

Direct Project FAQs

I. General and Background

1. [What is the Direct Project?](#)
2. [Why Direct?](#)
3. [How does the Direct Project help in achieving Meaningful Use?](#)
4. [What does “Direct-Enabled” mean and to what extent is it connected to MU certification?](#)
5. [How does Direct integrate with and complement other advanced forms of exchange, particularly query/retrieve?](#)
6. [When using Direct, how can my organization transition to enable other more advanced exchange capabilities?](#)
7. [What is the relationship between the Direct Project and the currently described Nationwide Health Information Network \(NW-HIN\) architecture?](#)
8. [Does the Direct Project replace the current Nationwide Health Information Network model? Is the Direct Project the current Nationwide Health Information Network model on “training wheels”?](#)
9. [Is a Personal Health Record \(PHR\) part of the Direct Project?](#)

II. Standards and Policy

1. [How were the specifications and standards for the Direct Project developed? Is standards development complete?](#)
2. [What policies and procedures do I need to develop for Direct?](#)
3. [Does Direct comply with Federal privacy and security regulations?](#)
4. [What use cases does the Direct Project support?](#)
5. [How does the Direct Project ensure semantic interoperability?](#)

III. Implementation

1. [How can Direct be deployed?](#)
2. [What are the minimum requirements for Direct?](#)
3. [How do I find someone’s Direct address?](#)
4. [How can I encourage my state’s providers to participate?](#)
5. [What vendors will support Direct?](#)
6. [How is privacy and security handled?](#)
7. [What is a HISP? What/who can be a HISP?](#)
8. [How do I find a HISP?](#)

IV. Technical Standards

1. [What is the recommended data standard \(like NCPDP, HL7 V2 etc.\) to be used? Has a Standards Development Organization \(SDO\) been selected to maintain the specifications?](#)

2. [What will be the Direct Project's transport specifications, and can more than one be used?](#)

V. Provider Directories

1. [What is the role of the Direct Project in the development of provider directories?](#)

VI. Certificate

1. [What is a digital certificate and how is it relevant to Direct?](#)
2. [What is a trust anchor?](#)
3. [What are the criteria for a trust anchor?](#)
4. [What type of certification does Direct support? Is it specific to the provider organization? To the end user? To both?](#)
5. [What should be the minimum requirements for identity verification and authorization?](#)
6. [How does Direct meet minimum certificate authority requirements?](#)
7. [How is trust established in the pilot projects? Are certificates from existing vendors acceptable?](#)

VII. Organization Decision

1. [Should our organization participate in Direct?](#)
2. [How should I format Direct addresses for my organization?](#)
3. [Can we re-use existing email addresses for Direct messaging? Can we re-use existing email clients for Direct messaging?](#)

VIII. Learn More and Get Involved

1. [How do states get involved in the Direct Project and the pilots?](#)

Detailed Questions and Answers

General and Background

1. What is the Direct Project?

The Direct Project is the set of standards, policies and services that enable simple, secure transport of health information between healthcare participants (e.g., providers, labs) who know each other and already have a relationship of trust. The Direct Project enables standards-based exchange of health information in support of core Stage 1 Meaningful Use measures. This can include communication of summary care records, referrals, discharge summaries and other clinical documents in support of continuity of care and medication reconciliation, as well as communication of laboratory results to ordering providers.

2. Why Direct?

There is a need to extend the Nationwide Health Information Network to support the core Meaningful Use outcomes and measures by enabling participation for a broader set of participants and providers through a simple, standards-based, widely deployed and well-supported method to securely transport health information to known destinations using the Internet.

As such, several State HIE programs have turned to Direct to enable information exchange between healthcare participants who will be less capable of adapting State HIE services in 2011, such as independent physicians, rural clinics, and small laboratories.

3. How does the Direct Project help in achieving Meaningful Use?

The Direct Project specifies the technical protocols and services necessary to securely push content from a sender to a receiver. Direct focuses on the transportation and security mechanism for the content being exchanged, but does not specify the actual content itself. However, 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).

4. What does “Direct-Enabled” mean and to what extent is it connected to MU certification?

Being “Direct-enabled” means that you can support the common specifications for the Direct Project, and can send and receive information to and from anybody else using Direct specifications. It means that you follow the Direct Project implementation guidance (as noted in the “applicability statement” – refer to

<http://wiki.directproject.org/Applicability+Statement+for+Secure+Health+Transport>), which constrains the use of the foundational standards on which Direct is built. It also means that you are able to send and receive information in accordance with the level of trust required.

As of March 2011, there is no independent certification process for establishing that an application or network is “Direct enabled” and it is not currently part of the Meaningful Use certification or EHR certification process. So this notion, for now, is more of an attestation by the vendor. States or other entities could, however, establish testing or certification processes for supporting Direct exchange.

5. How does Direct integrate with and complement other advanced forms of exchange, particularly query/retrieve?

The Direct Project “push” model (also known as “directed exchange”) enables a different, simpler set of functionality than the query and retrieve “pull” model. This can enable participants to share basic information using a simpler technical and data architecture; e.g., Direct providers do not have to share or expose their data or establish pointers to specific patient data. However, Direct’s simpler technical requirements can still benefit from some of the same infrastructure created for query/retrieve. In particular, although directed exchange can be performed as a point-to-point transaction that does not require the use of a provider directory, it can be used more broadly when supported by the same type of provider directory services as is needed to support query/retrieve-based exchange. Similarly, both directed exchange and query/retrieve can leverage certificate authority services to enable security and trust.

6. When using Direct, how can my organization transition to enable other more advanced exchange capabilities?

Although Direct and query/retrieve methods of exchange use different protocols and methods, many state HIE programs, for example, plan to implement Direct as part of their initial exchange efforts, then leverage the assets they use to support Direct — such as provider directory, certificate authority, and other health information service provider (HISP) services — as part of a longer-term strategy to support more advanced forms of exchange.

7. What is the relationship between the Direct Project and the currently described Nationwide Health Information Network (NW-HIN) architecture?

The architecture for the Nationwide Health Information Network (NW-HIN) as currently defined, is a method for universal patient lookup and document discovery and exchange between National Health Information Organizations, including Federal providers such as the Veterans Health Administration, Department of Defense Military Health System, RHIOs, and large Integrated Delivery Networks (IDNs). The Direct Project supports cases where information is pushed directly from one party (including clinicians, hospitals, laboratories, and other health settings of care) to another.

It is expected that Direct Project specifications will be incorporated into the broader set of NW-HIN specifications. As such, we expect the current members of the NW-HIN Collaborative to support the Direct Project model, and providers and enabling organizations for the Direct Project will support exchange use cases. So both capabilities are expected to be required of NW-HIN participants and will be in use at the same time, depending on the needs for information being exchanged.

8. Does the Direct Project replace the current Nationwide Health Information Network model? Is the Direct Project the current Nationwide Health Information Network model on “training wheels”?

No to both questions. The Direct Project and the current query/retrieve model employed by the Nationwide Health Information Network support different use cases, and will coexist to enable the full capabilities necessary for a robust nationwide system for health information exchange.

9. Is a Personal Health Record (PHR) part of the Direct Project?

Any system that supports Direct specifications can participate in Direct exchange. There have been a number of vendors of personally controlled health records which have participated in the Direct development process, including some that offer Direct addresses. Microsoft, for example, recently announced that they would create Direct addresses for all HealthVault personal health records. Some of the Direct Project implementation geography pilots include a personally controlled health record component and incorporate the patient into the information exchange workflows.

Standards and Policy

1. How were the specifications and standards for the Direct Project developed? Is standards development complete?

The specifications and standards were developed in a rapid, open process with participation from a varied set of stakeholders representing both public and private providers and technology enablers. While developing Direct, ONC wanted to assure flexibility for participants to explore different standards options.

Though the key specifications have been developed and pilot testing has begun, required elements for Direct-required services such as provider directories are still to be determined as of March 2011. The Direct Pilot projects will provide valuable lessons learned that will help demonstrate what works and what still needs to be developed. To provide further guidance and support for Direct, ONC will establish a Community of Practice (COP) in Spring 2011.

2. What policies and procedures do I need to develop for Direct?

Unlike Nationwide Health Information Network Exchange (NW-HIN) participants, Direct users have to establish their own policies and standards for deciding which other Direct addresses to trust. Current NW-HIN users are required to sign a data use and reciprocal service agreement (“DURSA”) that essentially establishes a commonly-shared code of conduct and legal framework to enable trust among users. Direct users are not required to establish such a framework, though state laws may require additional levels of patient consent and user authentication.

While the HIT Policy Committees will provide policy guidance for Direct, organizations must adopt and implement policies and practices that best support their specific environments.

That being said, remember that in many cases, Direct will fulfill the role previously played by paper, fax, courier, mail or clipboard – so user communities should be wary of creating a privacy solution that is overly complex for simple use cases.

3. Does Direct comply with Federal privacy and security regulations?

The Direct-mediated exchange is required to conform to applicable federal and state laws, including but not limited to those related to security and privacy of protected health information. Direct is designed to enable simple direct transactions via a secure electronic transport, thereby allowing electronic exchange of information that is currently exchanged via paper, fax, courier, mail, or clipboard, or in some cases via manual upload or duplicate data entry to allow viewing through a portal. Direct can be employed within the existing patterns for establishing and maintaining trust among exchanging entities, where patient identity is known and where consent and legal authorization allow the information to be transferred. Some state laws may have additional requirements that are not fully addressed through the use of Direct-mediated exchange alone.

4. What use cases does the Direct Project support?

The Direct Project aims first to address situations where one known entity pushes health information to another known entity in a secure manner; e.g., primary care provider refers patient to specialist and includes the summary care record, or primary care provider sends patient immunization data to public health. Information about the Direct Project’s set of common clinical scenarios based on core and menu Meaningful Use requirements can be found at <http://wiki.directproject.org/User+Stories>.

In addition to the common clinical scenarios, Direct can also be used in more advanced scenarios where *two consecutive directed exchanges* can enable valuable functionality; e.g., hospital pushes an ADT (Admission, Discharge & Transfer) Notification through a Direct message to a primary care practice; and the primary care practice responds with the patient’s clinical summary through another Direct message.

5. How does the Direct Project ensure semantic interoperability?

The core mission for the Direct Project is to enable secure transport of information between known parties. Intentionally, Direct chose not to define specifications for content, because the Final Rule (FR) and the existing work of standards development organizations (SDOs) already establish strong recommendations regarding information that should be exchanged and how it should be coded. It is expected that Direct will be used to transmit unstructured messages, including simple text and PDF, and highly structured messages and documents, including HL7 v2 messages, Continuity of Care Documents (CCD), and Continuity of Care Records (CCR) with well defined vocabulary. It is likely that new content representations will be created outside of the Direct Project to solve innovative use cases, such as messaging regarding gaps in care.

It is also anticipated that implementers of Direct Project might leverage enabling organizations to translate content in order to enable health information exchange between systems that use different standards. In other words, the Direct Project 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.

Implementation

1. How can Direct be deployed?

There are three primary deployment models for Direct. In the first model, an entity sends and receives Direct messages through a web portal offered as a service of a Health Information Service Provider, or HISP – the user experience is much like that of a web-based email account. In the second model, an entity sends and receives Direct messages using a standard e-mail client which has been Direct-enabled, e.g., through a software plug-in or an upgrade to the email client. In the third model, an entity uses an EHR system software that is Direct-compliant, through which it sends and receives Direct messages from within the application. The process of generating data from an EHR and sending a Direct message, and/or receiving and integrating the contents of a Direct message into your EHR, is completely dependent on the capabilities of the application provided by the software vendor.

In all three deployment models, routing of the Direct message from one recipient to another is typically facilitated by a HISP. Encryption of the message typically occurs on the HISP (refer to the section on Certificates below).

2. What are the minimum requirements for Direct?

From an end-user perspective, there are two minimum requirements to participate in Direct:

- 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 e-mail address (e.g., it may look like “bob@direct.myclinic.com”), and not usually one’s general-purpose e-mail address.
- A digital certificate (see Certificates below), which associates (“binds”) the Direct address to a public key (often referred to as a “public certificate”) and to a private key.

To send 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 Direct address, and will decrypt it with his 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.

3. How do I find someone’s Direct address and digital certificate?

As of March 2011, there is only one way to find it: just like finding e-mail, telephone, or Fax information, you must ask the person for it. However, searchable directories of Direct addresses will be established in the future, either in local areas or even nationally (see Directory below).

4. How can I encourage my state’s providers to participate?

Educational outreach and technical guidance are likely the two most important aspects of promoting the use of Direct among providers. States/SDEs should collaborate with their RECs to build awareness and provide technical assistance to eligible providers. Since provider directories can play a key role in facilitating Direct-mediated exchange, states/SDEs that are leveraging data sources from licensing agencies or state medical societies should consider collaborating with these entities to promote creation of a Direct address as one of the benefits of licensure or membership. Especially in areas where there is no existing infrastructure to support HIE, promotion of Direct as a simple means of achieving key objectives around Meaningful Use can be an effective draw for eligible providers. Finally, collaborating with the EHR vendors that support Direct and including them in preferred vendor lists can be helpful in building awareness among providers considering various EHR options.

5. What vendors will support Direct?

More and more vendors are signing up to support Direct. A list of the current vendors and other participants who have committed to implement Direct are listed and categorized here: <http://wiki.directproject.org/ecosystem>

6. How is privacy and security handled?

From a privacy perspective, Direct assumes that both the sender and the receiver have the appropriate authority and consent to share the message 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 the transport layer as defined in Direct. This privacy assurance is the responsibility of the sender and receiver. Some states are developing consumer preferences and consent management services to augment Direct and other state or state designated entity mediated exchange.

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, when properly implemented, ensures that only the intended recipient of a message can unlock and decrypt that message. Direct does not provide security for the message content once it is opened by the recipient. One can think of a digital certificate as a special kind of seal on a package that can only be opened by the addressee. It is secure as long as it remains unopened; after that, it is up to the recipient to maintain the security of whatever was inside the package. This means that the receiver's Direct-compliant interface (e.g., Direct-compliant EHR, email program or Web Portal) must provide assurance that the "opened package" (i.e., unencrypted message) is sufficiently secure, as they would do for any other sensitive patient data.

7. What is a HISP? What/who can be a HISP?¹

Put simply, a Health Information Service Provider (HISP) is an organization that provides services on the Internet to facilitate use of Direct. A HISP is a logical concept that encompasses certain services that are required for Direct-mediated exchange, such as the management of trust between senders and receivers. It may be a separate business or technical entity from the sender or receiver, depending on the deployment option chosen by the implementation. A user typically agrees to allow the HISP to maintain a digital certificate on his/her/its behalf. Using this digital certificate, the HISP can securely send or receive Direct messages for the entity. The user initiates outgoing messages, and accesses incoming messages, through facilities provided by the HISP (often through a secure e-mail portal or client).

There are various deployment models used in Direct Project implementations, some of which use a HISP and some of which do not. The details of the various options are presented in the Wiki Deployment Models page <http://wiki.directproject.org/Deployment+Models>. If the model chosen is one where the services performed by the HISP are not provided by a separate business or technical entity, an entity must implement additional capabilities to meet the various Direct Project specifications.

8. How do I find a HISP?

It is anticipated that a variety of companies will offer these services. A list of the current vendors and other participants who have committed to implement Direct are listed and categorized at <http://wiki.directproject.org/ecosystem>, and is the best place to identify potential HISPs. Some states are establishing a vetting or certification process for HISPs that want to operate within the state and intend to post information on these HISPs on their websites.

Technical Standards

1. What is the recommended data standard (like NCPDP, HL7 V2 etc.) to be used? Has a Standards Development Organization (SDO) been selected to maintain the specifications?

Specifications for Direct are neutral about the content of data transmitted using its protocol. The only requirement is for the use of Internet Engineering Task Force (IETF) standards <http://www.ietf.org/about/standards-process.html> to support the transport protocol over the Internet. For some Direct transactions, another set of relevant specifications are in fact an applicability statement for the use of Integrating the Healthcare Enterprise (IHE) based standards. It is very likely that the IHE standards will be vetted and approved through IHE's standards adoption process; however this has not been decided as of March 2011.

2. What will be the Direct Project's transport specifications, and can more than one be used?

The Direct project uses Simple Mail Transport Protocol (SMTP), the Internet standard for e-mail transmission.

In general, a Direct Project implementation is responsible for packaging message content, securing it, and transporting it from one location to another.

Content is packaged using MIME and, optionally, XDM. MIME (Multipurpose Internet Mail Extensions) is an Internet standard that extends e-mail to support content beyond simple ASCII plain text data. 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 an option 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. S/MIME provides

- privacy and data security through encryption and authentication,
- integrity assurance; and

- non-repudiation of origin (evidence that who is purported to send the document was the actual sender) through signing.

Authenticity of the Sender and Receiver is established with X.509 digital certificates, which are typically obtained through the HISP (refer to the section on Certificates below).

Provider Directories

1. What is the role of the Direct Project in the development of provider directories?

Under the Federal Advisory Committee known as the HIT Policy Committee, the Information Exchange Workgroup has established a Provider Directory Workgroup, which has been working to define issues, gather information and formulate recommendations; however, there is no timeline for the issuance of any standards for provider directories. In addition no strategy has yet been documented or recommended for organizing and governing provider directories. It is possible to initiate information exchange without a directory; however, Direct can support the creation of directories requiring only a place for (1) the universal Direct address and (2) the public certificate in that directory.

Certificate

1. What is a digital certificate and how is it relevant to Direct?

A digital certificate is a special electronic document—based on, in the case of Direct, the X.509 standard—that is tied to an individual or organization. It functions as a digital signature and ensures that an electronic transmission can be reliably traced to its source. It is also the means by which the identity of the individual or organization is bound to that entity's public key for encrypting the document.

2. What is a trust anchor?

Some entity must have the power to decide the criteria by which certificates may be issued for the purpose of message exchange within a given community. Such entities may include an HIE organization, a distributed IDN, a PHR system (e.g., HealthVault or Google Health), or a community of interest (e.g., NACHRI). This entity must have the ability to (1) at some level enforce compliance with community policies, and (2) physically issue certificates.

3. What are the criteria for a trust anchor?

Organizations implementing Direct specifications must configure what are called “trust anchors” to ensure common trust among information exchange participants who are

using Direct specifications. They can also delegate responsibility to their full-service Health Information Service Provider (HISP), or establish a trust anchor through a Business Associate Agreement or similar contractual document. The decision to add or not add a trust anchor has a significant impact on the privacy and security of health information exchange. Adding a trust anchor that does not ensure identity assurance, security and public key infrastructure management that meets a common high bar of trust may compromise the integrity of the exchange. For further information on trust enabling policy and decisions, refer to the Direct Project's Message Handling Policy <http://wiki.directproject.org/Security+and+Trust+Consensus+Proposal>.

4. What type of certification does Direct support? Is it specific to the provider organization? To the end-user? To both?

Direct supports a model where certificates can be unique to individual addresses (foo@hospital.com) or the domain for the collective organization (hospital.com). The community may choose to make a policy that requires certificates be associated with addresses; however, this places a significant additional burden on either the community or participating organizations to issue and manage a large number of certificates. Note that there is some momentum towards the use of individual certificates in the industry and the government, but this trend is not yet widely adopted.

Direct software does not *issue* certificates; it merely allows administrators to *associate* certificates with endpoints (user mailboxes) and domains (organizations). The certificates are issued by trust anchors, typically the HISP.

5. What should be the minimum requirements for identity verification and authorization?

A baseline policy might be simply that the participating organization has been physically verified to be a legitimate organization that sends or receives protected health information, and has confirmed their commitment to comply with HIPAA and/or other applicable regulations. This would provide basic assurance that the organization handles its technology systems in accordance with current expectations, including verifying identity in a manner consistent with at least NIST Level 2 for members and securing networks and data (see NIST special publication 800-63 http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf).

Community policy should recognize existing methods of identity assurance and authentication; for instance, hospital credentialing, certificate issuance for scheduled medication prescribing, and identity assurance and authentication required to gain access to EHR systems or EHR modules will often provide sufficient levels of assurance and authentication to issue certificates and private keys. In cases where such pre-existing methods do not exist, we recommend the following best practice for identity assurance for providers:

- Verify the place of practice, through means such as by contacting (e.g., by phone) the practice or provider through independently sourced contact information (e.g., white or yellow pages directories) or through knowledge-based methods (i.e. personal acquaintance or previous contact)

- Verify government-issued IDs and licensures, including search for licensure information in public registries.

For patient-focused organizations wishing to send Direct messages to an individual patient or a patient's authorized caregiver, a baseline policy that is agreed upon during the implementation of the initial phases may be that community members will only exchange messages with a patient address that was provided during an in-person clinical encounter in order to ensure that the HIPAA disclosure made in sending data to that address was authorized by an appropriate individual.

The identity and authorization requirements for certificate issuance must be uniform for issued certificates to have any meaning. Because identity assurance requirements will often be very different for certificates issued to patients and to patient organizations (e.g., PHR organizations) than those issued to providers, provider staff, and provider organizations, the trust anchors for each must be different.

Communities that are using one or more separate certificate authorities (CA) for certificate issuance should ensure that the criteria for certificate issuance of each CA are consistent with the requirements of the community. One role of the state/SDE would be to provide these baseline requirements for certificate authorities offering services for Direct-mediated exchange in the state.

6. How does Direct meet minimum certificate authority requirements?

Certificates can be issued at the community or national level. The Direct Project supports a model where certificates can be unique to individual addresses (bob@direct.hospital.com) or the domain for the collective organization (hospital.com). The community may choose to make a policy that requires certificates be associated with addresses; however, this places a significant additional burden on either the community or participating organizations to issue and manage a large number of certificates. The recommendation for organizational certificates is the same, regardless of whether the organization's system is hosted in an external data center, with a HISP, or located at the organization's premises.

Current requirements issued by ONC for Certificate Authorities include: 1) Conformity to any specifications and policies developed for issuing certificates, 2) If exchanging with a federal provider, adherence to federal certificate standards, 3) The ability to physically issue a certificate.

There are vendors (e.g., Verizon and AT&T) already contracting to provide certificate services. Additional information on certificate authority is located in the Direct Project's Policy and Technical Specifications document <http://wiki.directproject.org/file/view/DirectProjectOverview.pdf>.

7. How is trust established in the pilot projects?

The Direct Project is using standard X.509 certificates to verify identity, and is using those certificates to sign and encrypt messages to establish bilateral trust. Direct is designed around the concept of a “trust anchor”, so that, if any two communities share a common definition for a certificate and identity assurance, they can either use the same trust anchor or import each other's trust anchors, thus agreeing to share information with each other.

Organization Decision

1. Should our organization participate in Direct?

On a community-by-community basis, organizations should decide if:

- There is benefit in exchanging messages with other members of the community.
- They are willing to comply with the community policies required to obtain a community certificate.
- They are comfortable that the community policies provide adequate protection for exchange.

If the answer to all of these questions is yes, the organization can decide to participate by:

- Obtaining an organizational certificate from the community trust anchor
- Configuring the community trust anchor's certificate in their implementation
- Associating their new certificate with their organization

2. How should I format Direct addresses for my organization?

So long as addresses conform to the Direct address specification (in effect they are “normal” e-mail addresses), there is no additional requirement on how endpoint names are chosen or domains associated with organizations. However, it is recommended that:

- Fully qualified domains be allocated exclusively for the purpose of health information exchange; and
- The domain name not imply membership in a particular trust circle (in particular, not imply membership in the Nationwide Health Information Network)

Many organizations have chosen a pattern of "@direct.myorganization.org".

3. Can we re-use existing email addresses for Direct messaging? Can we re-use existing email clients for Direct messaging?

The core Direct Project specifications do not require special e-mail addresses or dedicated e-mail clients. Creating dedicated e-mail clients may, however, reduce the risk

of inadvertent use or mixing of business and clinical exchange functions.

Each organization should assess the risks and consider security, patient safety, impact on user workflow, likelihood of user error, etc. Similar analyses conducted for the Threat Models for simple SMTP and SMTP with Full Service HISPs may also be useful to consider. The use of dedicated e-mail domains for exchange and dedicated e-mail clients may reduce some of these threats.

Learn More and Get Involved

1. How do states get involved in the Direct Project and the pilots?

Information is updated frequently as consensus and direction evolves. The best source of up-to-date information is the Direct homepage (<http://www.directproject.org>). The Direct wiki (<http://wiki.directproject.org>) is a place to learn more about the project and current related activities.