Federal Health Architecture

Frequently Asked Questions (FAQ)

Federal Health Architecture
Directed Health Exchange
Security Sub-Work Group

May 2015

Federal Health Architecture Program Management Office | Office of the National Coordinator for Health IT | Department of Health and Human Services

Capital View Office Building
425 3rd Street SW, Washington, DC 20004

Website: healthit.gov/fha

General Email: federal.health@hhs.gov

ABSTRACT

This document is the work product of the Federal Health Architecture (FHA) Directed Exchange Working Group (FHA DEWG). It contains frequently asked questions that Working Group members determined relevant to examining federal participation in Direct. It provides interpretations and understanding of technology and policy matters pertaining exclusively to federal agencies. Every effort has been made to provide the best and most authoritative answers through consultation with knowledgeable experts; however, caution should be taken when extending use beyond its intent purely as a Working Group guideline. As such the viewpoints expressed may not be applicable to all readers.

Note: Reminder this is a FAQ document. For Guidance details, please see the FHA Directed Exchange Guidelines document located at www.healthit.gov/fha in the resource box on the right.

TABLE OF CONTENTS

1. Certificates

1.1 Must all Direct Exchange Certificates be Cross-Certified with the Federal Bridge in Order for Federal Agencies to Fully Participate in Direct?

Entities wanting to exchange direct messages with federal agencies must use federal bridge certificates until a commercial equivalent is available that provides that same level of assurance as the federal bridge certificate policy.

Please see Guideline one of the FHA Directed Exchange Guidelines PowerPoint located at www.healthit.gov/fha in the resource box on the right

1.2 Can Direct Certificates held by a HISP have the X.509 Non-Repudiation bit set?

There is no reason stated in the Direct applicability statement (see link below) or known technical reason why a HISP could not set the bit and stand by it.

How the messages are handled at the receiver would imply whether somebody can "use" that promise meaningfully for messages they've received. For more information about non repudiation please see the white paper titled: *Certificate Issuance and Assurance in Direct, page 11, A Note on Non-Repudiation located at http://Healthit.gov/fha*

http://wiki.directproject.org/Applicability+Statement+for+Secure+Health+Transport+Working+Version

1.3 Is it true that the non-repudiation (NR) bit in certificates used by HISPs must be turned off?

The source of this statement (urban myth) is not known; however, see: http://wiki.directproject.org/share/view/40943695?replyId=40961675from 2011consensus at the time was that the NR bit is fundamentally a statement that the certificate holder intends a signature from this certificate to be "binding" on them.

See Item 1.2, Specifically the *Certificate Issuance and Assurance in Direct white paper, page 11, A Note on Non-Repudiation located at http://Healthit.gov/fha*

1.4 What kind of certificates must be used to support BB+?

BB+ discussion regarding certificates can be found at: http://bluebuttonplus.org/transmit-using-direct.html#certificates

1.5 What are the Direct requirements for Certificate Verification?

Certificate Verification (Recipient)

Verify that Direct Address/Domain in Sender's certificate matches the Sender's "From" address. No assumption is made regarding who is in possession of certificates.

Certificate Verification (Sender)

Verify that Direct Address/Domain in Receiver's certificate matches the Receiver's "To" address. No assumption is made regarding who is in possession of certificates.

1.6 Is the subject of the Direct address bound certificate ever in possession (as defined by NIST) of the private key? If yes, then when?

- Option 1, STA/HISP managed service:
  Answer: This is implementation specific. In this case the HISP has physical custodianship of the private key however its use and logical access is under the control of the subject themselves. This mode of operation is most common.
- Option 2, End User operated service:
  Answer: This is also implementation specific. Typically in this case the subject will have both physical and logical access to the private key. This mode of operation is very uncommon.

1.7 What are the Pros and Cons of Address/Domain-bound Certificates?

The advantages and disadvantages of Address and Domain bound Certificates vary with the specific use case. In addition to the use case, an agency should consider the policies under which the certificates are issued and managed. For a discussion of some use cases as applied to Direct certificate usage see White Paper *Certificate Issuance and Assurance in Direct*

The following table provides comparative information for Direct Address and Domain-bound certificates for criteria that may be applicable to a specific use case:

Y=Yes, N=No, C=Conditionally Yes (with condition described in the footnote)

#	Criteria	Address bound	Domain bound
1	Direct address bound to certificate?	Y	N
2	Identity Proofing verifies individual has right to the Direct address?	Y	C[1]
3	Provides resistance to "Header Vulnerability" attack?	Y	C[2]
4	Direct mail can be sent to a recipient's Direct address?	Y	Y
5	Limits cost impact for patient use of Direct	C[3]	C[3]
6	Simple management model	C[4]	C[4]

[1]The owner of the domain is responsible for ensuring that the individual has the right to the Direct address. Degree of trust in this process is based on the policies of the specific trust framework.
[2] Requires that parties implement and follow the recommendations of the Direct Implementation Guide. Receiving parties should only use the Direct address inside the encrypted envelope for routing to the specific end-point.
[3] Where cost of certificate issuance is significant, the use of Domain bound certificates can reduce this burden. However, it should be noted that the primary cost of certificate issuance is typically the identity validation of the individual to a specific LOA. There may also be an impact on cost with large turnover or where multiple certificates may be needed for the same individual (e.g. when issuing certificates for each patient-provider relationships)
[4] Address bound certificates may require the management of a large number of certificates by the STA. Domain bound certificates reduce this STA burden, but requires the management of end-point validation by each Domain.
Identity Assurance

1.8 How can Direct Endpoint Users (Senders and Receivers) be known to each other at a prescribed Federal NIST level of assurance?

The FHA Directed Exchange Workgroup drafted a white paper to explain in more detail the nuances around Identity Assurance. For any particular transaction there is no way to know how the end user was authenticated since there is no SAML assertion submitted with Direct. You may know they have been ID proofed but at run time you may not know how they were authenticated at the moment of the transaction.

- HISP-managed Direct certificates require the primary end user, if either an organizational representative (Org Rep) or Healthcare Provider, to be identity-proofed minimally at FBCA medium or NIST LOA 3 In person prior to issuance,
- HISP-managed Direct certificates require the primary end user, if a patient or consumer, to be minimally identity-proofed at FBCA Basic or NIST LOA 2 prior to issuance,
- Legal relationship between a Covered Entity and a patient is established through appropriate rights, limitations and disclaimers established as conditions of service
- The PKI credentials at the HISP must be protected IAW NIST FIPS Pub 140-2,
- HISPs may be accredited under a trust framework e.g DirectTrust that requires a minimum level of authentication by the end user before Direct services can be accessed.

For more information please see the white paper titled: *Certificate Issuance and Assurance in Direct, located at* http://Healthit.gov/fha

1.9 Do patients entities/individuals have the same identity proofing requirements as an enterprise representative/individual?

Patients interact within Direct under different legal rules than enterprise representatives/individuals. For example, patients are in full control of the distribution of their information to others. In answering this question then, it is important to determine why patients need to be identity proofed.

For more information please see the *Patient Identity in Directed Exchange* document and the *FHA Directed Exchange Guidelines* PowerPoint located at www.healthit.gov/fha

1.10 How is the identity of representatives of organizations being issued certificates and individuals using HISP services established?

Per ONC Direct: Implementation Guidelines to Assure Security and Interoperability

May, 2013, Direct addresses are issued only to organizations and/or individuals2 that have had their identity verified according to NIST Level of Assurance 3 requirements, at a minimum, through in-person or remote options (Does not apply to patients).

ONC **recommended Registration Authority and Certificate Authority guidelines state that** representatives of organizations that are being issued certificates and individuals, who are not patients that are using HISP services are identity proofed as specified by NIST Level 3 of Assurance (as specified in NIST SP 800-63-1, dated December 2011). The identity of the applicant must be established no earlier than 30 days prior to the initial certificate issuance or use of HISP services.

For individual end-users identity is established by in-person or remote proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities (such as a notary public).

http://www.healthit.gov/sites/default/files/direct_implementation_guidelines_to_assure_security_and_interoperability.pdf

1.11 What are HIPAA's general requirements for verifying the individual's identity when the individual requests that the health care provider furnish an electronic copy of the individual's Blue Button health information?

The Privacy Rule requires covered entities (including health care providers) to verify the identity and authority of a person requesting protected health information (PHI), if the identity or authority of the person is not already known to the provider. See 45 C.F.R. 164.514(h)(1). These verification requirements apply to individuals who request access to their PHI that is maintained in a designated record set, including PHI maintained by or for a covered entity that is available through the Blue Button function (Blue Button health information). The Privacy Rule does not include specific or technical verification requirements, largely allowing a covered entity's professional judgment and industry standards to determine what is reasonable and appropriate under the circumstances. In addition to the Privacy Rule's verification requirements, where electronic access is being provided by or on behalf of a covered entity, the HIPAA Security Rule requires administrative safeguards be in place to authorize only appropriate persons to have access to the electronic protected health information (e-PHI) and technical safeguards be implemented to verify that a person seeking access to e-PHI is the one claimed. See 45 C.F.R. §§ 164.308(a)(4)(i) (information access management standard) and 164.312(d)) (person or entity authentication standard). http://bluebuttonplus.org/privacy.html

1.12 What are the Use cases for transmitting Blue Button health information?

1. While interacting in person with his HIPAA-covered health care provider's office the individual gives the provider either the individual's e-mail address or a Direct address and requests the provider to electronically transmit the individual's Blue Button health information to this e-mail or Direct address.
2. The individual has established an account with the portal of his HIPAA-covered health care provider and through that portal requests that the individual's Blue Button health information be transmitted to a trusted Direct address. http://bluebuttonplus.org/privacy.html

2. Direct Messaging, HIPAA and the Law

2.1 Are all providers who use Direct covered entities under HIPAA privacy rule?

No, the use of Direct does not determine whether a provider is a covered entity. A provider is covered by HIPAA if they electronically transmit information in connection with a HIPAA covered transaction. HIPAA transactions include filing of claims, checking eligibility, coordination of benefits--in short if a provider engages in any electronic health insurance claims related activity.

Please see the following link for reference:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html

The HIPAA regulations, including the HIPAA Security and Privacy Rules, applies to **45 CFR § 160.102 Applicability:** (a) except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities: (1) a health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter."

2.2 Is direct exchange information sent by a covered entity (CE) to a patient's HealthVault account using the patient's direct email account considered PHI once it is received and loaded into the patient's PHR under the following 2 scenarios? When HealthVault is a Business Associate of the Covered Entity?

a. When HealthVault is not a Business Associate of the Covered Entity?
b. When HealthVault is a Business Associate of an EHR vendor who has incorporated HealthVault functionality into its EHR?

Per Microsoft, HealthVault is never a Business Associate of a covered entity or vendor in the sense described. Data sent from a CE to HealthVault is done under HIPAA right to access and is just the same as if they provided a paper copy of the chart --- that copy is no longer subject to HIPAA controls in any way. Rather, it is subject to Microsoft terms of use with the end-user … which are enforced by the FTC.

*** Just to be complete, Microsoft does sign Business Associate Agreements with some clinical entities, for example if they want to integrate with HealthVault for testing purposes and they use real patient data in their test environments. Since there is no patient-directed disclosure here, we have to act as a BA, but we NEVER do this in production systems.

2.3 Does a Business Associate of a HIPAA entity need to sign an MOU or Business Associate Agreement to participate in Direct?

Yes, a Business Associate of a Covered Entity must have an MOU or Business Associate Agreement (BAA) with any third party (including a HISP) with whom they exchange PHI on behalf of the Covered Entity that includes all of the restrictions/obligations and penalties regarding use /disclosure of PHI required by the original BAA.

2.4 Does an entity that is not a HIPAA covered entity need to sign an MOU/contract with HISPs?

Yes, and make that agreement available so that HIPAA and non-HIPAA entities that request or have received PII are accountable for the manner in which they handle PII., e.g. a covered entity exchanging PHI with a non-covered entity under the HIPAA privacy rule treatment provision through the HISP.

2.5 Are patient actions in Direct with regards to their own healthcare information covered under HIPAA?

No. Patients are not HIPAA covered entities; therefore the HIPAA rules do not apply to patients. See 45 CFR 160.102. Patients have various rights under the HIPAA Privacy Rule, such as Patient Right of Access which Direct supports, but patients are not covered entities and the restrictions around use and disclosure of PHI do not apply to patients.

2.6 Is transmitting PHI on behalf of a patient using Direct a covered electronic transaction under the HIPAA regulation?

No. In general the electronic transactions specifically regulated by the HIPAA rules are addressed at 45 CFR Part 162, Subpart I. However, the transmission of PHI on behalf of a patient would be a covered function under the HIPAA Rules as a use and disclosure of PHI maintained by the covered entity. Therefore, the transmitting entity would have to comply with the HIPAA rules when performing this activity."

3. Direct

3.1 What is the architecture approach taken by the federal agencies participating in the FHA Directed Exchange activity?

The Directed Exchange Working Group has focused on the HISP to HISP communications which was identified as the most common approach. This approach is reflective of the architecture chosen by federal agencies. We concur that other approaches are possible and explicitly allowed by the Direct Applicability Statement.

3.2 What is the purpose of the FHA Directed Exchange Workgroup Risk Assessment?

The purpose of the risk assessment is to evaluate policy issues not addressed by the Direct Applicability Statement that are of particular concern to federal agencies. Specifically the risk assessment evaluates risk in the areas of:

- Life/Health/Safety
- Reputation/Customer Confidence/Public Trust
- Productivity
- Fines/Legal Penalties
- Financial Impact
- Other

The risk assessment purpose does not include evaluating the risk associated with various implementation approaches, all of which are assumed acceptable.

3.3 What is a Security and Trust Agent (STA) vs. a Health Information Service Provider (HISP) and how are they distinguished?

Security and Trust Agents (STAs) (which is software that may be operated by a healthcare entity, or—most commonly—by a 3rd party entity known as a Health Information Service Provider or HISP) facilitate Direct exchange services. See ONC, Implementation Guidelines on Direct Infrastructure & Security/Trust Measures for Interoperability, May, 2013

http://www.healthit.gov/sites/default/files/direct_implementation_guidelines_to_assure_security_and_interoperability.pdf

3.4 HealthVault and Direct Questions

The following was provided by Microsoft.

HealthVault Message Center allows HealthVault account holders with Direct email addresses to send to and receive Direct messages from providers with Direct email addresses. Is the HealthVault Message Center acting as a HISP?

Yes, HealthVault acts as a HISP in this case — in that HealthVault is the agent for the end-user's Direct certificate and interactions.

- If yes, why does each HealthVault account holder's direct email bind to an individual certificate instead of a HealthVault Domain certificate?

This is to protect against an in-transit attack between two HealthVault users. The reason an organizational certificate is "OK" in a provider/HIPAA environment is that it is bound to the legal entity that is relevant. That is, if the HIPAA Covered Entity is "MyPractice" and doctors A and B both work there … they can share a certificate because the guarantee required is that the interaction is with MyPractice. A may steal B's messages — but that is "OK" because the promise is at the MyPractice level.

This doesn't work for HealthVault because the interaction is not with "HealthVault" — it is with Patient "X" or "Y". If "X" and "Y" use the same cert, then the promise is broken … if "X" can get access to a (encrypted and signed) message intended for Y and I was using an org cert, they could decrypt it. Because SMTP is a channel where that kind of message interception is possible, we have to mitigate this.

So — the guidance for PHRs is that each end user should have their own certificate. Really at a broader level it's guidance for anywhere that the possibility of two members of the "org" seeing each other's messages is a problem.

3.5 Are there any restrictions on to whom a patient may send Direct messages?

The response is from § 170.314(e)(1) View Download Transmit Comments:

Comments. Commenters stated that the reference to the Applicability Statement for Secure Health Transport specification was the right direction to take for provider-to-provider (or clinician or organization) transmissions but that it was unclear whether this specification was also appropriate for a patient-focused certification criterion. They requested that the "transmit to third party" via this standard should be clarified to express that the intended transmission was to another provider or a personal health record (PHR). They contended

that the standard should not be required for transmission to other individuals who are not providers (e.g., friends, relatives, etc.). […]

Response: We expect that if the Applicability Statement for Secure Health Transport specification is used to complete a transmission to a 3rd party that the receiving party would be another health care-oriented entity, like a PHR company the patient is using and that it would not be a patient's friend or relative.

Editor's note: To send a Direct message, all that is needed is a Direct "To" address. There is no prohibition in the MU regulatory text to sending patient directed transmissions to whatever address the patient designates. PHR's like Microsoft HealthVault provide Direct addresses to anyone without any form of identity verification. Within HealthVault, there are no controls on who may have a Direct mail address and for what purpose.

§ 170.314(e)(1) View Download Transmit Comments

3.6 Per the Applicability Statement, Can a Direct user apply a digital signature to a document transported by Direct?

The payload for Direct is a MIME-formatted message. That payload is signed as part of the protocol for transport integrity. At what point this signature is applied to the message package is not specified by Direct and is implementation specific.

- **What about at the content level for source authentication of the document?**

Yes, Distinguish digital signatures used for message transport in Direct from content signatures applied for source authentication, or end-to-end integrity. However, document signing is out of scope of the applicability statement. In Direct, there is a distinction between a document signature (e.g. as an author, verification, consent, witness or some purpose other than transmission integrity (see ASTM E1762)) and a signature over a message payload package (which may include several documents) for transmission integrity. The protocol doesn't specific what happens at the edge — so whether a signature applied to a document within the payload and can be used "downstream" as source authentication — depends on what the receiver does with it.

For example, if the sender is in sole possession of a signing key that they alone control at all times, and they use that certificate to sign individual documents in the message payload, then the receiver may be able to assert source authentication and non-repudiation (strong binding) for the purpose intended. Regardless, transmission integrity will require a digital signature over the entire message package. Note that in this content signing case, the

signature is retained with the document, whereas after verification by the recipient transport integrity signatures are discarded.

- **At the transport level for transport integrity?**

  This is implementation specific. Note that in this case, the signature is NOT retained with the document once extracted from the message payload.

  There is no reason why the subject could not be in possession of the private key (e.g. PIV card) used to sign the transport package.

3.7 What is a Trust Framework and how does it apply to Direct Messaging?

Federal Identity Management Task Force, proposed definition.

There are two aspects to a Trust Framework, operational and legal.

The Operational Requirements consist of the technical specs, operational standards, and rules governing performance of each participant roles – i.e., the things that must be addressed so that the identity system "works" to the level of the desired performance metric. Thus, components with labels such as identity assurance framework, privacy framework, identity proofing framework, assessment framework, etc., would be component parts of the Operational Requirements section of the Trust Framework.

The Legal Rules: (1) make the Operational Requirements legally binding – i.e., it obligate each participant to actually comply with the technical specs, operational standards, and rules governing performance for that participant's roles, (2) add additional provisions to define the legal rights and responsibilities of each role – e.g., warranties, allocation of risk and liability, dispute resolution, enforcement, remedies, etc., and (3) also include existing law that might otherwise regulate the Operational Requirements (e.g., existing privacy law, crypto law, consumer law, etc.).

Examples of trust frameworks are, Federal Bridge Certification Authority, National Association for Trusted Exchange, DirectTrust, the Federal Directed Exchange Trust Framework Document and the Patient Identity in Directed Exchange document. Both documents are posted to www.healthit.gov/FHA in the resource box on the right.

3.8 What are the Consequences to a Covered Entity for Direct Messages "Sent on Behalf of" a Patient?

Under "Sent on Behalf of" the HIPAA-covered health care provider is sending PHI to a third party of behalf of and at the request of the patient. Per the HIPAA Privacy Rule, this request

must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information. See 45 CFR 164.524(c)(3)(ii).

1) If a patient has excluded a CE as part of an existing consent directive/HIPAA restriction, and subsequently requests a CE to send a message "Sent On behalf of" to the restricted CE Direct address, then that request will be denied. To send this message, the patient will need to modify their consent directive or repeal their HIPAA restriction.

2) If a patient requests a CE to send a message "Sent on behalf of" to any Direct recipient and their PHI is part of a Privacy Act system of records, the CE must have either a Routine Use Disclosure Statement promulgated in the system of records notice or an authorization for the disclosure. The sending of information "Sent on behalf of" does not relieve the CE from the requirement to maintain an accounting of disclosures when required by other law, such as the Privacy Act.

3) If patient has not authorized disclosure of their 42CFR Part 2, or 38 USC section 7332 covered information, and subsequently requests a CE to send a message "Sent On behalf of" to any Direct recipient, then that request will be denied. To send this message, the patient will need to sign an authorization for the disclosure.

4) Patient right to send or receive messages sent "Sent On behalf of" may be limited to those Direct participates supported by their provider. There should be no expectation that patients would be able to send Direct messages to Direct or receive Direct messages from entities not supported by the provider and not included in the providers Trust Bundle.

5) Under "Sent on behalf of" policies, patients would be able to send copies of their healthcare information but they would not be able to modify, delete or append information.

6) Patient use of provider Direct services under sent "On behalf of" policies will continue to conform to all policies, and technical mechanisms established by the provider as a HIPAA covered entity.

7) Patients may be required to sign a disclaimer acknowledging their understanding of these policies and the limits of responsibility of the CE in providing the services.