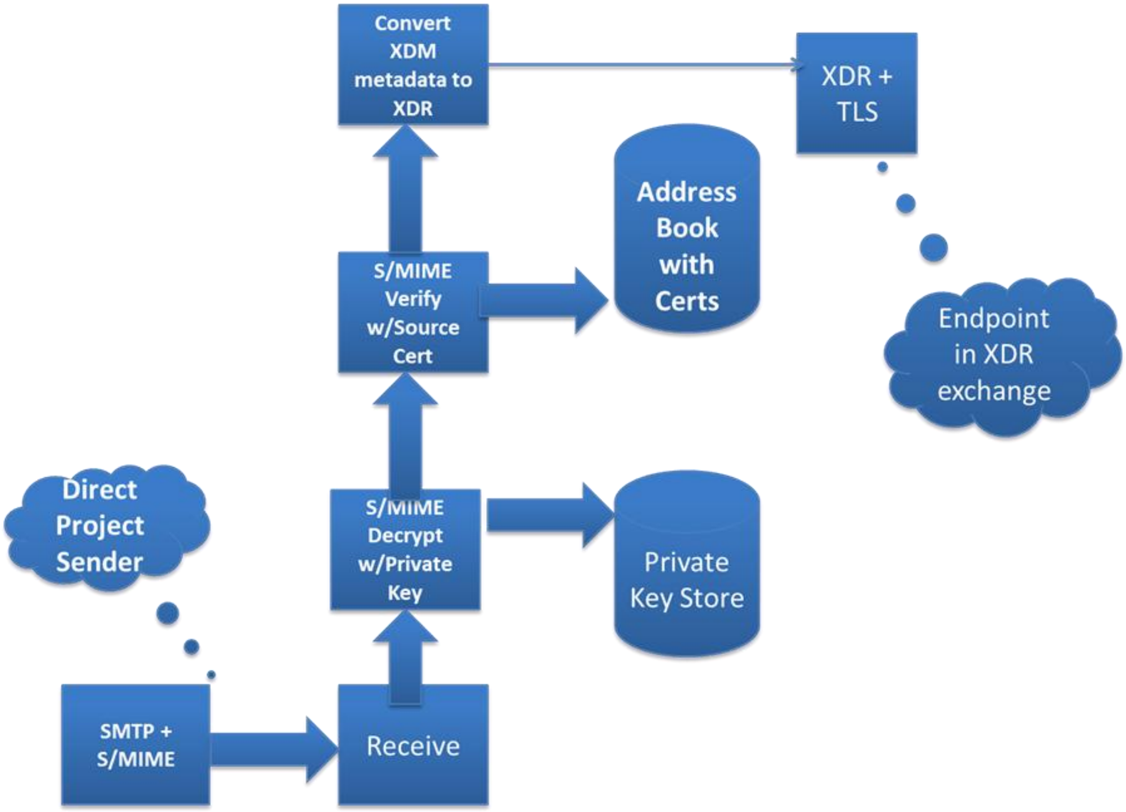
Benefits of deploying an EHR solution from your vendor include functionality built directly into the EHR, minimal disruption to clinical workflows and low use of internal technical resources. A list of vendors that are committed to implementing Direct are listed here: http://wiki.directproject.org/ecosystem

Participation

The Direct Project is an open government initiative. The decision to participate in the Direct Project depends on the value the organization will receive, willingness to comply with the protocols, and comfort with security and privacy protections.

The organization can obtain an organizational certificate from the community trust anchor, configuring the anchor in their implementation, and associating their new certificate with their organization. Trust anchors are configured by each organization implementing Direct specifications to ensure common trust among exchange participants. The anchor decides the criteria by which certificates may be issued for the purpose of message exchange within a given community. Direct software does not issue certificates, it merely allows administrators to associate certificates with endpoints and domains- so the certificates are issued by trust anchors. If two communities share a common definition for certificate and identity assurance they can either use the same trust anchor OR import each other's trust anchors, therefore sharing more information with each other. Certificates can be issued at the community or national level.

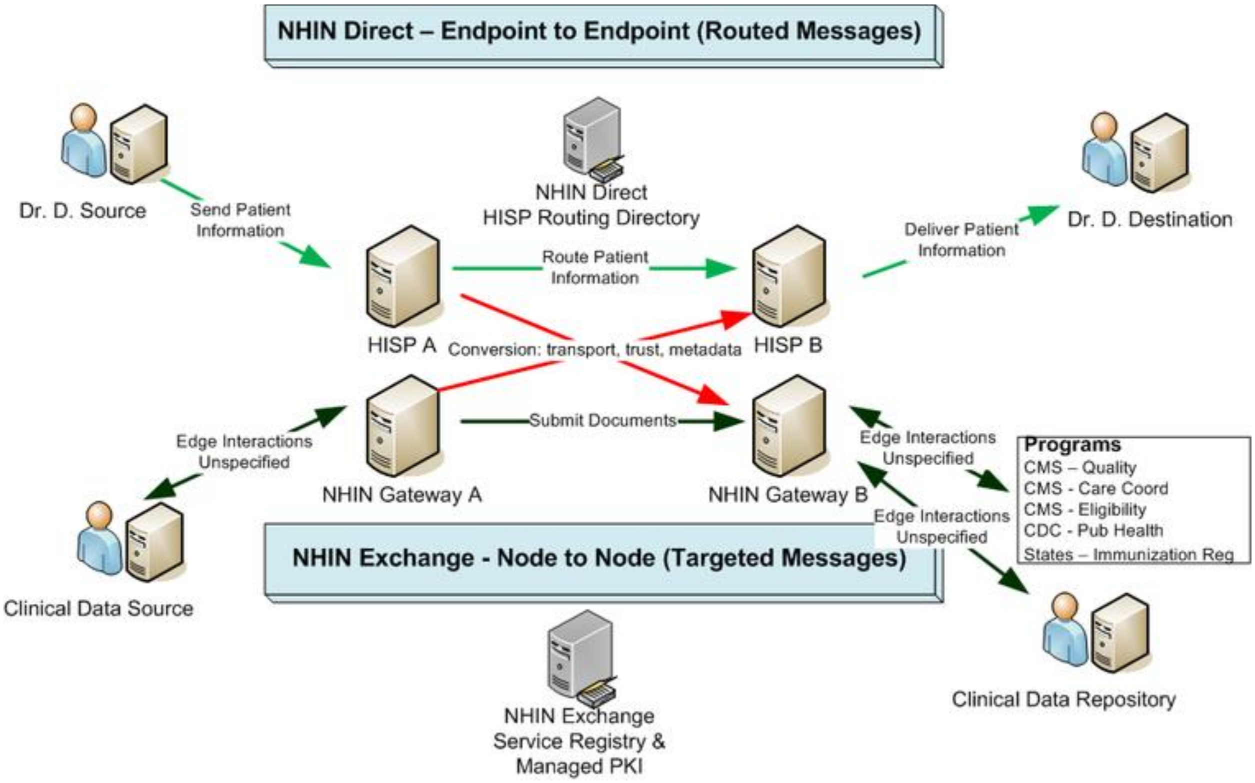
Diagram 1: Direct Project sending to XDR with Trusted Service Provider



In this diagram, 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. The Receiver has supplied the Sender with an address and digital certificate that route the message to the "Direct Project to XDR" Destination HISP. Therefore, the Receiver is explicitly indicating their trust of this Gateway. The "Direct Project to XDR" Destination HISP is considered a trusted service provider. Any Direct Project sender can send to any XDR endpoint as long as there is a Trusted "Direct Project to XDR" Destination HISP service available to do the translation. The XDR receivers have one way to receive directed messages regardless of whether the messages originate from inside their XDR network (e.g. Exchange) or from outside that network using the Direct Project.

There is no need for the XDR receivers to have independent digital certificates, although the Trusted Service could manage multiple individual digital certificates (even though there is little additional benefit, since all of them terminate in the one service).

Diagram 2: Direct Project and Exchange
(Please note that "NHIN Direct" has been renamed to "The Direct Project", and "NHIN Exchange", to "Nationwide Health Information Network Exchange.")


NHIN Direct – Endpoint to Endpoint (Routed Messages)
Dr. D. Source
Send Patient Information
NHIN Direct HISP Routing Directory
Deliver Patient Information
Dr. D. Destination
Route Patient Information
HISP A
Conversion: transport, trust, metadata
HISP B
Edge Interactions Unspecified
Submit Documents
Edge Interactions Unspecified
Programs
CMS – Quality
CMS - Care Coord
CMS - Eligibility
CDC - Pub Health
States – Immunization Reg
NHIN Gateway A
NHIN Gateway B
Edge Interactions Unspecified
NHIN Exchange - Node to Node (Targeted Messages)
Clinical Data Source
Clinical Data Repository
NHIN Exchange Service Registry & Managed PKI

Source: The Direct Project
http://wiki.directproject.org/Intersection+with+Exchange

In this diagram:
a) HISP A sends to NwHIN Gateway B
b) NwHIN Gateway A sends to HISP B

Regardless of the model, the transformation of three things is required:

- Transport - use of particular transport protocol (SOAP/REST/SMTP). These are fairly clear transformations and are considered relatively easy to implement
- Trust - transformation of trust models. Complexity is not yet clear as trust model for Direct has not been completely identified
- Metadata - needs detailed comparison and discussion to be able to see how far apart the two models are.

Note that both the Direct Project and NwHIN Exchange are content neutral so no transformation is necessary, although there may be issues in content exchange because some NwHIN Exchange partners may want to restrict the types of content they will accept.

Meaningful Use

Direct-enabled products can be used by providers and organizations to transport and share different types of content specified by Meaningful Use – thus the combination of Meaningful Use specified content and Direct project specified transport standards may satisfy certain Stage 1 Meaningful Use requirements that involve health information exchange (e.g. care summary, exchange and lab results delivery). Stage 2 Meaningful Use requirements that debuted in August 2012 included requirements on secure health transport specifications including XDR and XDM for Direct Messaging

Being "Direct-enabled" means that the user can support the common specifications for the Direct Project and can send/receive information to and from using Direct specifications. The user must follow the Direct Project Implementation guidance. There is no independent certification process for establishing that an application or network is "Direct enabled" and is not currently part of Meaningful Use certification or EHR certification.

The Direct Project will be the required transport for summary of care documents, specifically, the Applicability Statement for Secure Health Transport. There are optional transport standards as well. There are two choices for the use of optional standards:

1) Option 1: Certification can be performed for both the Applicability Statement for Secure Health Transport specification and the specification utilizing the XDR and XDM profile for Direct Messaging.

2) Option 2: Certify for both Simple Object Access Protocol (SOAP)-Based Secure Transport Requirements Traceability Matrix (RTM) version 1.0 standard and the XDR and XDM for Direct Messaging.

For the optional standards, the SOAP-Based Secure Transport Requirements Traceability Matrix (RTM) specification was selected instead of the more specific IHE profiles. SOAP is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks. It relies on Extensible Markup Language (XML) for its message format, and usually relies on other Application Layer protocols, most notably Hypertext Transfer Protocol (HTTP), for message negotiation and transmission.

The Direct Project specifications provide entry-level transport in a point-to-point fashion, while the SOAP-based IHE profiles provide for more advanced communications where healthcare facilities can query one another for patient information.

Meaningful Use Stage 2 compliance testing may begin by July 1, 2014. Then, on to Stage 3 criteria, which will be implemented in 2016 at the earliest.

Scope, Interoperability and Deployment

Scope Limits

The Direct project does not embody a model of "pulling information". Direct's focus is more on the transport of health information but it is not the complete "interoperability" package.

Interoperability

In order for effective interoperability with Direct the following must be determined:

1) How are messages sent and received (e.g. Direct Project specified transport)
2) Structure and format of the exchanged content
3) Items to use within their content (SNOMED Clinical Terminology)

Direct did not define specifications for content because the MU Final Rule and other standards groups have made strong recommendations for information to be exchanged and how it's coded. Direct will be used to transmit unstructured messages (text, PDF) and highly structured messages (including HL7 v2 messages, Continuity of Care records/documents).

Direct does not ensure semantic interoperability, but it helps to support data exchange by supporting one important foundational element of exchange- a common layer for transport. The content transported using Direct-mediated exchange is based upon shared standards for message structure and terminology; Direct can support semantic interoperability by being the conduit for information flow.

Deployment

There are three deployment models for Direct:

1) An entity sends and receives Direct messages through a web portal offered as a service of a HISP. This is much like a web-based email account.

2) An entity sends and receives Direct messages using a standard email client, which has been Direct-enabled. e.g., through a software plug-in or an upgrade to the email client.

3) An entity uses an electronic health record system software that is Direct-compliant, through which it sends and receives Direct messages from within the application. The process of generating data from a EHR and sending a Direct message and/or receiving and integrating the contents of a Direct message into your electronic health record, is completely dependent on the capabilities of the application provided by the software vendor.

Privacy and Security

The Direct -mediated exchange is required to conform to applicable federal and state laws. Direct is utilized within the pre-existing framework of trust among exchanging entities- where patient identity is known and where consent and legal authorization allow the information to be transferred.   Direct may not address all the additional requirements at the state level.

Direct assumes that both the sender and the receiver have the appropriate authority and consent to share the messages in question. There are no particular components embedded in Direct methodologies for ensuring that these rights and permissions have been established. In other words, privacy assurance is outside the bounds of transport layer as defined in Direct. The privacy assurance is the responsibility of the sender and the receiver.

Security is managed in the transport layer of Direct through the use of digital certificates issued by Certificate Authorities to encrypt messages as they travel from sender to receiver. The digital certificate model, ensures that only the intended recipient of a message can unlock and decrypt that message. Direct does not provide security for the message once it's opened by the recipient.   The receiver's Direct-compliant interface (Direct compliant EHR, email program or web portal) must provide assurance that they unencrypted message is sufficiently secure as they would for any other sensitive patient data.

Protocols, Specifications and Standards

The Direct project uses Simple Mail Transport Protocol (SMTP) for email transmission. SMTP is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

However, the Direct project is neutral about the content of data transmitted using its protocol.   The only requirement is for the use of Internet Engineering Task Force (IETF) standards. For other Direct transactions, another set of standards are the Integrating the Healthcare Enterprise (IHE) based standards.

MIME (Multipurpose Internet Mail Extensions) is an Internet standard that extends email to support content beyond simple ASCII plain text data. Content is packaged using MIME and optionally, XDM. XDM (Cross-Enterprise Document Media) is an interchange integration profile, a specification for the exchange of electronic health record documents on portable media. XDM provides for zipped file transfer over e-mail, which is very relevant to the Direct Project specifications.

Confidentiality and integrity of the content is handled through S/MIME encryption and signatures. S/MIME (Secure/Multipurpose Internet Mail Extensions) is an Internet standard for securing MIME data.

The Direct S/MIME provides privacy and data security through encryption and authentication, integrity assurance and no-repudiation of email origin through singing. Authenticity of the Sender and Receiver is established with X.509 digital certificates, which are typically obtained through the HISP. Direct relies on the use of embedded subject and issuing chain. X.509 standards for a PKI-based infrastructure will push Direct users to create trust policies that speak in terms of certificates, public key infrastructure and certificate authorities.

Specifically, the HISP to HISP backbone uses the XDR standard, a lightweight point-to-point protocol designed specifically to push documents from a source to a destination.

Use cases and common scenarios

The Direct project addresses situations where one known entity pushes health information to another known entity in a secure manner. A great resource about clinical scenarios based on core and menu Meaningful Use requirements can be found at http://wiki.directproject.org/user+stories

Direct can also be used in a more advanced scenario where two consecutive directed exchanges can enable value functionality e.g. hospital pushes admission, discharge and transfer notification through a Direct message to a primary care practice; and the primary care practice responds with the patient's clinical summary through Direct message.

Information Resources

http://www.corepointhealth.com/resource-center/healthcare-interoperability-glossary#XDR
http://directproject.org
http://www.healthit.gov/policy-researchers-implementers/federal-advisory-committees-facas/Nationwide-Health-Information
http://wiki.directproject.org
http://wiki.directproject.org/Consensus+Proposal
http://wiki.directproject.org/file/view/DirectProjectOverview.pdf
http://wiki.directproject.org/deployment+models
http://wiki.directproject.org/User+Stories
http://wiki.directproject.org/Abstract+Model+Examples

Glossary

Administrative-related functions

- Register/edit/delete: Processes executed by authorized individuals or entities to add or modify entries (entities and individuals) in a provider directory based on national and local policies. They may involve attestation, verification and/or validation of the information provided about the entities and individuals.
- Access control: Prevention of unauthorized use of information assets (ISO 7498-2). It is the policy rules and deployment mechanisms, which control access to information systems, and physical access to premises (OASIS XACML).
- Audit: Review and examination of records (including logs), and/or activities to ensure compliance with established policies and operational procedures. This review can be manual or automated.

Abstract Model **-** The basis of the Direct Project's technical specifications, the abstract model provides a common framework for stakeholders to investigate Direct standards and services.

Affinity Domain - A group of healthcare enterprises that have agreed to work together using a common set of policies and share a common infrastructure. With Direct, there is an implication of shared trust anchors.

Application Programming Interface (API) - A set of protocols intended to be used as an interface by software components to communicate with each other. An API library includes specifications for routines, data structures, object classes, and variables.

Attribute – A characteristic of an object or activity.

Authenticate **-** To verify an identity prior to granting access or asserting trust.

Certificate Authority **-** Issues digital certificates in a public key infrastructure environment.

Content **-** The health information being communicated, which is independent of the technical mechanism used to move it.

Direct Address **-** Used to identify an endpoint (a Sender or Receiver) when information is exchanged. The Direct Address has two parts, a Health End Point Name and a Health Domain Name, for example, drbob@samplehispname.org.

Direct Message **-** The content of the information being transferred from the Sender to the Receiver. The Direct Message is similar to a package that is sent from one person to another via the postal service, such as the content within an envelope or a box.

Discoverability - The ability of an individual/entity to access and obtain specific information about another entity, including demographic information, information exchange information and security credentials information.

Domain Name System (DNS)- An Internet system to translate human-readable names into Internet addresses.

Federal Health Architecture (FHA) - A collaborative body composed of several federal departments and agencies, including the Department of Health and Human Services (HHS), the Department of Homeland Security (DHS), the Department of Veterans Affairs (VA), the Environmental Protection Agency (EPA), the United States Department of Agriculture (USDA), the Department of Defense (DoD), and the Department of Energy (DOE). FHA provides a framework for linking health business processes to technology solutions and standards, and for demonstrating how these solutions achieve improved health performance outcomes.

Health Data Intermediary (HDI) **-** Health data intermediary or HDI means an entity that provides the infrastructure to connect computer systems or other electronic devices used by health care providers, laboratories, pharmacies, health plans, third-party administrators, or pharmacy benefit managers to facilitate the secure transmission of health information, including pharmaceutical electronic data intermediaries as defined in Minn. Stat. §62J.495. This does not include health care providers engaged in direct health information exchange. **[**Minn. Stat**.** §62J.498 sub. 1(e)].

Health Domain Name **-** The delivery location for messages to an individual Direct HISP, the HISP portion of a Direct Project Address.

Health End Point **-** The delivery location for messages to an individual Direct user, the user portion of a Direct Project Address.

Health Information Exchange (HIE) - The electronic transmission of health-related information between organizations according to nationally recognized standards.

Health Information Exchange Service Provider (HISP) **-** A health data intermediary or health information organization that has been issued a certificate of authority. The entity that serves the backbone exchange needs of Source and Destination actors and should be thought of in the context of message delivery/receipt and not in the context of governance responsibilities.

Health Identity Provider (HIDP) - This executes the roles of Registration Authority (RA) and Certificate Authority (CA) and ultimately is responsible for providing organizational and individual Direct certificates to verified organizations and individuals.

Health Information Organization (HIO) **-** HIO is an organization that oversees, governs, and facilitates the exchange of health-related information among organizations according to nationally recognized standards.

Healthcare Provider Directory (HPD) - An IHE profile, which supports management (persistence and access) to healthcare provider's information in a directory structure. Two categories of healthcare providers are included in the directory:

- Individual Provider – A person who provides healthcare services, such as a physician, nurse, or pharmacist.
- Organizational Providers – Organizations that provide or support healthcare services, such as hospitals, Healthcare Information Exchanges (HIEs), Integrated Delivery Networks (IDNs), and Associations.

Healthcare Provider Directory Plus (HPD Plus) - An enhanced version of the IHE Healthcare Provider Directory (HPD) persistence model, harmonizing it with the S&I Framework Electronic Service Information Discovery Data Model. HPDPlus is defined by the Statewide Send and Receive Technical Specifications Appendix – HPDPlus Implementation Guide_v1 and its persistence can be implemented in LDAP or in Relational Databases.

HPDPlus RDB - Defined as the adaption of the DSMLv2 based HPD to use a Relational Database (RDB) persistence model.

HPDRequestor – HPDRequestor is defined as an entity requesting the Direct address.

HPDResponder – HPDResponder is defined as an entity providing the Direct address.

Health Level 7(HL7) **-** A standard interface for exchanging and translating data between computer systems. HL7 is also a not-for-profit organization accredited by the American National Standards Institutes (ANSI) that develops standards for data transfer.

Individual Certificate - An X.509 certificate bound to the identity of an individual. An individual certificate is associated with exactly one Direct address, which is listed in the email Subject Alternative Name extension (preferred) or in the Email Address attribute of the Subject Distinguished Name (legacy).

Interoperability **-** The ability of two or more systems or components to exchange information and to use the information that has been exchanged accurately, securely, and verifiably, when and where needed.

According to the Interoperability Clearing House "interoperability is the ability of information systems to operate in conjunction with each other encompassing communication protocols, hardware software, application, and data compatibility layers. With interoperable electronic health records, always-current medical information could be available wherever and whenever the patient and attending health professional needed it. At the same time, EHRs would also provide access to treatment information to help clinicians as they care for patients."

Lightweight Directory Access Protocol (LDAP) **-** An application protocol for querying and modifying data of directory services implemented in Internet Protocol (IP) networks.

Meaningful Use(MU) **-** The use of certified electronic health record technology that includes e-prescribing, and is connected in a manner that provides for the electronic exchange of health information and used for the submission of clinical quality measures as established by the Center for Medicare and Medicaid Services and pursuant to sections 4101, 4102, and 4201 of the HITECH Act including subsequent regulations, rules and guidance issued pursuant to the HITECH Act.

Meaningful Use Transaction - An electronic transaction that a health care provider must exchange to receive Medicare or Medicaid incentives or avoid Medicare penalties pursuant to sections 4101, 4102, and 4201 of the HITECH Act.

Node - A node is simply a reference object that allows you to "select" a group of related pieces of content. It provides an intuitive method for organizing your content pages.

Organizational Certificate - An X.509 certificate bound to the identity of an organization and not necessarily an individual. An Organizational Certificate is tied to a domain name by the presence of a DNS Subject Alternative Name extension that lists the domain name.

Patient Matching **-** The process of cross-linking the multiple patient identifiers in a community from a variety of patient identifier sources and creating a master patient identifier with a key for cross-referencing the various community identifiers. This is also referred to as a record locator service.

Provider Directory (PD) **-** Refers to a persistence store with entries that pertain to end users acting as individual providers or other healthcare clinicians. Also stored are entities such as organizations or departments and the relationships between providers and entities. There are two types of provider directories:

- ELPD (Entity-Level Provider Directory) is a directory listing provider organizations.
- ILPD (Individual-Level Provider Directory) is a directory listing individual providers.

Receiver **-** Actor in the Direct workflow who receives the message content. A Receiver may be a person or a larger business entity.

Reference Implementation **-** Open-source software that implements the Direct Project specifications. There may be multiple reference implementations using different technologies (e.g., .NET, Java), and a reference implementation is not normative as the specifications are.

Root Certificate - 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. A root certificate has the X.509 CA basic constraint extension set to "true."

Sender **-** Actor in the Direct workflow who originates the message content. A Sender may be a person or a larger business entity.

Security Credentials - A physical/tangible object, a piece of knowledge, or a facet of an entity's or person's physical being, that enables the entity/person access to a given physical facility or computer-based information system. Typically, credentials are something the user knows (such as number or PIN), something owned (such as an access badge), something present on user (such as a biometric feature) or some combination of these items.

Services Registry - Contains metadata about the services available in the infrastructure including mappings between individuals or network resources (services or systems) and web service addresses and protocols. It is the primary directory that Nodes use to locate recipients of health information or systems from which to request information. This provides a central, reliable, distribution point for service related metadata (sometimes called the "green pages").

Simple Mail Transfer Protocol (SMTP) - An Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

Simple Object Access Protocol (SOAP) - A protocol specification for exchanging structured information in the implementation of Web Services in computer networks. It relies on Extensible Markup Language (XML) for its message format, and usually relies on other Application Layer protocols, most notably Hypertext Transfer Protocol (HTTP), for message negotiation and transmission.

Systematized Nomenclature of Medicine, Clinical Terms (SNOMED CT) **-** SNOMED CT is a dynamic, scientifically validated clinical health care terminology and infrastructure that makes health care knowledge more usable and accessible. The SNOMED CT Core terminology provides a common language that enables a consistent way of capturing, sharing and aggregating health data across specialties and sites of care. Among the applications for SNOMED CT are electronic medical records, ICU monitoring, clinical decision support, medical research studies, clinical trials, computerized physician order entry, disease surveillance, image indexing and consumer health information services.

Uniform Resource Identifier (URI) -A string of characters used to identify a name or a resource on the internet. The URI syntax consists of a URI scheme name (such as "http", "ftp", "mailto" or "file") followed by a colon character, and then by a scheme-specific part.

XDM **-** The IHE Cross-Enterprise Document Media Interchange integration profile, a specification for the exchange of electronic health record documents on portable media. XDM provides an option for zipped file transfer over e-mail, which is very relevant to the Direct Project specifications.

XDR **-** The IHE Cross-Enterprise Document Reliable Interchange integration profile, a specification for the interchange of electronic health record documents through reliable point-to-point network communication, based on a push of information.

*XDS***-** The IHE - Cross-Enterprise Documenting Sharing integration profile, a specification for managing the sharing, finding, and retrieval of electronic health record documents among a defined group of healthcare enterprises.

X.509 Digital Certificates **-** A standard for asserting that an entity is who it purports to be. The standard is strictly hierarchical, where a trusted entity asserts the identities of a set of child entities, which can make further assertions, ad infinitum.