DirectTrust

The most trusted names in health information exchange.

The Mission of DirectTrust is to support health information exchange that is secure, interoperable, affordable, and widely available, in the interest of the public good, and to do so as a non-profit, competitively neutral, membership 'learning organization' for voluntary self-governance of health information exchange.

What is Direct Exchange?

Direct exchange, also known as Direct messaging or simply, Direct – is a type of secure e-mail designed to connect users of different health IT systems in different organizations, thus creating interoperability. All users of Direct exchange possess Direct addresses of the type *name@direct.SunnyFamilyPractice.com*, and can send and receive messages plus attachments regardless of vendor or operating systems being used. To users, the Direct exchange experience is like regular e-mail. However, in the background Direct exchange service providers – known as HISPs – assure that the messages and attachments are encrypted and the identity of the users is validated in compliance with HIPAA privacy and security. These additional privacy, security and identity controls are what makes Direct exchange a safe way to move sensitive personal health information between providers, and between providers and their patients. Direct attachments can be any type of file format, e.g. XML, Word, PDF, image files, etc. Direct exchange is rapidly replacing less secure and non-electronic forms of communications based on paper documents, such as fax, e-fax, courier, and mail.

What is DirectTrust?

DirectTrust is a collaborative non-profit alliance of 123 healthcare organizations whose common goal is to accelerate the adoption of interoperable health information exchange with a focus on Direct. DirectTrust serves as the membership, policy and governance body for a vibrant community of Direct exchange participants, who have voluntarily established a Security and Trust Framework that serves as the "rules of the road" for Direct exchange.

There were 35.6 million Direct exchange transactions in the first quarter of 2017, an increase of 76% over the same period last year. DirectTrust anticipates transactions totaling 140 million by the end of 2017.

The Framework prescribes the technical, legal, security, and identity policies and practices that all members of the community agree to follow. In addition to the Framework, DirectTrust put in place a program of Accreditation and Audit (DirectTrust HISP Accreditation and DirectTrust-EHNAC CA/RA Accreditation) that transparently verifies the adherence of all DirectTrust service providers and their customers to the Framework's criteria. Federation of trust relationships allows the entire network to operate and grow at scale, without the need for individual one-off negotiations or costly legal contracting between exchange partners.

An analogy with Visa or MasterCard is helpful in understanding DirectTrust's role: DirectTrust is to confidence in the security of health information of trading partners using Direct, as Visa or MasterCard is to the acceptance by merchants for the payment of a good or service using credit cards. DirectTrust itself does not move or hold data and information, just as Visa doesn't handle any funds itself.   But the policies, legal agreements, and practices of each enable a federation of trust to thrive, and thus permit exchanges to occur at very large economies of scale.

Learn more at: DirectTrust.org

Participants in the DirectTrust Network

On the services side, DirectTrust participants include HISPs, Certificate Authorities (CAs), and Registration Authorities (RAs). On the user side, DirectTrust participants include vendors of applications of many kinds, users of those apps, and healthcare organizations of all sorts, including hospitals, medical practices, long term care facilities, payer organizations, laboratories, and so on. Patients and consumers can and do participate in Direct exchange through their providers' portals or stand-alone PHRs and patient facing applications. The great majority of Direct exchange users are in the private sector. But use by a number of Federal Agencies of Direct exchange under the DirectTrust umbrella is growing.

As of early 2017, the DirectTrust Network connects the following participants:

- 40+ Health Information Service Providers, or HISPs
- 400+ Direct-enabled, ONC certified EHRs and PHRs
- 94,000+ health care organizations, hospitals, and medical practices
- 50+ Health Information Exchanges, HIEs, in 20 states
- 2 Federal Agencies
- 1.4 Million Direct address holders or end-points
- Over 35.6 Million Direct exchange transactions in Q1 2017, over 140 million expected in 2017

What are the benefits of joining DirectTrust?

Membership benefits include:

Opportunities to influence and shape the DirectTrust Trust Framework;

Access to DirectTrust deliverables and intellectual property, as well as participation in workgroups;

Insight into the work being done by your colleagues in the community;

Up to date information about the continually evolving regulatory environment; and

Discounted access to DirectTrust products.

View this Benefits of Direct Messaging document for an overview of how Direct exchange in action:
(http://www.softwareadvice.com/resources/direct-messaging-for-ehr-interoperability/)

Learn more at: DirectTrust.org

DirectTrust Security and Trust Framework Components

Policies and Practices: DirectTrust policy and practice documents include the technical specifications of the Applicability Statement, ONC's technical framework for deployment of Direct; the DirectTrust Certificate Policy and HISP Policy documents; HIPAA Security and Privacy Rules; and numerous additional industry and federal policies and practices used as guidance and reference for security and trust in identity.

DirectTrust HISP Accreditation and DirectTrust-EHNAC CA/RA Accreditation: Accreditation and Audit of HISPs by DirectTrust and CA, and/or RA by DirectTrust-EHNAC brings recognition that these organizations and their customers operate at a very high level of privacy, security, and trust in identity, and signals to users/subscribers that these are trustworthy agents and service providers for Direct exchange deployments. DirectTrust HISP Accreditation and DirectTrust-EHNAC CA/RA Accreditation and Audit are requirements for all parties who wish to participate in one or more of DirectTrust's Trust Anchor Bundles.

Legal Agreements: DirectTrust provides standard brief legal agreements including the Federated Services Agreement and the Federated Services Agreement CA/RA addendum. These agreements allow participants to agree on one set of legal/trust documents to enable the exchange of data with all other participants. An example of the terms of the FSA is that all signatory HISPs and RAs agree not to charge one another any fees for transmission of basic messages and attachments sent over the DirectTrust network.

Governance: A trust community like that of DirectTrust is a living, evolving and very dynamic ecosystem which requires constant oversight and supervision, and occasional enforcement, to assure that trust is maintained and that no one "breaks the rules." The chain of trust for Direct or any secure transaction in health care is only as strong as its weakest link. Therefore, DirectTrust's Board of Directors, and the several Committees and Workgroups which meet regularly, are constantly reviewing policy and assisting new network members and all participants to maintain a state of vigilance with respect to adherence and compliance. In addition, DirectTrust's partner in the Accreditation and Audit process for CA/RA, EHNAC, attends to policy and compliance questions and issues on a regular basis on its own, and through liaison committee meetings with DirectTrust leaders.

Trust Anchor Bundles and Network Services: DirectTrust policy and practice requirements extend to the infrastructure DirectTrust maintains for distribution of trust anchor certificates. These are digital certificates that network participants use to verify the identity, accreditation status, and security elements in place at the time of Direct exchanges, in much the same way that web browsers use trust anchor certificates to verify the authenticity of web sites and to create secure sessions for browser-to-website transactions. Once qualified through a painstakingly thorough review process, a HISP and its partner CA earns the privilege of placing its trust anchor certificate in one of the DirectTrust Trust Anchor Bundles, which is a collection of these trusted digital credentials available for use by the community.

Learn more at: DirectTrust.org