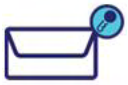
Direct Project Email with EMR Direct phiMail

Julie Maas - May, 2013

The healthcare industry is undergoing massive technological change today. Rapid, required adoption of electronic data transfer capability and associated interoperability is under way and is expected to lead to new business models and care delivery paradigms over the next few years. This paper will provide background on the technology behind Direct messaging, the status of its associated trust framework, and some unique features of EMR Direct's implementation.



Who needs to use Direct messaging?

Direct messaging is a secure email protocol designed for use in the healthcare industry, where data privacy and security are of legal importance. Direct messaging is required for use in several electronic health data communication workflows as part of Meaningful Use Stage 2 certification. This means that eligible healthcare providers seeking incentives from the Centers for Medicare & Medicaid Services (CMS) for adoption of certified Electronic Health Record (EHR) technology are required to use Direct in certain threshold volumes, for measures pertaining to specific EHR workflows.

Direct messaging must be used some percentage of the time, in the pertinent workflows, when Meaningful Use 2-compliant Consolidated CDAs (patient care summaries, also referred to as CCDAs) are transmitted[1] or received[2] by healthcare providers, and when patients initiate CCDA transmission to another Direct address of their choosing from within a Patient Portal or similar patient-accessible EHR interface.[3] Direct messaging may also be used as transport for the more generalized patient-provider Secure Messaging requirement.[4,5]

The Direct protocol is not based on new technology, but its specification is new and it is only recently becoming widely adopted. Direct leverages tried-and-true Simple Mail Transfer Protocol (SMTP), Secure Multipurpose Internet Mail Extensions (S/MIME), and Public Key Infrastructure (PKI), which have all been used widely for decades. What is new about this protocol is the way in which its underlying components are assembled to collectively form a new standard, the blessing it has received from CMS and the Office of the National Coordinator for Health Information Technology (ONC), and community efforts to establish a trust framework which will bring Direct to fruition.

---

[1] 170.314(b)(2)
[2] 170.314(b)(1)
[3] 170.314(e)(1)
[4] 170.314(e)(3)
[5] The workflows in which Direct messaging is required are listed in the ONC Final Rule document available here: http://www.healthit.gov/policy-researchers-implementers/meaningful-use-stage-2. Footnotes 1-4 identify the specific Meaningful Use Stage 2 criteria to which Direct messaging pertains.

What makes Direct messaging secure?

Direct messaging utilizes public and private key pairs in order to accomplish point-to-point secure email communication. Each sending and receiving entity possesses a public key, private key, and a Direct address.[6] The public key is made available in a public certificate, which provides both the key and identifying information about the key holder. The certificate may be self-signed, or certified by a third party Certification Authority. Identity-proofing policies for issuing Direct certificates vary, but generally involve an applicant showing at least one form of photo identification to the registrar or their agent.[7]

Direct messages are digitally signed using the sender's private key and password, encrypted utilizing a trusted recipient's public key, and then transmitted over SMTP. The recipient decrypts and verifies a message from a trusted sender utilizing the recipient's own private key and the sender's public key. Mutual trust is a pre-condition to successful exchange.[8] As long as private keys and their passwords are kept securely, no one other than the intended recipient can decrypt a message, and messages can be stored encrypted while they are not actively being viewed.

Beyond these technical stipulations, governance and accreditation policies are being established to guide the provisioning of Direct addresses and credentials, the operation of Direct services, and the maintenance and usage of these credentials over time. These policies are very similar to existing best practices for Certificate Authorities, and—where private keys are controlled by intermediaries—to other legal stipulations surrounding the handling of Protected Health Information (PHI).

How do Direct messaging users interoperate with each other?

Direct was designed for both security and interoperability. Although only an intended recipient can decrypt a message, Direct is intended to scale easily due to its common standards and widely-available specification. Developers of software that is Direct Project-compatible generally agree to follow the Applicability Statement for Secure Health Transport, commonly referred to as "the Applicability Statement". The most recent version of this document, version 1.1, was published in July, 2012. Regular connect-a-thons take place within the Direct developers' community, for the purpose of achieving and maintaining interoperability.

Direct certificates may form a chain of trust, wherein one Issuer signs the certificate of the next certificate down the chain, ending at the final certificate used by the sender or recipient. As was previously stated, at a minimum, a sender and recipient must each trust the other party's public certificate before they can exchange Direct messages. Alternatively, they may each trust a Trust Anchor, which may be any of the

[6] The private key may optionally be secured by a password or other method.
[7] This depends on the Level of Assurance of a particular credential. An exception is Level 1 identity-proofing, which requires no verification of photo identification.
[8] Specifically, the counter party's certificate or a superior Trust Anchor—a parent certificate of certificate(s) used for Direct exchange—must first be imported into a participant's STA before successful send or receive may take place with that counter party.

Issuers farther up the chain. For a self-signed certificate, the chain has only one link and the certificate itself is also the Trust Anchor. Trust Anchors may hail from different Certificate Authorities, who each generally publish information about the rules they follow when issuing credentials.[9] Trust communities who publish their own "bundles" of Trust Anchors are also beginning to emerge, and are expected to be the primary method by which Direct messaging interoperability scales.

EMR Direct was an active contributor to Direct Project's Implementation Guide for Direct Project Trust Bundle Distribution. This guide specifies how trust bundles are to be packaged and consumed, and our phiMail software already includes features which perform Trust Anchor and Trust Bundle management. These bundles of Trust Anchors are starting to be published by a few organized communities such as DirectTrust.org, the Western States Consortium, and the Automate the Blue Button Initiative (ABBI).

The existence of a particular Trust Anchor within a Trust Bundle is generally predicated either by mutually executed contracts between trust community members, self-attestation of adherence to common guidelines within a trust community, federated agreements executed by each member of a trust community, common accreditation or certification standards, or some combination thereof. These trust communities and the developing connections between them will come to form a more complete and liquid medical information network over time. A Direct address's public certificate always chains up to one or more Trust Anchors, and each Anchor may be a member of zero or more Trust Bundles. Individual senders and recipients may recognize any number of Trust Bundles at one time.

EMR Direct is a member of one such trust community, DirectTrust.org. We actively participate in the development of its agreements and policies, and are currently in the process of becoming DirectTrust accredited. As such, we expect our Trust Anchor will soon be published in the DirectTrust.org transitional trust community bundle. The accreditation program is being conducted by EHNAC and is now in its Beta stage.[10] Our Trust Anchor is currently included in the ABBI Provider bundle as well.

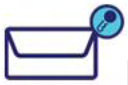
When formalized federation agreements are not in place, counter parties to Direct exchange sometimes require mutual agreement to be bound by HIPAA, HITECH, and any other state or local laws governing the treatment of PHI. They may also require other security criteria and/or minimum liability insurance coverage, or may stipulate that only HISPs who represent non-patients may be Direct exchange partners with them. The private keys associated with Direct messaging accounts need to be treated as securely as PHI itself, and when a HISP has the ability to cause a private key to be used, and as they typically process un-encrypted PHI as part of their service, they generally enter into a Business Associate Agreement (BAA) with a Covered Entity for whom they perform the STA function. It is expected that these varying and almost entirely unprecedented requirements will be harmonized over time, as adoption increases and standard setting bodies evolve.

The task of establishing a new HISP and its Trust Anchors among disparate geographic or vendor communities is very much like the early days of the Internet, in which trusted network nodes were coming online and beginning to recognize and interact with each other. EMR Direct provides boundary conditions and technical knowledge that help bring solid plans to the operations and governance workgroups in which we participate, helping to instill confidence and reliability in our national Direct messaging

[9] Referred to as a Certificate Policy, Certification Practice Statement, or a combination of the two.
[10] A good background on DirectTrust.org, the history behind interoperability, and the Direct Project can be found here: http://onhealthtech.blogspot.com/2013/04/game-of-interoperabilities.html.

infrastructure. As a developer of our own proprietary Direct messaging product, we bring substantial knowledge of PKI and message transport technologies to our industry, and actively share our technical knowledge and vision for this developing industry with our peers.

The Office of the National coordinator for Health Information Technology (ONC) also offers their input from time to time regarding implementation guidelines for Direct, and they have suggested that ultimately, providers must be the ones to decide with whom they will send and receive Direct messages.[11] Providers themselves are certainly held legally accountable for how reasonable their actions are, with respect to patient consent, and are generally advised to verify that there is a secure dial tone on the other end of a Direct connection before transmitting Protected Health Information to another entity. Fortunately, Direct messaging technology offers massive improvements in security and patient privacy over regular email, and phiMail is designed to make the most out of those opportunities for enhanced security. The harmonization of best practices into formal governance policies will help to ensure that the industry upholds the technology's promise of fostering confidence among users of Direct.



Direct Messaging Technical Details

Direct messaging gateways are referred to as Security/Trust Agents—STAs, or more commonly, and especially when an STA is operated by an intermediary for another entity, they are known as Health Information Service Providers—HISPs. The public key is certified by a Certificate Authority (CA) in an X.509 certificate issued to a credentialed user, binding it to a Direct address. Knowing only the Direct address, the corresponding public certificate is discoverable in either DNS or LDAP; STAs need to be capable of both. Private keys, and passwords when they exist, are stored securely by the user or their HISP. Some HISPs may perform, or may contract with others to perform, the role of the CA in identity-proofing and generating digital credentials for a Subscriber.[12] As part of EMR Direct's Security/Trust Agent role, the phiMail Direct gateway performs the following steps:

1) Look up a recipient's Direct address using our Provider Directory (coming soon)
2) Fetch a recipient's public digital certificate and confirm its validity
3) Verify that a recipient is trusted; enable trust, if necessary[13]
4) Form an encrypted message out of plaintext and optional attachment(s)
5) Transmit the outgoing encrypted message to an SMTP server
6) Process one or two Message Disposition Notifications (MDNs) from the recipient (these are different from read receipts), as specified by the outgoing message

For the reverse process of message receipt, analogous steps are performed that pertain to incoming rather than outgoing messages.

[11] Additional new ONC guidance may be found here: http://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/direct-implementation-guide-support-interoperability/
[12] Users of Direct, the senders and recipients, are referred to as Subscribers.
[13] phiMail customers are able to manage their own trust relationships, according to their unique business needs.

These steps take place within a customer's secure environment when phiMail is deployed locally. When phiMail is deployed in the cloud, the steps take place on a secure, cloud-based phiMail Server, and un-encrypted[14] message data is transferred to and from the secure cloud via HTTPS—or via SSL/TLS for EHR integrations or other custom applications built using the phiMail API.

phiMail is a Java® application which is operating system-agnostic and can run in any environment. Both phiMail Desktop and phiMail Server perform all required STA functions. phiMail Server has API and HL7 Bridge[15] interface options, as well as an administrator interface for multi-user support.

EMR Direct's solutions are optimized for EMR vendors or other application developers who require a robust and easily-integrated Direct messaging engine, but aren't interested in developing a business expertise in the fine details of Direct messaging. Because it is not an instantaneous service to stand up and maintain, outsourcing a Direct messaging solution means the costs of developing, testing, and managing the software, standing up and managing a Certificate Authority and the associated user credentialing, and growing the associated product management expertise, is distributed.

What's unique about EMR Direct phiMail™?

EMR Direct's software is designed for customers who want a straightforward path to add Direct messaging functionality to their applications, who intend to leverage existing email infrastructure as part of their Direct messaging solution, who prefer a higher degree of control and flexibility in their Direct messaging deployment and its underlying data stores, or any combination of the above. This patent-pending product was built from scratch to tightly adhere to the Direct standard and anticipated best practices with respect to trust framework, and does not utilize the Reference Implementation prototypes in Java® or Microsoft® .NET Framework.[16]

A phiMail Direct messaging gateway can be either an entirely local deployment, entirely cloud-based, or a custom model somewhere in-between. We also offer hosting of the entirely cloud-based deployment model, for customers who prefer it. [17]

[14] With respect to S/MIME encryption.

[15] The phiMail HL7 Bridge converts HL7 data streams encoded with a Direct address into complete Direct messages, and vice-versa. The HL7 Bridge product is currently in Beta.

[16] Trademark Notice: Java® is a registered trademark of Oracle Corporation. .NET is a Microsoft Corporation brand. phiMail is a trademark of EMR Direct.

[17] phiMail's cloud-based deployment model will soon be officially launched, and deployment characteristics may vary depending on customer requirements. Please contact us directly, for a detailed discussion of the best deployment scenario for your particular environment and available edge protocols.

Customers who choose our on-premise deployment model become their own Security/Trust Agent, since they are hosting their own phiMail Direct messaging gateway. This allows customers complete oversight of their healthcare business data and system resources, and there is no third party management of a customer's private keys or unencrypted data. This configuration may be preferable to EMR vendors who already provide hosting services, or by our customers at medical practices who also manage their own EMR software on-premise and have access to IT expertise. Healthcare IT consultants or regional organizations who wish to become their own HISP, leveraging our CA and RA services, are another customer of this deployment model.

Most commercial HISP offerings consist of a webmail interface in which customer data is first uploaded over HTTPS or other secure protocol to the HISP and is then encrypted as a Direct message and sent out to the intended recipient(s), with a mirror of this process on the receive side. While this can be easily achieved with phiMail, some implementers prefer the on-premise phiMail deployment model because the elimination of third parties (namely, the typical HISP role) reduces the number of potential points of failure between sender and recipient, and only S/MIME encrypted messages leave the customer's secure environment.

Another strategic advantage of our architecture is that the phiMail API contains only the Direct-specific logic our customers need: phiMail can work with any mail server the customer prefers, allowing for highly customizable configuration and hosting models. Access to our open source OpenEMR integration and numerous web templates and code samples make MU2 or other application integration a breeze.

On a more business-centric side of things, EMR Direct is also able to provide Direct addresses to customers at their own domains. This capability extends the brand of a private practice or EMR to their Direct messaging applications. Whether the mail server is local or in the cloud, EMR Direct alternatively offers the option of forwarding encrypted messages from our domain to a customer's, when a customer cannot support mail at their own domain, or prefers not to do so. Similarly, when customers' DNS servers do not support the hosting of public certificates in CERT records, and because customers may not have

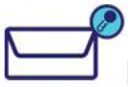
suitable LDAP technology available, EMR Direct can also host customers' public certificates a part of our service.

Each phiMail deployment model offers the opportunity for custom user interfaces, thanks to the phiMail API, phiMail Server, and private labeling of phiMail Desktop and phiMail Web and Mobile. The phiMail API is platform-independent and has been used to integrate Direct messaging into EHR and custom webmail applications. With API documentation, example templates, and sample EHR integration code that's made readily available to our customers, we're able to take new deployments live in a very short amount of time. We also offer a test server sandbox, for use by developers while evaluating our software and prior to configuring our software in their own environment.

System Requirements

The minimum system requirement to get up and running with one's own phiMail gateway is a computer with an Internet connection and Java® 7. In this case, EMR Direct hosts a customer's public certificate, NS record, and forwards encrypted Direct messages to any email address the customer controls. This "unlisted" mailbox should be dedicated to Direct messaging (no commingling of Direct with regular email messages) and will work behind the scenes as a carrier of encrypted messages.

To experience the richest feature set from one's own phiMail gateway, the system requirements are: Internet connection, server(s) running Java® 7, phiMail Server, a mail server, a web server capable of PHP, and phiMail Web.[18] In this case, the customer edits their own DNS records and hosts their public certificate in DNS or LDAP. With the fully hosted deployment model, a browser is all you'll need.



Beyond Meaningful Use – Meaningful Care

It is important to bear in mind that a nationally-acceptable form of encrypted email is a relatively new idea for the fax-driven healthcare industry to digest. However, once Direct messaging is more widely understood, user interfaces and acceptable use cases are more familiar, trust frameworks are better-established, and timelines for required adoption near, rapid uptake is expected. The rationale for Meaningful Use involves providing better care, at lower cost, and with greater patient involvement. The improved outcomes attributed to the use of Direct are expected to accelerate adoption, even for workflows in which use of Direct is not required by law or in order to receive incentives, because those who are required to adopt the technology will create demand for partners with whom to exchange. Increased efficiency and accuracy of data are also expected to motivate new applications of Direct such as telemedicine & remote consults, enhanced medical website communications, and Direct messaging-based scheduling and billing systems.

[18] phiMail Web is currently in Beta for devices, as mobile device operating policies for use of web-based Direct messaging services outside of a secure environment and EMR Direct's own mobile device certification testing are still in process.

Functionality beyond these first steps of using Direct for transport is already being written into ONC's and CMS's future health IT plans. Provider Directories, which help providers or patients to look up another provider's Direct address, are in the Meaningful Use Stage 3 draft criteria.[19] They are expected to ensure interoperability and information liquidity of Direct messaging, by making healthcare providers' Direct addresses easier to discover. Additional features for patients' management of their own data's transfer and "pull" or "query" technology will expand upon Direct's "push" capability in Meaningful Use Stage 3, as query capability is also outlined in the Stage 3 draft.

phiMail's flexible architecture lends itself well to products that go beyond basic data transport. Client-side applications of all varieties may be built, consisting of functionality beyond SMTP transfer, decryption, and validation. Smart calendar, finance, scheduling, or task management logic, that might be desired as part of a customized workflow management product, are all possible features that can be applied atop the phiMail API.

Through our software development efforts and ongoing workgroup involvement, EMR Direct continues to be the experts in Direct Messaging. We extend this expertise to our customers on a daily basis, and are continuing to innovate as the momentum of healthcare IT demands. We're almost ready to write our next white paper, where we'll delve into the ways our API is evolving to enable the next phase of Meaningful Care.

[19] Meaningful Use Stage 3 RFC:
http://www.healthit.gov/sites/default/files/draft_stage3_rfc_07_nov_12.pdf