DataMotion

/ Whitepaper

Direct Secure Messaging: Improving the Secure and Interoperable Exchange of Health Information

Within the healthcare industry, the exchange of protected health information (PHI) is governed by regulations such as HIPAA and the HITECH Act, which require adequate security be used to protect the information contained in personal health records from accidental or malicious public disclosure. In addition, the regulations seek to encourage electronic health information exchange to both improve the quality of patient care while reducing the cost, through the Health and Human Services agency incentive programs such as Meaningful Use.

For data in motion, proprietary email encryption is a viable and frequently used technology to meet HIPAA security requirements. But inspite of the availability of email encryption services to achieve efficiency in the secure exchange of PHI, until recently, most PHI has been exchanged via fax, in person or through the mail. The critical needs of clinical health information exchange over the internet requires the adoption of a more robust and integrated secure messaging technology. This technology needs to go beyond typical email encryption to include:

- Service interoperability and service provider accreditation
- Address holder identity validation
- End-to-end trust and accountability
- Integration with electronic health record systems (EHRs)

These needs were recognized by the US Department of Health and Human Services, and as part of the HITECH Act, the Office of the National Coordinator initiated a new approach in 2010. Defined as the Direct Project, it specified a secure, scalable and standards-based method for the exchange of PHI across a virtual health information service provider network (also known as Direct Secure Messaging, Direct Exchange, DSM and just 'Direct'.)

New Solution: Direct Secure Messaging (aka 'Direct')

As a specific secure messaging technology for healthcare, Direct is designed to go beyond HIPAA compliance requirements offering a comprehensive set of compliance, interoperability and accountability features, beyond those available in standard email or proprietary email encryption services (see figure 1).

Direct is a universal communications method for sending patient information, which can address gaps in quality of care on the clinical side. One use case example is during transition of care, which has been identified as a significant patient safety issue. Incomplete exchange of patient health information among providers when discharging or referring a patient from one care environment to another is a point of vulnerability that can compromise the overall quality of care a patient receives. Integrating Direct with EHR systems to exchange health records between care settings to improve this transition is the leading use case for Direct.

CONTACT US WITH QUESTIONS:
Toll-Free: 1.800.672.7233 Tel: 1.973.455.1245 Fax: 1.973.455.0750
Email: info@datamotion.com www.datamotion.com
DataMotion, Inc. 200 Park Ave Florham Park New Jersey 07932

To reduce costs on the business side, Direct matches the efficiency of generic email encryption by reducing inefficiency associated with unformatted fax data and workflows, and by transitioning relatively expensive, paper-based fax communication to less expensive data communication workflows.

Figure 1: Electronic Messaging Comparisons

Email	Encrypted Email	Direct Secure Messaging
Standard Message Format	Standard Message Format	Standard Message Format
Internet Delivery	Internet Delivery	Internet Delivery
	Proprietary Encryption	Standards-Based Encryption
	Supports Regulatory Compliance	Supports Regulatory Compliance
		Supports Interoperability*
		Identity Validation
		End-to-end trust & accountability

*interoperability between Direct Secure Messaging address holders regardless of the health information service provider (HISP)

Direct Secure Messaging is expected to provide many benefits including:

- One unified standard that is vendor agnostic
- Regulatory compliance for the security and privacy of PHI
- Improved clinical communications
- Simplified patient referral management and reporting
- ONC deemed standard and foundation for CONNECT
- Improved practice workflow and related cost reduction

How does Direct Secure Messaging work?

In many ways, Direct is implemented and used just like email. Its benefits for the healthcare industry are incorporated into the methodology and technology within the virtual Direct Secure Messaging network that operates over the Internet. Direct can be integrated into a variety of user interfaces such as an email client, a mobile device, and healthcare IT system portals or as an automated data delivery feed. Any of these interfaces are capable of sending or receiving Direct messages. Healthcare IT systems such as EHRs can also integrate Direct in multiple ways depending on the desired workflow.

In order to use Direct, both sender and recipient users need a specific Direct Secure Messaging address, which can be assigned to organizations, individual providers, and even patients.

DataMotion

/ Whitepaper

Direct Secure Messaging Addresses

A Direct address has a similar structure as an email address.

Direct address example: your.name@direct.clinic-name.org

Although this looks like a standard email address, it is different. Like standard email, Direct uses the SMTP protocol, and both use the Internet for delivery. In addition, Direct has two components standard email does not: an identity validation component, and a secure encryption component.

Where can you get a Direct Secure Messaging address?

Direct Secure Messaging addresses and services are provided by a Health Information Service Provider or HISP. The term 'Health Information Service Provider' has been used by the Direct Project both to describe a function (the management of security and transport for directed exchange) and an organizational model (an organization that performs HISP functions on behalf of the sending or receiving organization or individual).

A HISP's services are instrumental in the delivery of Direct Secure Messaging services. The HISP issues Direct Secure Messaging (Direct) addresses and attach certificates that validate sender and recipient identities to those addresses. A HISP also provides the secure messaging network operations to make sure your messages are delivered securely to the intended Direct-enabled recipient with end-to-end trust and accountability.

HISP responsibilities:

- Provide your Direct address
- Enable backbone transport for interoperable HISP to HISP message transport
- Publish digital certificates to establish trust
- Package message contents using Direct standards and specifications
- Encrypt content and attachments to secure confidentiality and integrity
- Ensure authenticity of sender and recipient

Since the introduction of the Direct Project, many HISPs have entered the market to facilitate the use of Direct Secure Messaging within the healthcare industry. Since Direct was established as a secure messaging standard – every HISP is required to interoperate in order to efficiently exchange secure messages between their respective subscribers. A HISP accreditation process established by the Direct Trust and the Electronic Healthcare Network Accreditation Commission (EHNAC) helps ensure that individual HISPs are in compliance with the Direct Secure Messaging specification and service delivery.

DirectTrust EHNAC ACCREDITED DTAAP HISP

CONTACT US WITH QUESTIONS:
Toll-Free: 1.800.672.7233 Tel: 1.973.455.1245 Fax: 1.973.455.0750
Email: info@datamotion.com www.datamotion.com
DataMotion, Inc. 200 Park Ave Florham Park New Jersey 07932

Identity Validation and Certificates

When a HISP receives an application for a new Direct address, the first step in issuing the address is validating the identity of an applicant. Validation can be done in two ways. One, by using a government issued ID or two, by have a previously established relationship with an entity that has already been validated. Once the identity is validated, an X.509 certificate is issued to the applicant. The certificate is used to automatically confirm the address holder's identity every time a message is sent or received using the Direct address. The X.509 certificate becomes the baseline for both identity validation and encryption.

There are three different entities that play a role in issuing X.509 certificates:

Registration Authority (RA) - confirms the identity of the Direct address applicant (either an individual or an organization).

Certificate Authority (CA) - issues the digital X.509 certificate.

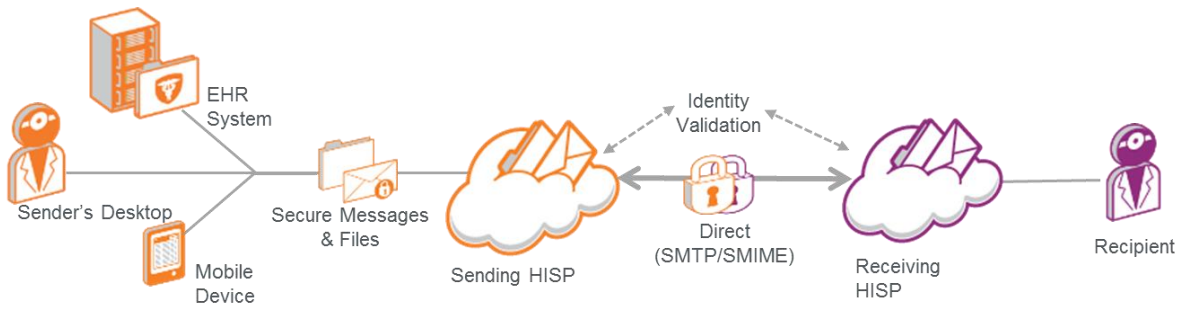
Health Information Service Provider (HISP) - facilitates the actual Direct communication by managing the relationships with the X.509 certificate, the exchange of the information, the encryption keys and moving the Direct message from point A to point B.

Sometimes HISPs will also assume the CA and RA roles when issuing new Direct addresses to applicants to expedite the process and promote scalability.

Sending Direct Secure Messages

The initiating sender sends their message using the recipients Direct address, which is routed over the virtual health information service provider network. The originating HISP gets the public certificate from the receiver, validates the identity, encrypts the message, and passes it to the receiving HISP, who then decrypts and moves the message into the receiver's inbox. Everything that occurs from the sender to the recipient is compliant to PHI regulation by ensuring privacy through identity validation, and security through encryption.

Figure 2: Sending a Direct Secure Message



DataMotion

/ Whitepaper

Direct Secure Message Delivery Notification

Message Delivery Notifications, or MDNs, are a fundamental component of Direct, which confirm delivery of the message The MDNs are delivered from the sending to the receiving HISP. Unlike traditional email Direct does not have read receipt functionality. Message delivery may just mean that the the message has been received and processed by the receiving HISP.

Practical Uses for Direct Secure Messaging

The original intent of Direct was to replace the use of fax and paper when discharging patients from one care setting to another, such as from a hospital to a long term care facility. This is the use case for meeting Meaningful Use objectives for transitions of care. Yet the capabilities of Direct go well beyond this use case. The following use cases are just a few examples of where Direct can serve the healthcare community.

Direct Secure Messaging Use Cases:

- Lab orders and reports transmitted to the ordering physician
- Sending data to public health organizations and registries
- Obtaining pre certifications and prior authorizations for services
- Referrals
- Secure patient-provider communications
- The curb-side consult
- Research exchange

Summary

The future of healthcare is focused on outcome-based medicine. Positive outcomes are the natural progression of the best minds sharing and interacting to find the best course of treatment for their patients. Healthcare providers who incorporate Direct Secure Messaging into their workflows gain a secure, interoperable and efficient communication tool to support improved dialog between providers, patients, and their care teams, while meeting regulatory requirements, government mandates and in some cases the benefits of financial incentives.

Across the healthcare continuum, the adoption of Direct Secure Messaging can ultimately provide a higher level of care and better outcomes; a scenario that all involved clearly want and are trying to achieve.

ABOUT DATAMOTION

Our mission is to dramatically reduce the cost and complexity of exchanging private health information in a secure and compliant way! Our easy-to-use encryption solutions for Direct Secure Messaging, secure email, file transfer, forms processing and customer contact leverage the DataMotion Platform for unified data delivery. As a provider of secure messaging solutions such as email encryption and Direct Secure Messaging – we are constantly engaged by providers to help them stay in compliance with expanding regulations, including HIPAA and HITECH. We are an EHNAC accredited Health Information Service Provider (HISP), and actively promote the adoption of Direct Secure Messaging across the healthcare industry. DataMotion is privately held and based in Florham Park, N.J.