Demystifying Direct Messaging

Orion Health Whitepaper
Author: Paul de Bazin, Integration Portfolio Manager
Table of Contents

1 Introduction .......................................................................................................................................................... 3
2 Background .......................................................................................................................................................... 3
  2.1 Standard Use Cases ....................................................................................................................................... 3
3 Direct Messaging standards ............................................................................................................................... 3
4 How does direct messaging work? ................................................................................................................... 4
  4.1 Workflow ....................................................................................................................................................... 4
5 What does a HISP provide? .................................................................................................................................. 5
6 What are the meaningful use requirements regarding direct messaging? ......................................................... 6
7 Should an organization become a HISP? ........................................................................................................... 7
8 Does direct replace traditional HIEs? ............................................................................................................... 7
9 What does Direct Messaging mean to your organization? ................................................................................. 8
  9.1 Direct for Integrated Delivery Networks (IDN) and Providers ......................................................................... 8
  9.2 Direct for Public Health .................................................................................................................................... 8
  9.3 Direct for Health Information Exchanges ...................................................................................................... 8
  9.4 Direct for Payers .............................................................................................................................................. 9
10 Summary .......................................................................................................................................................... 9
Demystifying Direct Messaging

1 INTRODUCTION

Direct Messaging is a relatively new initiative promoted by the Office of the National Coordinator (ONC), and has been adopted as the key information exchange technology required to comply with stage 2 Meaningful Use. However, general understanding of Direct in the healthcare industry is still limited. This document aims to demystify the Direct Messaging standards and how they impact clinical workflow throughout the country.

2 BACKGROUND

Effective and efficient communication between care providers has been identified as a key contributing factor to providing better patient care and lowering healthcare costs. On average, primary care physicians in the United States have to interact with 229 other doctors in 117 different practices, but, in spite of a recent increase in EHR adoption, without a broadly adopted standard for secure electronic communication in the U.S., many providers still remain reliant on paper, phone, fax and physical transport to pass patient information between organizations. These methods are slow, unsecure and add significantly to administration overhead.

Direct Messaging offers the healthcare industry a universal, secure messaging exchange method that can help to bring it into the 21st century. Combined with the recent nationwide adoption of standard formats, such as the care summary Continuity of Care Document (CCD), Direct Secure Messaging allows physicians located anywhere to quickly send accurate patient information to other trusted parties. This not only reduces administrative overhead, it also increases the security of patient records and ensures that records reach their intended destination in a complete and auditable way.

The vision of a Direct-enabled healthcare system is to provide a secure healthcare network where all participants are verified and can securely communicate with anyone else within this network. This connectivity will empower clinicians, administrators and systems to securely share information.

2.1 Standard Use Cases

A number of “standard use cases” for Direct Messaging are being promoted by the ONC and others as a way to encourage the uptake of the standards. These represent the common scenarios in which early adopters have used Direct Messaging but are only a small set of possible use cases:

- Referrals between organizations and clinicians
- Discharge summaries sent to the Primary Care Provider (PCP)
- Lab reports transmitted to the ordering physician
- Sending data to public health organizations
- Prior authorizations for services
- Transmit care summaries as part of the Meaningful Use stage 2 View/Download/Transmit requirements
- Secure patient-provider communications

However, Direct Messaging can be used for a range of other tasks where secure communication is required. In the future, it is likely that exchanging Direct addresses will be all that’s required to securely share information. Other secure networks will only be required for specialized communication tasks – such as the sharing of high definition medical images.

3 DIRECT MESSAGING STANDARDS

Direct Messaging utilizes proven secure standards being used by many other industries and adds some additional healthcare specific standards from Integrating the Healthcare Enterprise (IHE).

---


The key standard adopted is the use of encrypted email as the basis for the Direct exchange. Secure email uses a standard called S/MIME (or secure MIME) for the exchange of encrypted emails. This same set of standards can be utilized by advanced email clients and is supported by many different development tools and libraries. This should ensure that vendors are able to easily adopt the “new to healthcare” standards. At the simplest level, supporting Direct requires email capabilities, support for the right encryption algorithms and the recipient’s certificate so that the message can be encrypted for the specific reader.

However, secure email is traditionally implemented in a specific domain and for specific use cases. This means that there is one central body responsible for the verification and allocation of identities and certificates. The healthcare industry doesn’t work in this manner, so standards for the automated discovery and retrieval of certificates were also incorporated. These certificate discovery services utilize DNS and LDAP technologies and allow systems to dynamically find the recipients’ certificates across the internet.

In addition to the S/MIME standards, Direct messaging also incorporated the IHE standard for point-to-point messaging already in use by many healthcare technology vendors. The Cross Enterprise Reliable Interchange (XDR) interface can be used as an alternative to the S/MIME standards.

4 HOW DOES DIRECT MESSAGING WORK?

Direct Secure Messaging is a secure network for the exchange of healthcare information. Users can locate recipients’ Direct addresses, securely encrypt the information and ensure that information is delivered appropriately. In order for this to occur, organizations join Healthcare Information Service Providers (HISPs).

HISPs are responsible for the formation of a trust network that ensures that verified users of one HISP network can communicate with verified users of another HISP network. A HISP can be thought of in the same way as an Internet Service Provider: It provides a healthcare-specific service that enables connection with other healthcare organizations – but the connectivity is all based on secure trust relationships that the HISP maintains.

In the Direct Secure Messaging system, each organization is assigned a secure certificate key pair that is used to encrypt the information sent to them. The public key is used by senders to encrypt the message, and the private key is used for decrypting the message. The private key of the sender is also used to sign the encrypted message. This allows the recipient to accurately validate the sender of the message.

Users can be assigned an individual-level certificate, but it is industry standard for all users in an organizations to share a common certificate. This reduces the cost and overhead associated with maintaining users in the system.

The encryption of the data can be provided by either the originating system, or the HISP can be used to encrypt the information. The system performing the encryption is called a Security Trust Agent (STA). If the HISP performs the Direct-compliant encryption, the communication between the organization and the HISP utilize any secure protocol.

4.1 Workflow

1. When a user sends a message, the sending system signs the content with the sender’s private key, and encrypts the message with the recipient’s public key. The encrypted message is then sent via one of the supported protocols to the destination.
   • The encryption can be performed either by the user’s software system, or the HISP can perform the task of encrypting the data (as long as the connection to the HISP is secured).

2. Messages can be delivered to any domain within the trust network using the Direct Messaging standards. The trust network consists of any organizations using a HISP that shares a trust relationship with your organization’s HISP.
   • The HISPs are responsible for routing the messages to the correct location, based on the Direct address used and for delivering it in the format supported by the recipient’s organization.

3. Once the message is received by the recipient’s system, it is decrypted with the recipient’s private key. The secure signature of the message is also checked to ensure that the message was actually sent by the person claiming to send the message. This is called non-repudiation.

The encryption of the data can be provided by either the originating system, or the HISP can be used to encrypt the information. The system performing the encryption is called a Security Trust Agent (STA). If the HISP performs the Direct-compliant encryption, the communication between the organization and the HISP utilize any secure protocol.
Diagram 1 – The sending organization uses a Direct-compliant HER system to encrypt and send the Direct messages.

Diagram 2 – The sending organization uses a secure, but not Direct-compliant message to the HISP, where it is encrypted using Direct-compliant standards before being transmitted to the end recipient.

5 WHAT DOES A HISP PROVIDE?

A HISP is the organization that provides connectivity and trust network services to an organization utilizing Direct Messaging. The HISP facilitates connection to other users of Direct Messaging by ensuring that messages are securely sent to the recipient using the correct edge protocols (e.g., XDR or S/MIME).

A HISP can be used to encrypt the data on behalf of an organization and should support the technology requirements of a range of organizations. Connections to the HISP must be via a secure communication channel, but are not required to use the Direct Messaging standards. Organizations and HISPs can use any secure communication the HISP supports, but the HISP is responsible for ensuring compliance with Direct Messaging when communicating with users of other HISPs.

The HISP is typically responsible for managing and sharing organization certificates via Direct-supported standards. The HISP is also responsible for connecting a trust network with other HISP organizations. This trust network allows the users within one HISP to communicate with users of another HISP. This HISP-to-HISP agreement, or building of the trust network, needs to occur due to the closed nature of the secure Direct Messaging network. Only validated participants can share messages on the network, and the HISP-to-HISP agreements ensure that unauthorized users cannot make use of the secure network. This security also provides protection against unsolicited mail messages (spam) because the sender is always identified within the network.

A high-quality HISP will provide:

• Support for a diverse range of technical capabilities
  o A web-based mail portal with accessibility support
  o Support for EHR systems with integrated Direct project standards support; including S/MIME messages and IHE XDR standards
  o Support for standard email clients and custom interfaces
• Protocol transformation and routing: SMIME/SMTP, IHE XDR, web services
• Support for managing the encryption and decryption at the HISP level
• Certificate issuance and certificate lifecycle management using certificates from a certificate authority approved at the federal level
Many HISPs also provide traditional Health Information Exchange (HIE) services. These organizations provide the benefit of not only having a secure messaging infrastructure, but also the ability to integrate the secure messaging with the patient record and clinical information. When combined, the HIE’s clinical record becomes even more valuable because the information can also be shared with those not affiliated with the HIE. A standards-based Continuity of Care Document (CCD) can be generated and sent to a third party using standards-based Direct Messaging.

This clinical integration provides users with other rich features, such as the ability to provide secure notifications (to a Direct address) based on clinical events in the community and offers the best value when evaluating HISP organizations.

6 WHAT ARE THE MEANINGFUL USE REQUIREMENTS REGARDING DIRECT MESSAGING?

The 2011/2012 Edition (Stage 1) Meaningful Use requirements are largely silent on the use of the secure health transport using Direct to meet meaningful use objectives. Stage 1 objectives are largely concerned with the structure and formatting of content being exchanged as a CCD containing specific information and using specific vocabulary standards. Stage 1 is less concerned about the security and transport of that content using Direct or any other mechanism. ONC suggests that the Direct Project may satisfy some Stage 1 Meaningful Use requirements, such as a primary care physician referring a patient to a specialist and exchanging a clinical summary in support of the consultation. However, there are no certification criteria under Stage 1 that specifically examine any usage of Direct.

The 2014 Edition (Stage 2) Meaningful Use requirements change this picture dramatically to incorporate Direct. Stage 2 makes use of secure health transport in a variety of objectives targeted towards both the ambulatory (Eligible Professional) and inpatient (Eligible Hospital) domains. In the Meaningful Use test objectives, secure health transport technology is referred to as the “ONC Applicability Statement for Secure Health Transport” and the “ONC XDR and XDM for Direct Messaging Specification”.

The specific test objectives that utilize Direct are:

<table>
<thead>
<tr>
<th>TEST #</th>
<th>DESCRIPTION</th>
<th>DOMAIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>170.314.b1</td>
<td>Transitions of care – receive, display and incorporate transition of care/referral summaries</td>
<td>Inpatient and Ambulatory</td>
</tr>
<tr>
<td>170.314.b2</td>
<td>Transitions of care – create and transmit summary care records</td>
<td>Inpatient and Ambulatory</td>
</tr>
<tr>
<td>170.314.e1</td>
<td>View, download and transmit to a 3rd party</td>
<td>Inpatient and Ambulatory</td>
</tr>
</tbody>
</table>

Of particular note, test objective 170.314.e1 “View, download, and transmit to a 3rd party” requires EHR technology to allow patients and their authorized representatives to download and transmit the ambulatory summary, inpatient care summary or referral summary to a third party entity. The patient and the patient’s representative must both be able to securely transmit the information using Direct.

In all cases, eligible providers and eligible hospitals can qualify for Meaningful Use incentive payments using Stage 2 certified electronic health record technology, as long as that technology has the ability to receive, create, display, incorporate, download and transmit standards-compliant health information using Direct or optionally using XDR and XDM.

When testing Direct transport, Meaningful Use requires that technology vendors identify and demonstrate the ability to discover and utilize Direct security certificates, as well as domain-bound certificates hosted in both DNS and LDAP. Testing validates the proper usage of valid and invalid certificates, proper data encryption, proper audit logging processes and inspection of the receipt of exchanged content for
accuracy and compliance. A series of online testing tools developed by the ONC and the National Institute of Standards and Technology (NIST) help vendors and test proctors evaluate each of these steps.

7 SHOULD AN ORGANIZATION BECOME A HISP?

Many organizations looking to implement Direct are trying to determine how they can best meet the Meaningful Use Stage 2 criteria. Under the certification criteria for Stage 2, EHRs will be required to support Direct Messaging, and be capable of discovering certificates, validating certificates and encrypting/decrypting the messages. However, EHRs or other Direct-compliant messaging systems still require the services of a HISP in order to participate in the Direct ecosystem. As part of this investigation, organizations are examining whether they need to become a HISP, or whether they sign up to one of the established HISP services available in the market.

In general, the technical components used by Direct messaging are widely used and available from a number of different sources and vendors. There is even a Direct-specific, open source reference implementation that can be used for the encryption and decryption of messages at an organization boundary. Technically, it is possible for an organization to implement the reference implementation and then manage DNS and LDAP servers for the discovery of their certificate. The organization could then contact other HISP organizations and start building their own trust network.

However, the technical aspects of Direct project integration are only one part of the problem. Once an organization becomes a supplier of HISP services (even just to their own employees), there are legal and security requirements that must be enforced. These requirements ensure the organization adheres to HIPAA legislation and will be required for many HISP-to-HISP agreements.

Direct Messaging is also in its infancy and, in reality, the expectations of the role of a HISP are continuing to evolve. There is much discussion around the additional requirements for a Healthcare Provider Directory (HPD), and a HISP certification process is expected to be established in 2013. This will provide increased universal communication, but will place additional requirements on HISPs.

Joining a full service HISP can simplify the process of becoming Direct-enabled. The HISP will isolate your organization from major changes in HISP requirements and HISP certification. Joining a HISP will offload the following responsibilities and costs:

- Certificate issuance and registration authority: Allow the HISP to manage the relationship with the certificate authority, generate key pairs and certificate requests, obtain and distribute keys and certificates, and provide access to certificate validation services
- Certificate lifecycle management: manage distribution, keystore, inventory, expiry, renewal, revocation and other maintenance actions
- Directory services: Deliver and manage the Provider Directory (HPD+) supporting discovery of Direct addresses and certificates
- Certificate discovery services: Allow the HISP to establish and maintain the DNS and LDAP interfaces for certificate discovery, which reduces the IT expenditure to deploy Direct in the organization
- HISP certification: Allow the organization to be protected from HISP certifications or requirement changes
- Trust network: Manage the procedural process of establishing trust with other HISPs, and the technical process of maintaining certificate Trust Bundles or Trust Lists
- Routing and transformation services: Manage the protocol and payload transformations required to exchange Direct Messages among differing Direct implementations eg SMTP/SMIME – SOAP/XDR
- High-availability and disaster recovery: Operate all of the HISP services as a highly available, highly scalable, secure and redundant service
- Support: Provide 24x7 support services

Many statewide health information exchange organizations are funded to provide low cost Direct services to organizations joining the statewide HIE. This can offer benefits beyond the Direct Messaging connection and should be thoroughly reviewed by any organization looking to implement Direct.

8 DOES DIRECT REPLACE TRADITIONAL HIES?

Direct provides a new way for healthcare organizations to exchange information and can have a significant impact in cost reduction and workflow efficiency, but what does this mean for traditional HIES?

Traditional HIEs provide access to a consolidated patient record, built from information sourced from many different systems and organizations. They provide important summary information at the point of care, along with the ability to run business analytics over the aggregated patient record. The information exchange is based on the clinical user “pulling” the information from the HIE.
Direct messaging provides event-based communication, and does not make any statements about the content of the messages. Clinical content may include a complete patient record, a partial record or no clinical information at all (the content is determined by the sender). In this way, Direct Messaging is a “push-based” system and cannot provide information at the point of care when patient information is required. This “pull” of information is best provided by a traditional HIE.

So, Direct messaging and traditional HIEs are complementary offerings that work together to provide a complete integration solution. If the clinical team needs to send information to a known entity or person, they use Direct. If the clinical team is looking for complete patient information, then the traditional HIE can provide the answers.

A leading HIE will integrate Direct Messaging with the HIE’s clinical record to provide users with both a complete patient record and a standards-based mechanism for exchanging that information with users outside the HIE. This can greatly increase the value of the HIE data because it can be shared even when the care giver has no relationship with the HIE. The care giver just needs to be a recipient of a Direct message with the attached clinical information.

Direct messaging can also be used to communicate with traditional HIEs – both for the submission of data to the HIE, and for event-based messaging and notifications coming from the HIE.

9 WHAT DOES DIRECT MESSAGING MEAN TO YOUR ORGANIZATION?

9.1 Direct for Integrated Delivery Networks (IDN) and Providers

Under the Stage 2 Meaningful Use requirements, each organization is required to be able to send and receive clinical summaries via Direct Messaging.

IDNs and providers should make sure that their EHR vendors are implementing the Direct Messaging standards, and are coupling the technology with the clinical record in a way that works with the clinical workflow of their physicians. By empowering clinical teams to quickly and efficiently use Direct Messaging, the organization can achieve efficiencies in administrative tasks and clinical workflow.

Providers should ensure that the Direct Messaging becomes tightly coupled with their clinical record to allow attachment of human-readable and programmatic clinical data to messages. The clinical record should also allow the import of documents from Direct Messages into their clinical record so that the content itself becomes a part of the auditable clinical record, and is not only held in the secure mail system.

Direct Messaging can also be a great method for driving electronic referrals to an organization with small clinics and ambulatory providers utilizing Direct Messaging – even if their technical infrastructure is low.

9.2 Direct for Public Health

Direct Messaging offers public health authorities a secure and consistent, standards-based exchange that can replace many of the custom solutions in use today. For instance, the public health information network messaging service (PHIN-MS) was designed as a secure, standards based system. However this system was only adopted within the public health domain and included many complexities in deployment.

Direct Messaging offers the ability to consolidate the different technologies and standardize on a secure technology that will provide universal connectivity.

Direct Messaging not only offers a method for the secure communication of electronic alerts between organizations, public health departments and the Centers for Disease Control and Prevention (CDC), it also offers a secure channel to communicate directly to clinical teams within an organization or region. During outbreaks of notable public health events, departments of health can utilize Direct Messaging to notify and inform the clinical community in a way that’s secure, simple and well adopted.

As organizations and EHR systems are being incentivized under stage 2 Meaningful Use to deploy Direct-compliant systems and for sending public health data to health departments, public health organizations should prepare for the electronic reception of public health data from providers using Direct Messaging. As the utilization of Direct Messaging grows, public health officials will be able to grow networks of Direct-enabled clinicians for notifications and follow-up enquiries on reportable encounters.

9.3 Direct for Health Information Exchanges

Traditional HIEs and Direct Messaging are complementary services that form the foundations of coordinated care and a cost effective, patient-centric system. These two solutions can be integrated to provide a number of different services to the HIE community. Most notably, the HIE can use Direct Messaging to:

• Receive clinical data feeds from participating organizations
• Provide clinical notifications of events in the community based on patient-provider relationships
• Allow clinicians to send information from the HIE to their primary clinical system
• Allow clinicians to send information from the HIE to a care provider not associated with the HIE

Other integrations and services will develop over time as market need and adoption of Direct Messaging identifies additional opportunities.

9.4 Direct for Payers

Direct Messaging does not yet have a significant foothold in the insurance market, and progress in this area is not yet clear. The usage of secure email as the core for Direct Messaging ensures simplicity and a proven technology, but also incurs limitations around the management of large files. While the secure transmission of claims seems like a good use for the new secure network, the size of large claims can cause technical issues with the use of the secure Direct Messaging standards.

There are also existing networks in place across the nation for the management of claims data and these networks are unlikely to migrate to Direct Messaging standards in the short term.

However, many other interactions with payers can be streamlined using Direct Messaging. Direct Messaging enables a single, secure mechanism for communication with multiple payers for all of the irregular exchanges that occur around the claims process. For instance, in some regions, prior authorizations for procedures are already being exchanged using Direct Messaging. When paired with national standards for clinical summaries (the CCD), and legislative changes in the industry, payers will find Direct Messaging offers great flexibility and the ability to improve productivity.

It is likely that payer-specific workflows will increase as more organizations adopt Direct Messaging.

10 SUMMARY

Direct Messaging provides a standard, vendor-agnostic method for the secure communication of healthcare data. The workflow optimizations and efficiencies gained by having this universal exchange will positively impact physicians' day to day activities and an organization's bottom line. And with the inclusion of Direct Messaging to obtain Meaningful Use stage 2 compliance, there is a clear commercial driver that will accelerate adoption through 2013 and beyond. It's fair to say that Direct messaging is a "must have" technology for every organization.

To gain the full benefits of a Direct Messaging exchange, an organization should look for a full-service HISP service that can provide the best connection options for their organization. An organization will need to either participate with a HISP, or implement one to meet Meaningful Use stage 2 requirements.

Key services that an organization should look for in a HISP include:

• Support for a secure connection that works with your EMR/EHR system if you have one, or an accessible web-based mail interface if you don't
• Support for Direct-enabled EMR/EHR systems where the content is encrypted before transmission. This provides the most secure communication.
• Certificate issuance and certificate lifecycle management using certificates from a certificate authority approved at the federal level.
• Address discovery and directory interoperability
• Certificate discovery via LDAP and DNS
• Maintenance of certification with certification and testing bodies
About Orion Health Inc.

Founded in 1993 in Auckland, New Zealand, Orion Health is the only global, independently owned eHealth technology company. With an inherent ability to interconnect a wide variety of healthcare information systems, Orion Health has become the world’s leading provider of health information exchange (HIE) and healthcare integration solutions. Orion Health has extensive experience in the design and installation of complex systems within demanding healthcare environments. Today, Orion Health products and solutions are implemented in more than 30 countries, used by hundreds of thousands of clinicians, and help facilitate care for tens of millions of patients. Clinicians, provider facilities and OEM partners rely on Orion Health to facilitate data exchange between hospitals, health systems, HIEs, and affiliated providers and medical devices, resulting in improved care coordination, increased cost savings and efficiencies, and enhanced quality of care.

In the U.S., Orion Health™ HIE provides the technology backbone for state and regional HIEs across the country. Orion Health Rhapsody® Integration Engine is used by nearly all state and local health departments for public health reporting. Customers include Catholic Health Initiatives, the Centers for Disease Control and Prevention, Beacon Community of the Inland Northwest, Geisinger Health System, Inland Empire HIE, Kaiser Permanente, Lahey Clinic, Louisiana Health Care Quality Forum, Lehigh Valley Health Network, Maine HealthInfoNet, Massachusetts Health Information Highway and St. Vincent’s HealthCare. For more information, visit www.orionhealth.com. Connect with us on Twitter, facebook and LinkedIn.