FHA Directed Exchange Risk Assessment Pertaining to Federal Agency Policy Concerns

Federal Health Architecture
Directed Health Exchange
Security Sub-Working Group

Version 2.0
May 2014

ATTN: Mike Davis
VHA Security Architect
CHIO Emerging Health Technologies
Department of Veterans Affairs
COMM (760) 632-0294
Mike.Davis@VA.GOV

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

Document Change Control

Version	Release Date	Summary of Changes	Addendum Number	Name
1.0	TBD	New Report	N/A	
2.0	TBD	Formatting, cosmetic changes, updated date	N/A	Zhan Caplan
2.1	TBD	508 formatting	N/A	Shannon Leigh

Table of Contents

1 Executive Summary

The objective of this Risk Assessment is to identify and prioritize risks or concerns that may inhibit full participation in Direct by federal agencies. More specifically, this assessment seeks to identify those policy concerns associated with using the Direct specification for interactions between federal partners, and those non-federal Direct participants who have not demonstrated their conformance with applicable federal policies.

The interactions in scope for this assessment involve the following uses cases:

- Federal agencies to Non-federal agencies
- Non-federal agencies to federal agencies
- Patient Directed Exchange 2 (Blue Button approach served by federal Security and Trust Agents (STAs) or Health Information Service Providers (HISPs).

Key information:

- **Environment Under Evaluation:** Federal Use of Directed Exchange

- **Reason for Risk Assessment:** To identify, prioritize and address policy concerns which may inhibit full participation in Direct by Federal Health Architecture (FHA) participants.

- **Results:** Collectively, the FHA stakeholders captured 93 candidate risks/policy concerns which were identified from Stakeholder outreach meetings, Vector Analysis documents, and Issue Papers prepared and submitted by FHA representatives.

  The risks/policy concerns were analyzed for relevance and scope; risks which were specific or unique to federal participation in Direct were considered in scope for the assessment. Those risks that were broadly applicable to all Direct participants were also captured, but not included in the detailed risk analysis.

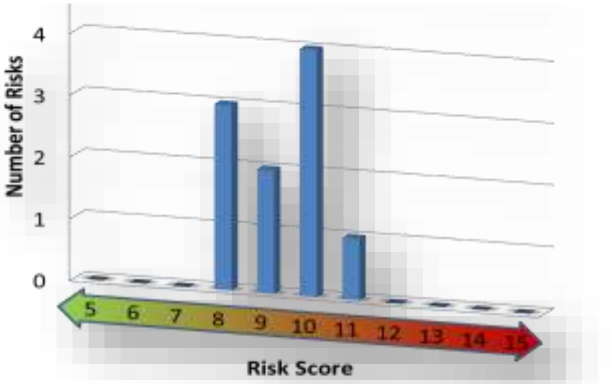
  As show in Figure 1 below, of the 93 risks identified, the analysis showed that there were ten 10 unique concerns associated with the implementation of Directed Exchange within the identified use cases. Each of these concerns was analyzed using a Risk Evaluation Criteria (REC) in order to prioritize potential impact for federal participants. Using a scoring system and the REC, one of the risks/policy concerns stood out alone as the highest impact risk (with a risk rating of 11), Two policy concerns had a risk rating of 9, and three with a risk rating of 8.

In all, 7 recommendations/mitigation strategies are proposed to help address the 10 policy concerns (some recommendations support more than one concern). Note that there is not a one-to-one relationship between the number of unique risks and the number of mitigation strategies. For example, while the source of some risks may be different, the resulting outcome (if the risks occur) may be the same. In such cases, implementation of one recommendation may address multiple risks.

Raw results detailing analysis of the 93 issues/risks identified are contained in the supporting spreadsheet at http://www.healthit.gov/sites/default/files/FHA-Directed-Exchange-Risk-Assessment-Pertaining-to-Federal-Agency-Policy-Concerns-final-06-09-2014.xls

The top ranking risk (in terms of impact) was in the category of Certificate Authorities, and captured the concern that currently, federal participants can only accept credentials that are approved by the Federal Bridge Certification Authority (FBCA). Because it is not known whether all external agencies participating in Direct (e.g. DirectTrust.org) meet the FBCA requirements, federal agencies may not be able to fully participate in Direct.

Figure 1: Number of Risks by Risk Score (Prioritized Risk Ranking)



This policy risk and other high priority concerns are further discussed in the Frequently Asked Questions (FAQ) and Issue Papers under development by the Security Sub-Working Group.

- **Conclusion:** Implementation of several proposed policy and guidance efforts will provide additional clarity for FHA participants and effectively address concerns inhibiting progress towards full and ubiquitous federal agency participation in Direct.

During the analysis, it was noted and understood that use of the Federal Bridge is not required for participation in Direct, and that normal FISMA mitigations for authorization of the communication path should be sufficient for federal agency participation.

The issue paper “FHA Directed Exchange Issue Paper: Cross-Certification with Federal Bridge” contains a more thorough discussion regarding the use of DirectTrust.org and how federal agencies may trust certificates at the appropriate level. It was also noted that the use of manual workflows (e.g. fax, out of band communications) are available as a workaround.

Additionally, risks and policy concerns were identified surrounding the differing Levels of Assurance between patients, federal participants, and potentially non-federal providers. The paper “FHA Patient Identity in Directed Exchange” discusses in more detail the concerns associated with what LOA may be appropriate for patients to use. The paper focuses on the risks associated with the act of sending health information using Direct, regardless of the number of records being sent in any particular transaction. It also points out that the documents to be submitted for identity proofing at LOA 2 are the same as for LOA 3, however the level of rigor required for verification of those same documents is what differs. Note also that in the use case where a patient directs the exchange of healthcare information to an endpoint, it is the EHR system that signs the health information payload used in the communication, not the patient. Therefore, the level of assurance of the patient’s certificate is less important. It is for these reasons that there is little impact on patients between whether or not the LOA 2 proofing or LOA 3 proofing is conducted. Recognizing that there are differences between LOA 2 and LOA 3 in terms of how the credentials are subsequently managed is also important, however it is expected that CA capabilities exist to perform the necessary functions at LOA 2 and LOA 3.

Finally, the FAQ paper was written to provide additional clarity on key topics in order to help separate opinion from fact and to provide a common baseline for readers. The document may need to be updated again in the future, as additional information and guidance is promulgated from authoritative sources such as ONC.

The fundamental issues FHA participants face in their implementations of Direct are policy concerns that are not fully addressed by Direct. Federal partners are implementing federal and agency policy, which are sometimes more stringent than what has been described in the Direct applicability statements and implementation guidance. The recommendations contained in this risk assessment are to help provide a common denominator for federal partners to consider when they make their own determinations on how to more fully participate in Direct. In addition, it is hoped that this paper may be informative to policy makers – at least in articulating the challenges that federal partners are experiencing.

In all, 7 recommendations have been provided for consideration. The recommendations are recommendations are intended to help address 10 unique policy concerns, and are listed in listed in Table 3 outlines the eight mitigation strategies/recommendations proposed as a starting point to addressing the 10 unique policy concerns, which in turn were derived from 93 issues offered by FHA stakeholder participants.

Table 3: Summary of Recommendations

.

2 Introduction

2.1 PURPOSE AND OBJECTIVES

This document contains the results of a focused FHA risk assessment for Directed Exchange use cases, pertinent to federal agencies. This risk assessment report is the agreed upon deliverable of the Security Sub-Working Group and contains the risks, concerns, and recommended mitigation strategies to address the policy concerns surrounding use of Directed Exchange.

Key objectives of the risk assessment include the identification and analysis of risks that federal participants may assume in the case of Directed exchange with non-federal participants of direct (e.g. participants operating at Level of Assurance 2 or lower).

2.2 SCOPE AND ASSUMPTIONS

This document will address any risks associated with using the Direct specification for interactions between federal and non-federal partners against three use cases including:

- Federal agencies to Non-federal agencies
- Non-federal agencies to federal agencies
- Patient Directed Exchange 2 (Blue Button approach served by federal STA/HISP)

The following three use cases were considered and subsequently deemed out of scope on the basis of having no net impact to federal agencies:

- Patient Directed Exchange 1 (Blue Button served by Non federal HISP)
- Non-federal agencies to Non-federal agencies

- Federal agency to federal agency (assumes agencies are adhering to a common baseline of policies and security requirements)

Finally, this scope is based on the following assumptions:

- The risk assessment will address policy considerations; the goal is not to identify or recommend technical changes to the Directed Exchange specification.
- The term "Non-federal Partners" are considered organizations which are participating in Direct, but that do not utilize Federal Bridge Certification Authority (FBCA) cross-certified certificates or that otherwise would not meet criteria that would satisfy federal agency Requirements.

Those risks that are considered impediments to federal agencies more fully participating in Direct are in-scope. Those risks that are impediments to full participation beyond federal participation (e.g. broader issues that affect all participants) are noted and captured where identified, and flagged as outside the scope of this assessment. The WG may later wish to revisit the out-of-scope risks with the broader Direct community.

2.3 BACKGROUND

The following organizations are FHA stakeholders that provided participation in the FHA Security SWG and associated risk assessment:

- CMS
- DOD / DOD MHS
- HHS ONC
- IHS
- IPO VLER Health
- SSA
- VA
- VHA

Other stakeholders/bodies who provided input and SME support to this activity include:

- DirectTrust.Org
- NIST
- FBCA
- FISMA
- FICAM
- HITSC and Privacy and Security WG

2.4 ORGANIZATION

This document is organized as follows:

- Section 2 discusses the overall purpose and objectives, including scope and assumptions.
- Section 3 is a technical discussion to more fully introduce the key issues

- Section 4 describes the tailored Risk Assessment methodology.
- Section 5 documents threat identification.
- Section 6 documents the risk analysis, including the risk evaluation criteria.
- Section 7 discusses in more detail each of the key steps.
- Section 8 provides a summary of the recommended mitigation strategies.

2.5 REFERENCES

1. Federal Bridge Requirements
2. SHA-1 replacement
3. NIST SP 800-63 -1 Dec. 2011 - Electronic Authentication Guideline
4. NIST Special Publication (SP) 800-30r1: Guide for Conducting Risk Assessments
5. Federal Information Security Management Act (FISMA)
6. Health Insurance Portability and Accountability Act

3 Technical Discussion

The objective of this Risk Assessment is to identify risks that federal agencies may assume when using DIRECT with non-federal partners. It should be noted that the results of this report are based on a snapshot in time and should be revisited periodically. The methodology utilized for the Risk Assessment is consistent with NIST-SP 800-30 and has been tailored to suit the needs of this particular assessment.

Participants of Direct considered stakeholders in the risk analysis include:

- Individual consumers/patients
- Non-federal/Private sector clinicians and their provider organizations
- Federal providers and federal provider organizations
- federal Health Information Service Providers (HISPs)
- Security and Trusted Agents (STAs)

Among the key issues and concerns identified by FHA stakeholders are those concerning difficulty reconciling seemingly conflicting policies. For example, federal agencies are required under the Federal Information Security Management Act of 2002 (FISMA) to adhere to certain requirements for Certification and Accreditation of information systems. Among those requirements is the use of federal PKI class 3 digital certificates for authentication. In apparent contrast to this requirement, the use of Direct allows for non-federal organizations, to employ self-signed certificates or certificates that may not meet the requirements described in NIST SP 800-63 for Level of Assurance (LOA) 3.

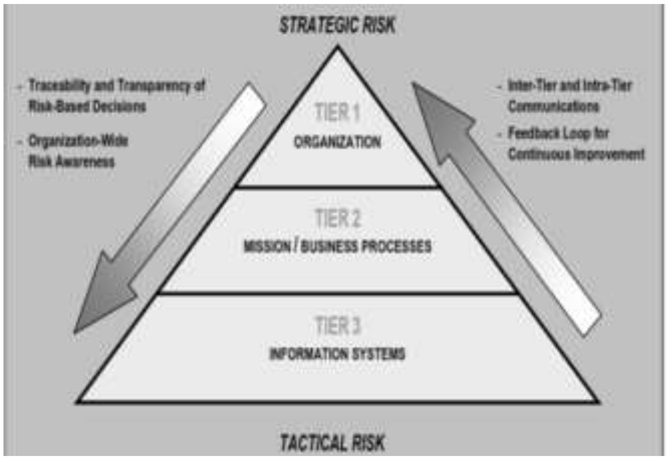
Other concerns include the potential harm that could result from patients using Direct in an environment where the infrastructure and capability is served by federal partners. For example, patients may wish to communicate with non-federal endpoints, and may do so under the false assumption that the communications will be fully protected under HIPAA, the Privacy Act, and will be managed in a way that is fully consistent with federal policies and procedures for ensuring appropriate information security and privacy.

4 Risk Assessment Methodology

The Risk Management methodology described in NIST SP 800-30 accommodates a tailored approach to threat, vulnerability, impact, probability, and mitigation analysis. It should be noted that:

- Each organization or community may define a risk model appropriate to its view of risk (i.e., formulas that reflect organizational or community views of which risk factors must be considered, which factors can be combined, which factors must be further decomposed, and how assessed values should be combined algorithmically).
- Organizations have maximum flexibility on how risk assessments are conducted, where such assessments are applied, and how the results will be used.
- Organizations are encouraged to use the guidance in a manner that most effectively and cost-effectively provides the information necessary to senior leaders/executives to facilitate informed risk management decisions.

Figure 2: NIST SP 800-30: Risk Management Hierarchy


STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
- Inter-Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
TACTICAL RISK

As noted within Figure 1 below, this targeted assessment approach aligns directly with the Risk Management hierarchy, Tiers 1 and 2 as follows:

1. Scope is narrowly defined to produce answers to specific questions (e.g., what is the risk associated with relying on a given technology?)
2. Organizations may consider assessing risk at Tier 1 and Tier 2 arising from a set of common threats and vulnerabilities applicable to a wide range of organizational information systems.

3. Assessing risk at Tiers 1 and 2 allows organizations to reduce the number of threats and vulnerabilities considered at the individual information system level and develop common risk responses for such organization-wide risks.

Risk management is understood here as a broader concept than risk assessment, where the latter is usually part of the risk management process and addresses risk identification and quantification or qualification. Risk assessment is also referred to as risk analysis. Risk is fundamentally composed of three elements: the risk event or threat, the probability of occurrence, and the impact or severity of the consequence. The risk exposure of an organization arising from a risk event (materializing of a threat) will be defined by the combination of the last two variables: probability and impact. To the degree that the probability and the impact can be assessed and influenced, risk is manageable.

5 Threat Identification

Various threats to the key components may help identify the possible outcomes of different types of threats. In this context, the threat vector is specifically tailored to existing and potential policy within the federal and private communities that may serve as an indication of a potential undesirable event.

Additional threat vectors may be evaluated within subsequent risk analysis that could focus upon situations where persons could do something undesirable or where a natural occurrence could cause an undesirable outcome.

The resulting effects or outcomes of scenarios typically fall into the following categories:

- Disclosure or viewing of sensitive information
- Modification of important or sensitive information
- Destruction or loss of important information, hardware, or software
- Interruption of access to important information, software, applications, or services

6 Evaluation of Risks

The organizational Risk/Impact Evaluation Criteria (Table 1) was agreed to by consensus of the FHA Security SWG participants and contains thresholds for specifically defining what was to be considered “high”, “medium”, or “low” organizational impact in the following categories:

- Life/Health/Safety
- Reputation/Customer Confidence

- Productivity
- Fines/Legal Penalties
- Financial Impact
- Other

Table 1: Risk Evaluation Criteria

CATEGORY	IMPACT VALUE: HIGH (Risk Rating = 3)	IMPACT VALUE: MEDIUM (Risk Rating = 2)	IMPACT VALUE: LOW (Risk Rating = 1)
Life / Health/Safety	Safety/Health occurrence or safety event likely	Safety/Health exposure increased	Health/Safety not affected
Reputation / Customer Confidence	Reputation of federal agency irrevocably or substantially destroyed or damaged	Reputation of federal agency damaged; some effort and expense required to recover	Reputation of federal agency minimally affected; little or no effort or expense required to recover
Productivity	Federal agency cannot connect to any DIRECT endpoint; therefore the quality of the health information service may be substantially affected.	Federal agency can connect to some DIRECT endpoints but not all and therefore the quality of the health information service may be moderately affected.	Federal agency ability to connect to DIRECT endpoints is not affected and therefore the quality of the health information service is not affected.
Fines/Legal Considerations	Intentional public violation of HIPAA rule(s) or other regulatory requirement resulting in exposure to maximum penalties *(e.g. $50,000 per violation, with an annual maximum of $1.5 million+ up to 10 imprisonment)*	Unintentional public violation of HIPAA rule(s) or other regulatory requirement *(e.g. HIPAA violation due to reasonable cause and not due to willful neglect = $1,000 per violation, with an annual maximum of $100,000 for repeat violations)*	Non-public violation of HIPAA rule(s) rule or other regulatory requirement *(e.g. $100 per violation, with an annual maximum of $25,000 for repeat violations)*
Other Financial Considerations	Equipment Purchase or unplanned capital expense of more than $5M per agency *(e.g. cost of applying encryption to all laptops, credit monitoring, PR notices and letters)*	Equipment Purchase or unplanned capital expense of $1M to $5M	Equipment Purchase or unplanned capital expense of under $1M

Each of the threats listed below were identified as risks to use of the Directed Exchange framework. They were evaluated against the risk evaluation criteria to identify the most severe (high) organizational impacts should any of those threats and associated outcomes be realized. Table 2 illustrates the assessment of “High”, “Medium” and “Low” impact, by category, for each of the threats. The threats were prioritized according to the number of “High”, “Medium” and “Low” impact items each threat was assigned. A simple scoring scheme was used to help prioritize the threats, where a “High” impact was assigned a value of 3, “Medium” impact assigned a value of 2, and “Low” impact assigned a value of 1.   Threats with high total values are therefore deemed higher priority for mitigation.

Under this schema, a risk value of 15 denotes the highest possible risk score (H,H,H,H,H = 3 x 5) and a risk value of 5 denotes the lowest possible risk score (L,L,L,L,L = 1 x 5).

Table 2: Prioritized Risks/Policy Concerns

RISK / POLICY CONCERN DESCRIPTION	Potential Outcome (Disclosure / Modification/ Loss/ Interruption)	Potential Impact: Life / Health	Potential Impact: Reputation	Potential Impact: Productivity	Potential Impact: Fines/Legal	Potential Impact: Financial	Risk Value
RISK #21a: Restricted to use Certificates issued by Cross-Certified CAs using FBCA certificate policy. If federal participants can only accept credentials that are approved by the FBCA, the ability of federal agencies to more fully participate in Direct will be limited. Note: It is not known if all external participants (E.g. DirectTrust.org) meet these requirements. Conforming to policies with FBCA is not the same as being cross-certified with the FBCA. Note that although some of the certificates issued by DirectTrust are cross certified with FBCA (e.g. Digicert), they may not be asserting the FBCA CP while operating in a Direct environment. See issue paper "Issues impeding Full Federal Healthcare Agency Participation in Direct" and FAQ.	Interruption (inability to communicate with all Direct participants)	H	H	M	L	M	11
RISK #28c: Use of Non-Federal CAs. If federal agencies become allowed to rely on non-federal certificate authorities that are not as trustworthy as those of the federal government then trust cannot be assured. Without assured trust, the information cannot be relied upon and provides no healthcare benefit and provides health/safety issues for patients. This would in effect be relaxing an existing federal control.	Disclosure, Modification, Interruption	M	M	L	H	M	10

RISK / POLICY CONCERN DESCRIPTION	Potential Outcome (Disclosure / Modification/ Loss/ Interruption)	Potential Impact: Life / Health	Potential Impact: Reputation	Potential Impact: Productivity	Potential Impact: Fines/Legal	Potential Impact: Financial	Risk Value
RISK #23a: Business Associate Agreements and MOU. If an acceptable use policy (e.g. for Title 38 Section 7332 or 42 CFR Part 2) is not available then information may be used for purposes other than intended, and handling instructions of the sender may not be enforced. Specific user disclosure requirements such as "do not redisclose" may not be honored by the receiving party.	Disclosure	L	M	M	M	H	10
RISK #9b: HISP Operating Policies and Trust - Access to Encryption Keys. If the HISP has access to the encryption keys and to all protected information belonging to multiple patients, then without proper controls, improper exposure, and breach of protected health information could occur.	Disclosure, Interruption	M	M	M	M	M	10
RISK #2a: STA/HISP Operating Policies and Trust. If federal Agency acts as STA/HISP on behalf of patients, then they may be at risk in event of data breach.	Disclosure	L	M	M	H	M	10
RISK #25a: Use of Certificates as Declaration of Conformance with Virtually any Policy If the Direct model is one in which the requirements for certificate issuance can be “virtually anything” then it will be unlikely to meet the specifics required by federal agencies, thus limiting the operational applicability of Direct.	Disclosure	H	M	L	M	L	9

RISK / POLICY CONCERN DESCRIPTION	Potential Outcome (Disclosure / Modification/ Loss/ Interruption)	Potential Impact: Life / Health	Potential Impact: Reputation	Potential Impact: Productivity	Potential Impact: Fines/Legal	Potential Impact: Financial	Risk Value
RISK #10a: Legal Safeguards. If Direct participants are not HIPAA Covered Entities, then HIPAA privacy protections and safeguards may not apply, exposing protected health information to misuse without adequate recourse.	Disclosure	H	M	L	M	L	9
Risk #23b: Patients Assume Transactions are Protected. If patients are not provided a simple way of determining the safety and assurance of a receiver, then they may unknowingly be placing their sensitive information at risk and could hold the agency culpable. e.g. if a patient uses BB+ federal to send data to a non-federal direct endpoint, the patient may assume that the entire transaction is protected by policy and regulation. The patient may therefore hold the agency culpable for any subsequent misuse of the information.	Disclosure	L	M	L	M	M	8
Risk #12a: Certification of HISP Operating Policies and Trust Risk: If the Direct HISPs do not have open and transparent CPs, perform risk assessment and mitigation according to an established certification process, then federal agencies can have no assurance that sensitive information is being handled responsibly.	Disclosure	M	M	M	L	L	8
Risk #28a: Business Associate Agreements and MOU for Trust Relationships If trust relationships do not meet federal standards, then federal agencies may be precluded from participating in Direct exchanges with non-federal recipients.	Interruption	M	M	M	L	L	8

7 Risk Discussion

The risks, in terms of potential organizational impact, are discussed below:

7.1 RISK #21A: RESTRICTED TO USE CERTIFICATES ISSUED BY CROSS-CERTIFIED CAS USING FBCA CERTIFICATE POLICY:

If federal participants can only accept credentials that are approved by the FBCA, the ability of federal agencies to more fully participate in Direct will be limited. Note: It is not known if all external participants (E.g. DirectTrust.org) meet these requirements. Conforming to policies with FBCA is not the same as being cross-certified with the FBCA. Note that although some of the certificates issued by DirectTrust are cross certified with FBCA (e.g. Digicert), they may not be asserting the FBCA CP while operating in a Direct environment. (See issue paper "Issues impeding Full Federal Healthcare Agency Participation in Direct" and FAQ.)

Source/Applicability Statement:
Some organizations may have constraints on which Certificate Authorities they may use. For example, federal providers and agencies must conform to federal Government policies regarding certificate authorities and certificate issuance. Nothing in this document [applicability statement] or the Direct Project specifications require any organization to adopt a wider set of Circles of Trust than they are able to by policy.

Communities that wish to exchange data with federal providers and agencies must have certificates that chain to the Federal Bridge Certification Authority. See the IDManagement.gov website for more details.

Risk Score: (15 = highest Possible risk, 5 = lowest possible risk).

Analysis of this risk resulted in an overall risk score of 11.

Impact (Per Risk Evaluation Criteria)
Scoring: Low = 1, Medium = 2, High = 3

Life/ Health	Reputation	Productivity	Fines/ Legal	Other Financial	Overall Impact Score
H	H	M	L	M	**11**

Recommendation:

- To mitigate this risk, federal agencies participating in Directed Exchange could determine that the use of Federal Bridge is not required. Normal FISMA mitigations for certification of the communication path are all that is needed. For example, if a trusted Framework such as DirectTrust.org is deemed to be consistent with the policies of the federal agencies, then agencies may choose to leverage this as part of their FISMA mitigation. Refer to FAQ 1 for use of DirectTrust and whether it can be trusted by federal agencies to the appropriate level. Use of manual workflows (e.g. fax, out of band communications) are available as workarounds.
  Note: DirectTrust is able to positively identify those entities which are cross certified with the FBCA and can assert that position using certificate policy OIDs.
- As an alternative, if federal agencies determine that the use of Federal Bridge cross certified CAs is required, then Federal agencies may require all Directed Exchange trading partners to obtain FBCA credentials.

7.2 RISK #23A: BUSINESS ASSOCIATE AGREEMENTS AND MOU:

If an acceptable use policy (e.g. for Title 38 Section 7332 or 42 CFR Part 2) is not available then information may be used for purposes other than intended, and handling instructions of the sender may not be enforced. Specific user disclosure requirements such as "do not redisclose" may not be honored by the receiving party.

Source/Applicability Statement:
The receiver of the information agrees to use the information for the purpose it was sent, not for other purposes. In addition, the receiver agrees to abide by any obligations and prohibitions bound in a security label to the information received such as requirements to not redisclose the information without the patient’s consent.

Risk Score: (15 = highest Possible risk, 5 = lowest possible risk).

Impact (Per Risk Evaluation Criteria)
Scoring: Low = 1, Medium = 2, High = 3

Life/ Health	Reputation	Productivity	Fines/ Legal	Other Financial	Overall Impact Score
L	M	M	M	H	**10**

Recommendation: To mitigate this risk, federal agencies participating in Directed Exchange should consider requesting an update to the guidelines from ONC to include "receivers of information should abide by special handling instructions such as do not redisclose, where required by law".

Other possibilities include recommendations for use of Data Segmentation to help ensure only authorized individuals, such as providers or individuals acting in an emergency situation can access the information when needed.

7.3 RISK #28C: USE OF NON-FEDERAL CAS

If federal agencies become allowed to rely on non-federal certificate authorities that are not as trustworthy as those of the federal government then trust cannot be assured. Without assured trust, the information cannot be relied upon and provides no healthcare benefit and provides health/safety issues for patients. This would in effect be relaxing an existing federal control.

Source/Applicability Statement:
Note that by "Certificate Authority" we do not mean the usual Certificate Authorities that issue TLS certificates used in ordinary browsers. The Certificate Authorities used for the purposes in this document are likely to either be special purpose for healthcare, or be highly trusted Certificate Authorities that are used for other similar purposes, such as issuing certificates for interoperability with the federal Government. Note that the same organizations that maintain Certificate Authorities for electronic commerce may also maintain Certificate Authorities for these purposes, but the root Trust Anchors will almost certainly be different.

Risk Score: (15 = highest Possible risk, 5 = lowest possible risk).

Impact (Per Risk Evaluation Criteria)
Scoring: Low = 1, Medium = 2, High = 3

Life/ Health	Reputation	Productivity	Fines/ Legal	Other Financial	Overall Impact Score
M	M	L	H	M	**10**

Recommendation:
To mitigate this risk, federal agencies participating in Directed Exchange should acknowledge that the premise that agencies only accept FBCA credentials should be re-evaluated with respect to Directed Exchange. Federal agencies should consider establishing a policy that provides for acceptance of other trust frameworks that

meet federal requirements. The trust frameworks should have been assessed for adherence to federal requirements (including Governance, FISMA, HIPAA etc.) so that agencies can make informed decisions. This would allow agencies to evaluate their participation in order to communicate via DIRECT beyond the limits of the Federal Bridge.

To implement Directed Exchange outside of the Federal Bridge trust framework, federal agencies would need to extend trusted credentials to include credentials from entities accredited by approved trust frameworks such as DirectTrust.org (which is the exemplar that HHS brought forward) or similar organizations.

If so, the risk becomes normal risk for communication security and compliance with X.509 certificate specifications.

Guidelines would then need to be updated accordingly.

7.4 RISK #9B: HISP OPERATING POLICIES AND TRUST - ACCESS TO ENCRYPTION KEYS.

If the HISP has access to the encryption keys and to all protected information belonging to multiple patients, then without proper controls, improper exposure, and breach of protected health information could occur.

Source/Applicability Statement:
Exchange of data protected by strong encryption over the open Internet using pure routing functions (e.g., TCP/IP switching, SMTP servers handing encrypted data) generally does not need these levels of protection so long as the routing organizations do not have access to the decryption keys. Commercial HISPs have access to the encryption keys and to all protected information belonging to multiple patients.

Risk Score: (15 = highest Possible risk, 5 = lowest possible risk).

Impact (Per Risk Evaluation Criteria)
Scoring: Low = 1, Medium = 2, High = 3

Life/ Health	Reputation	Productivity	Fines/ Legal	Other Financial	Overall Impact Score
M	M	M	M	M	**10**

Recommendation:
To mitigate this risk, federal agencies participating in Directed Exchange should

implement recommendations already provided by Direct covering the case where HISP have access to unencrypted data or could have access to unencrypted data because they hold decryption keys for encrypted data.

As mitigation for this risk, Covered Entities (CE), (this includes federal agencies such as the DoD, VA, CMS, IHS), should establish Business Associate Agreement (BAA) with any HISP providing Directed Exchange services on the CE's behalf that explicitly constrain access, use, and retention of unencrypted or encrypted PHI for which the HISP holds keys.

There may be instances where Business Associates wish to sign legal agreements with HISPs. The Business Associates should require the HISP to establish legally enforceable contracts binding any intermediary participating in Directed Exchange services on the CE federal agency's behalf to stipulations at least as stringent and comprehensive as their CE BAA.

As mitigation for this risk, federal agencies, which are not CEs, should establish legally enforceable contracts binding HISPs to stipulations at least as stringent and comprehensive as a BAA with a federal Agency that is a CE.

Non-CE federal agencies should require their HISPs to establish legally enforceable contracts binding Directed Exchange services provided on the agency behalf to stipulations at least as stringent and comprehensive as the HISP's contract with the federal Agency customer.

7.5 RISK #2A: STA/HISP OPERATING POLICIES AND TRUST.

If federal Agency acts as STA/HISP on behalf of patients, then they may be at risk in event of data breach.

Source/Applicability Statement:
Each STA MUST, for each address or organization, be able to discover a set of trusted anchor certificates (trust anchors, as defined in RFC 5280, section 6). The mechanism by which that association is performed and by which trust anchors are selected and maintained is a critical matter of policy that is not defined in this document.

In other words, a patient may choose to send their information to an endpoint not trusted by the federal Agency.

Risk Score: (15 = highest Possible risk, 5 = lowest possible risk).

Impact (Per Risk Evaluation Criteria)
Scoring: Low = 1, Medium = 2, High = 3

Life/ Health	Reputation	Productivity	Fines/ Legal	Other Financial	Overall Impact Score
L	M	M	H	M	**10**

Recommendation:
To mitigate this risk, federal Agency STA/HISP should consider presenting Terms and Conditions and a warning to the patient upon the patient's initiation of Directed Exchange, regardless of whether the endpoint is trusted or not, to inform them that the patient is responsible for the transaction.

If the federal STA/HISP has not established a trust relationship with the endpoint chosen by the patient, then additional warnings may need to be displayed to the patient indicating the level of potential risk for proceeding with the Directed Exchange.

Alternatively, the federal HISP may suggest the patient use a non-federal HISP for transactions to untrusted endpoints. This may relieve the Agency of the risk, technically, however this approach may not meet the Meaningful Use certification *criteria § 170.314(e)(1) View Download Transmit*, which requires the EHR technology to support patient Directed Exchange transmission, despite the CMS requirement for calculating Meaningful Use measure for criteria allowing any type of transport to be used by the provider's certified EHR because federal Providers are not regulated by CMS [Note i].

Federal agencies should consider whether there is an ethical responsibility to send the information anyway, per the wishes of the patient, in addition to potential for public relationship outfall for declining to facilitate patient Directed Exchange.

For any of these recommended mitigation strategies, federal agencies should seek proper legal counsel on requirements for compliance to Meaningful Use certification criteria § 170.314(e)(1) View Download Transmit and means by which to indemnify the organization from any legal liability that may accrue.

This recommendation may be helpful and applicable to all Direct users, not just federal agencies.

[Note i]: § 170.314(e)(1) View Download Transmit - HHS Response to Comments

Transmit Comments. Many commenters asked that we clarify why a SOAP-based transport standard was not proposed as part of this certification criterion when it was for the transitions of care certification criterion. Commenters contended that this was an inconsistency and asked that ONC and CMS reconcile the two. They also referenced CMS's proposed rule and preamble that stated that transmission could occur via any means of electronic transmission according to any transport standards for the view, download, and transmit to a third party objective. Other commenters stated that other transport standards should be permitted for use, such as those for query and response. Last, commenters asked questions about workflow and how transmission should be implemented so that a patient's information can be transmitted to a 3rd party.

Response: There was no inconsistency between the ONC and CMS proposed rules. The proposed transport standard(s) for each certification criterion were purposefully chosen and proposed to specify the capabilities EHR technology would need to include in order to demonstrate compliance with each certification criterion. Commenters have confused two very distinct concepts: (1) What is required for EHR technology to demonstrate compliance with a certification criterion; and (2) how EHR technology, once certified, must be used to demonstrate meaningful use. We seek to make this distinction clear to prevent any further confusion.

The certification criteria adopted in this final rule apply to EHR technology and only EHR technology. The final rule specifies the technical capabilities that EHR technology must include and other requirements that must be met in order for EHR technology to be certified. This rule does not specify in any way how EHR technology, once certified, must be used in order to achieve meaningful use. That policy is expressed in CMS's rules and is identified for each MU objective and associated measure. In this scenario with the view, download, and transmit to a 3rd party and transitions of care objectives and measures, CMS purposefully proposed two different policies.

For view, download, and transmit to a 3rd party CMS expressly indicated that other transport standards beyond those required for certification could be used by EPs, EHs, and CAHs

7.6 RISK #25A: USE OF CERTIFICATES AS DECLARATION OF CONFORMANCE WITH VIRTUALLY ANY POLICY

Risk:

If the Direct model is one in which the requirements for certificate issuance can be "virtually anything" then it will be unlikely to meet the specifics required by federal agencies, thus limiting the operational applicability of Direct.

Source/Applicability Statement:

This goal is facilitated by using possession of x.509 certificate artifacts to "proxy" for policy adherence. In this model, a policy-enforcing body is responsible for issuing certificates only to those they have confirmed can and will adhere to their requirements. These requirements may be virtually anything. A few examples: undergo an annual HIPAA compliance audit, use biometric authentication for system login, have a valid license to practice medicine in one of the 50 states, adhere to the access control and handling caveats specified in security labels bound to the health information, and so on.

Risk Score: (15 = highest Possible risk, 5 = lowest possible risk).

Impact (Per Risk Evaluation Criteria)
Scoring: Low = 1, Medium = 2, High = 3

Life/ Health	Reputation	Productivity	Fines/ Legal	Other Financial	Overall Impact Score
H	M	L	M	L	**9**

Recommendation:

CAs currently publishes the Certificate Policy (CP) and the Certificate Practice Statements (CPS). The CA also operates as a certificate service provider, under a trust framework (such as DirectTrust), which ensures the CAs operate in accordance with the trust framework.

To mitigate this risk, federal agencies should consider only engaging with trust frameworks and CAs which have been reviewed and approved as meeting the base set of federal requirements should be trusted.

ONC and federal agencies should monitor these trust frameworks, and participate (as appropriate) to provide continued input and guidance to ensure the frameworks continue to meet federal Requirements.

Policy OIDs in a certificate may be helpful for federal agencies to determine which policies the certificate holder is asserting. Examples include the use of OIDs to represent different LOAs, conformance with federal HIPAA requirements, etc.

7.7 RISK #10A: LEGAL SAFEGUARDS.

If Direct participants are not HIPAA Covered Entities, then HIPAA privacy protections and safeguards may not apply, exposing protected health information to misuse without adequate recourse.

Source/Applicability Statement:
HIPAA provides legal safeguards and clear requirements for Individuals (patients/consumers) and Covered Entities. There are some participants that will desire to participate in directed exchange, but will not meet the legal triggers for Covered Entity status. Including such participants in directed exchange without ensuring the same legal safeguards provided under HIPAA is problematic. HIPAA extends the application of privacy safeguards and protections to Business Associates (and certain subcontractors) of Covered Entities. Directed exchange of PII that involves intermediaries or third parties that are not Business Associates or covered by equivalent protections is likewise problematic, unless separate mutual contracts are in place to protect the privacy, security, and transparency asserted under the Fair Information Practices Principles Because a model that requires mutual contracting is not operationally scalable, it is desirable to limit exchange to entities that have clear recognized responsibilities under HIPAA or more stringent privacy laws.

Risk Score: (15 = highest Possible risk, 5 = lowest possible risk).

Impact (Per Risk Evaluation Criteria)
Scoring: Low = 1, Medium = 2, High = 3

Life/ Health	Reputation	Productivity	Fines/ Legal	Other Financial	Overall Impact Score
H	M	L	M	L	**9**

Recommendation:
Implementation of the recommended mitigation for Risk #25a will also effectively mitigate this risk.

7.8 RISK #23B: PATIENTS ASSUME TRANSACTIONS ARE PROTECTED.

If patients are not provided a simple way of determining the safety and assurance of a receiver, then they may unknowingly be placing their sensitive information at risk and could hold the agency culpable.

e.g. if a patient uses BB+ federal to send data to a non-federal direct endpoint, the patient may assume that the entire transaction is protected by policy and regulation. The patient may therefore hold the agency culpable for any subsequent misuse of the information.

Source/Applicability Statement:
The receiver of the information agrees to use the information for the purpose it was sent, not for other purposes. In addition, the receiver agrees to abide by any obligations and prohibitions bound in a security label to the information received such as requirements to not redisclose the information without the patient's consent.

Risk Score: (15 = highest Possible risk, 5 = lowest possible risk).

Impact (Per Risk Evaluation Criteria)
Scoring: Low = 1, Medium = 2, High = 3

Life/ Health	Reputation	Productivity	Fines/ Legal	Other Financial	Overall Impact Score
L	M	L	M	M	**8**

Recommendation:
Implementation of the recommended mitigation strategy for Risk #2a will also mitigate this risk. For this reason, a separate mitigation strategy is not required for this risk.

7.9 RISK #12A: CERTIFICATION OF HISP OPERATING POLICIES AND TRUST.

Risk:
If the Direct HISPs do not have open and transparent operating policy, perform risk assessment and mitigation according to an established certification process, then federal agencies can have no assurance that sensitive information is being handled responsibly.

Source/Applicability Statement:
Pilot Recommendation: HISPs that manage private keys must perform specific risk

assessment and risk mitigation to ensure that the private keys have the strongest protection from unauthorized use. That risk assessment must address the risk of internal personnel or external attackers gaining unauthorized access either to the keys or to the health information functions for which the keys enforce trust.

Risk Score: (15 = highest Possible risk, 5 = lowest possible risk).

Impact (Per Risk Evaluation Criteria)
Scoring: Low = 1, Medium = 2, High = 3

Life/ Health	Reputation	Productivity	Fines/ Legal	Other Financial	Overall Impact Score
M	M	M	L	L	**8**

Recommendation:
To mitigate this risk, federal Agency STA/HISP should ensure that Direct HISPs have open and transparent HISP Operating Policy and the corresponding HISP Practices Statement. Federal agencies should conduct Directed Exchange solely with HISPs who have been audited and meet policies required by federal agencies such as only including trust anchors in the HISP's trust bundles that assert compliance with privacy laws.

7.10 RISK #28A: BUSINESS ASSOCIATE AGREEMENTS AND MOU FOR TRUST RELATIONSHIPS.

Risk:
If trust relationships do not meet federal standards, then federal agencies may be precluded from participating in Directed exchanges with non-federal recipients:

Source/Applicability Statement:
In the same way that clinicians currently do not assume that it is safe to fax PHI to anyone with a fax number, or mail PHI to anyone with a post office address, Direct users will not assume that it is safe to send messages to any Direct address. Direct users will need to establish real-world trust relationships with other Directed exchange participants on their own terms, but once they have established this real-world trust, they can be sure that their Direct network will securely deliver Direct messages to the trusted Direct user.

Risk Score: (15 = highest Possible risk, 5 = lowest possible risk).

Impact (Per Risk Evaluation Criteria)
Scoring: Low = 1, Medium = 2, High = 3

Life/ Health	Reputation	Productivity	Fines/ Legal	Other Financial	Overall Impact Score
M	M	M	L	L	**8**

Recommendation:
This is the same as Risk #9b in terms of result, and the mitigation strategy for this risk is therefore covered by the mitigation strategy for risk #9b.

8 Mitigation

Table 3 outlines the eight mitigation strategies/recommendations proposed as a starting point to addressing the 10 unique policy concerns, which in turn were derived from 93 issues offered by FHA stakeholder participants.

Table 3: Summary of Recommendations

Mitigation #	Recommendation/Mitigation Strategy	Risk Number	Related Risks	FAQ Reference
1	To mitigate this risk, federal agencies participating in Directed Exchange could determine that the use of Federal Bridge is not required. Normal FISMA mitigations for certification of the communication path are all that is needed. For example, if a trusted Framework such as DirectTrust.org is deemed to be consistent with the policies of the federal agencies, then agencies may choose to leverage this as part of their FISMA mitigation. Refer to FAQ 1 for use of DirectTrust and whether it can be trusted by federal agencies to the appropriate level. Use of manual workflows (e.g. fax, out of band communications) are available as workarounds. Note: DirectTrust is able to positively identify those entities which are cross certified with the FBCA and can assert that position using certificate policy OIDs. In the alternative, if federal agencies determine that the use of Federal Bridge cross certified CAs is required, then federal agencies may require all Directed Exchange trading partners to obtain FBCA credentials.	21a	22a, 3a, 1a, 5, I1, I3, I7, I8, I9, CMS1,	
2	To mitigate this risk, federal agencies participating in Directed Exchange should consider requesting an update to the guidelines from ONC to include "receivers of information should abide by special handling instructions such as do not redisclose, where required by law".	23a	-	

Mitigation #	Recommendation/Mitigation Strategy	Risk Number	Related Risks	FAQ Reference
	Other possibilities include recommendations for use of Data Segmentation to help ensure only authorized individuals, such as providers or individuals acting in an emergency situation can access the information when needed.			
3	To mitigate this risk, federal agencies participating in Directed Exchange should acknowledge that the premise that agencies only accept FBCA credentials should be re-evaluated with respect to Directed Exchange. Federal agencies should consider establishing a policy that provides for acceptance of other trust frameworks that meet federal requirements. The trust frameworks should have been assessed for adherence to federal requirements (including Governance, FISMA, HIPAA etc.) so that agencies can make informed decisions. This would allow agencies to evaluate their participation in order to communicate via DIRECT beyond the limits of the Federal Bridge. To implement Directed Exchange outside of the Federal Bridge trust framework, federal agencies would need to extend trusted credentials to include credentials from entities accredited by approved trust frameworks such as DirectTrust.org (which is the exemplar that HHS brought forward) or similar organizations. If so, the risk becomes normal risk for communication security and compliance with X.509 certificate specifications. Guidelines would then need to be updated accordingly.	28c	-	
4	To mitigate this risk, federal agencies participating in Directed Exchange should implement recommendations already provided by Direct covering the case where HISP have access to unencrypted data or could have access to unencrypted data because they hold decryption keys for encrypted data. As mitigation for this risk, Covered Entities (CE), (this includes federal agencies such as the DoD, VA, CMS, IHS), should establish Business Associate Agreement (BAA) with any HISP providing Directed Exchange services on the CE's behalf that explicitly constrain access, use, and retention of unencrypted or encrypted PHI for which the HISP holds keys. There may be instances where Business	9b	15a, 15c, 28a	

Mitigation #	Recommendation/Mitigation Strategy	Risk Number	Related Risks	FAQ Reference
	Associates wish to sign legal agreements with HISPs. The BA should require the HISP to establish legally enforceable contracts binding any intermediary participating in Directed Exchange services on the CE federal agency's behalf to stipulations at least as stringent and comprehensive as their CE BAA. As mitigation for this risk, federal agencies, which are not CEs, should establish legally enforceable contracts binding HISPs to stipulations at least as stringent and comprehensive as a BAA with a federal Agency that is a CE. Non-CE federal agencies should require their HISPs to establish legally enforceable contracts binding Directed Exchange services provided on the agency behalf to stipulations at least as stringent and comprehensive as the HISP's contract with the federal Agency customer.			
5	To mitigate this risk, federal Agency STA/HISP should consider presenting Terms and Conditions and a warning to the patient upon the patient's initiation of Directed Exchange, regardless of whether the endpoint is trusted or not, to inform them that the patient is responsible for the transaction. If the federal STA/HISP has not established a trust relationship with the endpoint chosen by the patient, then additional warnings may need to be displayed to the patient indicating the level of potential risk for proceeding with the Directed Exchange. Alternatively, the federal HISP may suggest the patient use a non-federal HISP for transactions to untrusted endpoints. This may relieve the agency of the risk, technically, however this approach may not meet the Meaningful Use certification *criteria § 170.314(e)(1) View Download Transmit*, which requires the EHR technology to support patient Directed Exchange transmission, despite the CMS requirement for calculating Meaningful Use measure for criteria allowing any type of transport to be used by the provider's certified EHR because federal Providers are not regulated by CMS [Note i]. Federal agencies should consider whether there is an ethical responsibility to send the information anyway, per the wishes of the patient, in addition to potential for public relationship outfall for declining to facilitate patient Directed Exchange.	2a 23b	1b, 3b, 4b 10b 14b 16b 17b 19b 20 21b 22b 24b 26b 27b 28b 29b, I17, I20	

Mitigation #	Recommendation/Mitigation Strategy	Risk Number	Related Risks	FAQ Reference
	For any of these recommended mitigation strategies, Federal agencies should seek proper legal counsel on requirements for compliance to Meaningful Use certification criteria § 170.314(e)(1) View Download Transmit and means by which to indemnify the organization from any legal liability that may accrue. This recommendation may be helpful and applicable to all Direct users, not just federal agencies.			
6	CAs currently publishes the Certificate Policy (CP) and the Certificate Practice Statements (CPS). The CA also operates as a certificate service provider, under a trust framework (such as DirectTrust), which ensures the CAs operate in accordance with the trust framework. To mitigate this risk, federal agencies should consider only engaging with trust frameworks and CAs which have been reviewed and approved as meeting the base set of federal requirements should be trusted. ONC and federal agencies should monitor these trust frameworks, and participate (as appropriate) to provide continued input and guidance to ensure the frameworks continue to meet federal Requirements. Policy OIDs in a certificate may be helpful for federal agencies to determine which policies the certificate holder is asserting. Examples include the use of OIDs to represent different LOAs, conformance with federal HIPAA requirements, etc.	25a 10a	14a 17a 19a	
7	To mitigate this risk, federal agency STA/HISP should ensure that Direct HISPs have open and transparent HISP Operating Policy and the corresponding HISP Practices Statement. CPs and CPSs. Federal agencies should conduct Directed Exchange solely with HISPs who have been audited and meet policies required by federal agencies such as only including trust anchors in the HISP's trust bundles that assert compliance with privacy laws.	12a	16a	

Appendix A: Points of Contact

Table 4: FHA Stakeholder Risk Assessment Participants

Name	Organization/Title	Email
Bob Dieterle	CMS	rdieterle@enablecare.us
Paul Grant	DoD CIO DoD MHS	paul.grant@osd.mil
Edward Zick	DoD CIO DoD MHS	edward.zick@osd.mil
Timothy Fong	DoD CIO DoD MHS	timothy.fong@osd.mil
Debbie Bucci	HHS ONC	Debbie.bucci@hhs.gov
Glenn Janzen	IHS	Glenn.janzen@ihs.gov
Peter Burton	IHS	Peter.burton@gdit.com
Ravi Nistala	IHS	Ravi.nistala@gdit.com
Bill Williams	IHS	Bill.williams@gdit.com
Ryan Chapman	IHS	Ryan.chapman@ihs.gov
Marty Prahl	SSA	Martin.prahl@ssa.gov
Mike Davis	VA	mike.davis@va.gov
Chris Shawn	VA	christopher.shawn2@va.gov
Marcia Berg	VA	Marcia.Berg2@va.gov
Theresa Hancock	VA	Theresa.hancock@va.gov
Jennifer Teal	VA	Jennifer.teal@va.gov
Elaine Hunolt	IPO-VLER Health	Elaine.hunolt@va.gov
Glen Crandall	IPO-VLER Health	glen.crandall@va.gov
Melissa Sands	IPO-VLER Health	Melissa.sands@va.gov
Brian Jefferson	IPO VLER Health	brian.jefferson.ctr@tma.osd.mil
Eric Larson	FHA	Eric.larson@hhs.gov

Table 5: Subject Matter Expert Support

Additional Stakeholder POCs

Name	Organization/Title	Phone	Email
Dr. David Kibbe	DirectTrust.Org		kibbedavid@mac.com
TBD	NIST		
Deb Gallagher	FBCA		deborah.gallagher@gsa.gov
	FISMA		
	FICAM		
	HITSC Privacy and Security Working Group		

Appendix B: Direct Glossary

Term	Acronym	Definition
Associated X.509 certificate		Associated X.509 certificates must be assigned to at least one of two levels: • Organizational Certificates, tied to the Health Domain Name • Address Certificates, tied to each Direct Address [Source: Applicability Statement for Secure Health Transport v.1, 28 April 2011] An X.509 certificate is a certificate that conforms to the ITU-T X.509 Public Key Infrastructure and Privilege Management Infrastructure standard.
Certificate		A digitally signed representation of information that 1) identifies the authority issuing it, 2) identifies the subscriber, 3) identifies its valid operational period (date issued / expiration date). In the IA community certificate usually implies public key certificate and can have the following types: Cross certificate – A certificate issued from a CA that signs the public key of another CA not within its trust hierarchy that establishes a trust relationship between the two CAs. [CNSSI No. 4009]
Certificate Authority	CA	A trusted entity that issues and revokes public key certificates.
Credential Service Provider	CSP	A trusted entity that issues or registers Subscriber tokens and issues
Circle of Trust		When users of the Direct Project make message handling trust decisions, they will often be able to do so in the context of trusting the identity assurance and authentication policies of an entire group of other Direct Project endpoints. A group of Direct Project endpoints who use certificates issued by a single Certificate Authority and agree to follow the identity assurance, authentication, security, and other policies of that Certificate Authority are considered a "Circle of Trust." By having large groups of endpoints who all agree to identical message handling policy positions, the number of trust decisions that Direct Project Users will need to make will be decreased. Hopefully, this will mean that the quality of each trust decision will be improved. The Circles of Trust concept is a critical part of the Direct Project innovation to enable distributed trust at scale, without sacrificing on the quality

Term	Acronym	Definition
		of trust decisions. Each Circle of Trust is enabled by a single Certificate Authority, which signs the certificates of all of the endpoints of the Circle of Trust and publicly discloses what security posture is enforced within the Circle of Trust. The Direct Project will call such Certificate Authorities "Trust Anchors". [Direct Project Security Overview]
Code Signing		A certificate issued to digitally sign software obtained from remote systems and executed on a local system without explicit installation or execution by the recipient. These certificates are used to digitally sign executable code to ensure the authenticity and integrity of the code. [DOD ECA Certificate Types]
Component Certificate		A certificate issued to devices such as web servers or routers for limiting access or securing communications. These certificates are issued to web servers and other information systems or infrastructure components to enable them to identify themselves to users or other components, and to enable establishment of encrypted communications between components or between users and components. [DOD ECA Certificate Types]
Credential		An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber. While common usage often assumes that the credential is maintained by the Subscriber, this document also uses the term to refer to electronic records maintained by the CSP which establish a binding between the Subscribers' token and identity.
Digital Signature		Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the unit and protect against forgery e.g. by the recipient. [ISO 7498 - 2]. An authentication mechanism which enables the creator of a message to attach a code that acts as a signature. The signature guarantees the source and integrity of the message.[Stallings] An authentication tool that verifies the origin of a message and the identity of the sender and receiver. Can be used to resolve any authentication issues between the sender and receiver. A digital signature is unique for every transaction. [O'Reilly, 1992] A means to guarantee the authenticity of a set of input data the same way a written signature verifies the authenticity

Term	Acronym	Definition
		of a paper document. A cryptographic transformation of data that allows a recipient of the data to prove the source and integrity of the data and protect against forgery. Specifically, an asymmetric cryptographic technique in which each user is associated with a public key distributed to potential verifiers of the user's digital signature used to encrypt messages destined for other users, and a private key known only to the user and is used to decrypt incoming messages. To sign a document, the document and private key are input to a cryptographic process which outputs a bit string (the signature). To verify a signature, the signature, document, and user's public key are input to a cryptographic process, which returns an indication of success for failure. Any modification to the document after it is signed will cause the signature verification to fail (integrity). If the signature was computed using a private key other than the one corresponding to the public key used for verification, the verification will fail (authentication). [ASTM E1762]
Digital Signature Certificate		A certificate that allows the user to digitally sign documents and messages. See " identity certificate."
Direct Address		Provides a method of routing from an origination point to the addressed recipient. A Direct Address is not intended to provide a single, definitive ID for the intended recipient. One real-world person may have multiple Direct Addresses to be used for different purposes (e.g. one address for each practice location, multiple addresses for different processing purposes such as labs, routed to the HER, vs. unstructured messaging, routed to the secure messaging client and copied to the chart). Direct Addresses consist of a Health Domain Name portion and a Health Endpoint Name. E.g. johndoe@direct.sunnyfamilypractice.example.org In the example, direct.sunnyfamily practice.example.org is the Health Domain Name; johndoe@ is the Health Endpoint Name. Direct Addresses MUST be linked to an associated certificate that confirms the identity either of the domain name or of the full address. [Source: Applicability Statement for Secure Health Transport v.1, 28 April 2011]
Direct Certificate		A Certificate, in the context of this document, is a standard X509 Certificate. The Certificate has certain properties that allow software to verify that the certificate was issued to

Term	Acronym	Definition
		the person or organization it purports to, that it is in current standing, etc. Certificates are generally signed by a second certificate held by a Certificate Authority, which establishes policies by which it will issue signed certificates. By inspecting certificates, it is possible to prove that the Certificate was issued by the trusted Certificate Authority, by inspecting a chain of certificates that root to a known Trust Anchor. If you trust a Certificate Authority's issuance policy and you hold a Trust Anchor certificate that corresponds to the Certificate Authority, you can prove that any certificate that purports to be trustworthy does was, in fact, issued by the Certificate Authority (or by a secondary Authority that, in turn, is trusted by the root Certificate Authority). You can do so even if the certificate you hold was obtained through means you do not trust (e.g., by extracting it from a signature you do not yet trust or over the possibly spoofed Domain Name System (DNS)). Note that by "Certificate Authority" we do not mean the usual Certificate Authorities that issue TLS certificates used in ordinary browsers. The Certificate Authorities used for the purposes in this document are likely to either be special purpose for healthcare, or be highly trusted Certificate Authorities that are used for other similar purposes, such as issuing certificates for interoperability with the Federal Government. Note that the same organizations that maintain Certificate Authorities for electronic commerce may also maintain Certificate Authorities for these purposes, but the root Trust Anchors will almost certainly be different. [Direct Project Security Overview]
Encryption Certificate		A certificate used to establish session keys for encrypted communication. These certificates can be used for encrypting information. This type of certificate asserts encryption and does not assert digital signing or non-repudiation. They contain e-mail addresses to facilitate their use in encrypting e-mail messages. The private keys associated with encryption certificates are escrowed. [DOD ECA Certificate Types] A certificate containing a public key that can encrypt or decrypt electronic messages, files, documents, or data transmissions, or establish or exchange a session key for these same purposes. Key management sometimes refers to the process of storing protecting and escrowing the private component of the key pair associated with the encryption

Term	Acronym	Definition
		certificate. [CNSSI No. 4009]
Federal agency	F	Organization established by law and which by policy complies with Federal Law, regulation, Directives, NIST FIPS and Special Publications and requirements of the FPKIPA.
Federal Bridge Certification Authority	FBCA	The Federal Bridge Certification Authority (FBCA) is an information system that facilitates acceptance of certifications for transactions. Since its initial conceptualization and operation, the FBCA has evolved into the Federal Public Key Infrastructure Architecture (FPKIA) that encompasses Certification Authorities (CAs) from multiple vendors supporting different FPKI policy and function. The FPKIA enabling policy CAs are the: (1) FBCA, (2) Federal PKI Common Policy Framework (FCPF) CA, and (3) Citizen and Commerce Class Common (C4) CA. The operation also incorporates the E-Governance Certificate Authorities used to issue Secure Sockets Layer/Transport Layer Security protocol certificates supporting assertion-based credentials for Security Assertion Markup Language (SAML) data exchanges. Source: IT Law]
Health Domain Name		A Health Domain Name is a fully qualified domain name that identifies the organization that assigns the Health Endpoint Names and that is, ideally, dedicated solely to the purposes of health information exchange. E.g. direct.sunnyfamilypractice.example.org. [Source: Applicability Statement for Secure Health Transport v.1, 28 April 2011]
Health Endpoint Name		Health Endpoint Names express real-world origination points and endpoints of health information exchange, as vouched for by the organization managing the Health Domain Name. Examples: • johndoe – referring to an individual • sunnyfamilypractice or memoriallab – refers to organizational inboxes • diseaseregistry – refers to a processing queue [Source: Applicability Statement for Secure Health Transport v.1, 28 April 2011]
Health Information Service Provider	HISP	The term Health Information Service Provider (HISP) 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). In this best practice document, we are mainly concerned with the HISP

Term	Acronym	Definition
		organization and the implications for privacy, security and transparency when the HISP is a separate business entity from the sending or receiving organization. [Source: Direct Project-Best Practices for HISPs]
Identity Certificate		A certificate primarily issued to individuals. This type of certificate asserts the digital signature and non-repudiation and is primarily used to identify the subscriber to information systems. [DOD ECA Certificate Types] A certificate that provides authentication of the identity claimed. Within the NSS PKI, identity certificates may be used only for authentication or may be used for both authentication and digital signatures.[CNSSI No. 4009]
Individually Identifiable Health Information	IIHI	Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and: • Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and • Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and • That identifies the individual; or • With respect to which there is a reasonable basis to believe the information can be used to identify the individual. General Provisions: Definitions - Individually Identifiable Health Information - § 160.103
Message Encryption		The S/MIME protocol supports the capability to encrypt the message as targeted to only the destination Direct Project endpoint identity as described by that endpoint digital certificate. This encryption is mandatory in the Direct Project specifications to protect the confidentiality of the message. [Direct Project Security Overview]
Message Integrity		The S/MIME protocol supports the capability to sign the message for the purposes of transmission integrity, even though the name or direct address of the sender may be included in the signature. This signing capability is mandatory within the Direct Project specifications. The Message Signing and Message Encryption capabilities of S/MIME will provide the necessary message integrity of Direct Project Messages. [Direct Project Security Overview]
Non-Federal Organization	NF	Organization outside of the umbrella of Federal law as applicable to Federal agencies, and which by policy is not

Term	Acronym	Definition
		required to comply with such law, regulation, Directives and other requirements that would otherwise apply to a Federal agency.
Patient Transmit		(ii) Transmit. Enable a user to electronically transmit the transition of care/referral summary created in paragraph (b)(2)(i) of this section in accordance with: (A) The standard specified in § 170.202(a). (B) Optional. The standards specified in § 170.202(a) and (b). (C) Optional. The standards specified in § 170.202(b) and (c). [PART 170—HEALTH INFORMATION TECHNOLOGY STANDARDS, IMPLEMENTATION SPECIFICATIONS, AND CERTIFICATION CRITERIA AND CERTIFICATION PROGRAMS FOR HEALTH INFORMATION TECHNOLOGY]
Personal Identity Verification card	PIV	Standard: FIPS PUB 201-1 Standard: FIPS PUB 201-1. NIST definition: A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, and digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).
Personal Identity Verification card - Interoperable	PIV-I	Standard: FIPS PUB 201-1 Evolved originally for use by short-term federal contractors who had frequent communications with the federal government.
Protected Health Information	PHI	Protected health information means individually identifiable health information: Except as provided in paragraph (2) of this definition, that is: • Transmitted by electronic media; • Maintained in electronic media; or • Transmitted or maintained in any other form or medium. • Protected health information excludes individually identifiable health information: • In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; • In records described at 20 U.S.C. 1232g(a)(4)(B)(iv); • In employment records held by a covered entity in its

Term	Acronym	Definition
		role as employer; and • Regarding a person who has been deceased for more than 50 years. General Provisions: Definitions - Protected Health Information - § 160.103 Health information means any information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.
Receiver		The end-user to whom a message is addressed.
Registration Authority	RA	A trusted entity that establishes and vouches for the identity or attributes of a Subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s). NIST SP 800-63
Secure/Multipurpose Internet Mail Extensions	S/MIME	S/MIME provides a consistent way to send and receive secure MIME data. Digital signatures provide authentication, message integrity, and non-repudiation with proof of origin. Encryption provides data confidentiality. Compression can be used to reduce data size. [Source: Internet Engineering Task Force (IETF) RFC 5751, Secure/Multipurpose Internet Mail Extensions (S/MIME), v. 3.2, Message Specification]
Security/Trust Agent	STA	Software 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. [Source: ONC Direct Implementation Guidelines] A Message Transfer Agent, Message Submission Agent or Message User Agent supporting security and trust for a transaction conforming to the Applicability Statement for Secure Health Transport specification. [Source: Applicability Statement for Secure Health Transport, v.1, 28 April 2011]
Sender		The originator of a message.
Simple Mail Transport Protocol	SMTP	An Internet protocol designed to transfer mail reliably and efficiently. An important feature of SMTP is its capability to transport mail across multiple networks using the Mail

Term	Acronym	Definition
		exchanger mechanisms of the domain name system to identify the appropriate next-hop destination for a message being transported. [Source: RFC 5321, SMTP]
Transition of Care	ToC	Meaningful Use standard for Transition of Care (ToC) CCDA.
Transport Security		For transmission of already S/MIME signed and encrypted content the Direct Project solution is encouraged to support transport level security. This capability can be used to assure that connections are made only to trusted systems, that the network communications are additionally encrypted and integrity protected. For transmission of any content that has not already been encrypted (e.g., incoming SMTP or outgoing IMAP connections to the Full Service HISP), transport level security and encryption is mandated. [Direct Project Security Overview]
Trust Anchor		Each Circle of Trust is enabled by a single Certificate Authority, which signs the certificates of all of the endpoints of the Circle of Trust and publicly discloses what security posture is enforced within the Circle of Trust. The Direct Project will call such Certificate Authorities "Trust Anchors". [Direct Project Security Overview] All of the Direct Project endpoints that are signed by a single Certificate Authority agree to abide by the policies of that Certificate Authority. The Certificate Authority has the responsibility to perform the appropriate auditing to ensure that its policies are enforced. These Certificate Authorities are called "Trust Anchors." Some Certificate Authorities will choose to enforce very detailed and extensive security postures with frequent and thorough audits. Other Certificate Authorities may choose to enforce fewer security measures. The security posture and auditing levels that a given Certificate Authority enforces will be publicly published so that Direct Project users will be able to determine if it is a good decision to trust the Certificate Authority and all of its users. Direct Project users can configure their implementation with the “Trust Anchors” they are willing to trust for sending and receiving messages. Direct Project endpoints might reasonably decide that they will only allow outgoing messages to other Direct Project endpoints who participate in Circles of Trust with comparable or higher levels of enforced security postures. However, they might also decide that they will accept incoming messages from Circles of Trust that have much

Term	Acronym	Definition
		lower standards of security and privacy standards. For instance, a clinic or hospital might choose to accept incoming messages from the users of a PHR system. The PHR system might not perform the same high level of identity assurance on its users that the hospital or clinic requires internally. While the hospital or clinic might be willing to receive messages from the PHR, they might choose to send outgoing messages only after they have manually verified that the address is actually owned by a particular patient. The concept of "Trust Anchors" and the flexibility of configuring "Trust Anchors" distinctly for sending and receiving messages provides the required flexibility for Direct Project users to adopt various policies that they deem necessary for their organization. [Direct Project Security Overview]

Appendix C: Use Cases

This Appendix provides a description of the three use cases under review by the FHA Directed Exchange Sub-Working Group (SWG). These use cases include:

1. Federal agency to Non-Federal Organization
2. Non-Federal Organization to Federal agency
3. Patient Directed Exchange using Federal agency STA/HISP

Other potential use cases have been discarded as not relevant to Federal policy concerns include:

4. Federal agency to Federal agency (Assumed shared policy framework)
5. Non-Federal agency to Non-Federal agency (Out of scope)
6. Patient Directed Exchange using Non-Federal HISP (Out of scope)

1. USE CASE 1. FEDERAL AGENCY TO NON-FEDERAL ORGANIZATION

In this use case the Federal agency is sending a Direct message to a Non-Federal organization. It is assumed that the Non-Federal organization may not need to be in full compliance with all policies that apply to the Federal agency. Pre-conditions establish a basis for mutual trust required between the Sender and Receiver not covered by the Direct Applicability Statement.

Preconditions

The table below provides pre-conditions that apply to this use case. STA/HISP preconditions are determined from a variety of sources as are Sender and Receiver. Direct Project preconditions taken from the Direct WIKI are assumed to apply to all use cases and are provided in a separate Appendix to this Attachment.

STA/HISP Precondition	*Sender* Precondition	*Receiver* Preconditions
• All HISPs must have contractually binding legal agreements with the sender or receiver of directed exchange of Personally Identifiable Information (PII), including all terms and conditions required in a BAA. • Provides any Direct Services that are not explicitly provided by the Sender.	• Sender is holder of Direct Address that appears in the TO line of the SMTP/SMIME message. • If needed, Sender has established a BAA with their HISP.	• Receiver is a member of the Sender's Trust Bundle/Trust Circle that Sender has approved for use by Sender's STA/HISP. • Receiver has a valid X.509

STA/HISP Precondition	*Sender* Precondition	*Receiver* Preconditions
• STA/HISP Knows Sender's Direct Policies. • The operation of the STA/HISP is audited and certified by a recognized accreditation agency as meeting established federal policies for the secure exchange of transactions from federal entities. • A STA/HISP participating in a trust community such as Direct Trust has aggregated trust anchors from those members of a trust community that issues certificates and publishes them within trust anchor bundles. • Trust in Sender/Receiver identity is established by identity proofing those individuals and associating their identity with the Direct address that appears in the subject alt name attribute of the STA/HISP certificate (Per ONC Guidelines, this is NIST SP 800-63-1 LOA3). Per Applicability Statement: • Health Endpoint Names express real-world origination points and endpoints of health information exchange, as vouched for by the organization managing the Health Domain Name. • The organization maintaining the Health Domain Name MUST also associate the Health Domain Name and/or Direct Address with one or more X.509 certificates. • An organization that maintains Organizational Certificates MUST vouch for the identity of all Direct Addresses at the Health Domain	• If needed, Sender has established a BAA with Receiver that is not a CE. • Patient has provided any needed authorization. • Sender has satisfied any message specific needs, e.g., digital signature needed for source authentication and content integrity/repudiatio n, and any encryption required for content security, e.g., masking per applicable policy.	certificate that meets federal requirements with regard to identity proofing at LOA3 of the direct address and issuance with an appropriate policy OID indicating CA compliance with all relevant federal policies and/or the Sender has manually established that the Receiver's CA CP complies with relevant federal policies.

STA/HISP Precondition	*Sender* Precondition	*Receiver* Preconditions
Name tied to the certificate(s). • For STA/HISPs participating in a trust community, certificate policies of the CA explicitly require identity proofing at NIST LOA3 • Binding of the Direct Address with the identity of the address holder can be verified with a policy OID in the Direct certificate held by a STA/HISP and/or by manually examining the CP of the CA that issued the address holder's Direct certificate. • The STA/HISP has obtained necessary verification that the owner of the Direct address in the certificates, which the STA/HISP holds, has been identity proofed to NIST SP 800-63-1 LOA 3. • *Sender* and *Receiver* selected Trust Bundles have been selected based on *Sender* or *Receiver* assurance requirements. • If a *Sender or Receiver uses a* HISP, then the *Sender* and *Receiver* organizations need a discoverable contract for trading partners, which specifies how the organizations expects their HISPs to operate. • If *Sender or Receiver* is CE, then a BAA with HISP must be established, and if not established, under the Omnibus rule, the HISP will be considered a BA anyway.		

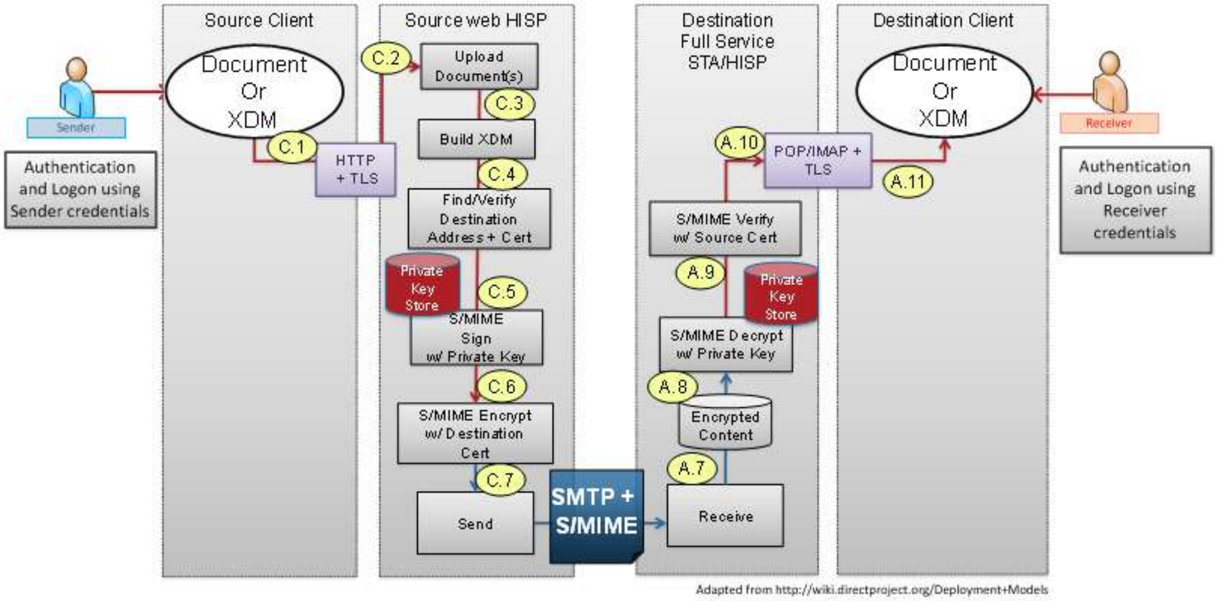

Source Client
Source web HISP
Destination Full Service STA/HISP
Destination Client
Document Or XDM
Sender
Authentication and Logon using Sender credentials
C.1
HTTP + TLS
C.2
Upload Document(s)
C.3
Build XDM
C.4
Find/Verify Destination Address + Cert
Private Key Store
C.5
S/MIME Sign w/ Private Key
C.6
S/MIME Encrypt w/ Destination Cert
C.7
Send
SMTP + S/MIME
Receive
A.7
Encrypted Content
A.8
S/MIME Decrypt w/ Private Key
Private Key Store
A.9
S/MIME Verify w/ Source Cert
A.10
POP/IMAP + TLS
A.11
Document Or XDM
Receiver
Authentication and Logon using Receiver credentials
Adapted from http://wiki.directproject.org/Deployment+Models

Figure 3: Federal to Non-Federal Direct Exchange

1.1. User Story: Federal provider sends clinical summary to a Non-Federal Provider using Direct

Federal Web Portal with Full Service STA to Non-Federal e-Mail Client with Full Service HISP.

1.1.1. Sender to Sender's HISP

Primary care IHS physician Dr. B. Wells is a Federal Sender who initiates a Direct message using an EHR or via a local web portal. In this example, she has referred one of her patients to a gastroenterology specialist, Dr. G. Aye, a non-federal IHS clinician in a Tribal Clinic, and she would like Dr. Aye to have some background information about the patient. She uses her EHR to generate a clinical summary and sends it to Dr. Aye using the EHR or her web portal and a Direct address that Dr. Aye gave her. Her EHR or web portal authenticates to establish its identity to her organization-managed STA, and then it delivers the message including the clinical summary to the STA (link encrypted with HTTPS/TLS if separate from the EHR or Portal).

Workflow:

a. Dr. Wells has authenticated to her EHR system as required and the organizational Direct web portal.
b. Dr. Wells may optionally digitally sign the medical documentation using her PIV card and EHR signature services for content data integrity/source

authentication purposes (outside the scope of Direct specifications) (see Author of Record Level 2 Use Case for the S&I standard for digital signatures on documents).

c. Dr. Wells' EHR or web portal authenticates to the organization STA.
d. Dr. Wells' EHR or web portal delivers the to the organization's STA
e. Dr. Wells' organization trusts the Sender's STA, which trusts that the Receiver's HISP has authenticated the Receiver e-mail client, which has authenticated Dr. Aye.

1.1.2. Sender's STA to Receiver's HISP

Dr. Wells' STA, after locating and verifying the address of the Receiver, as indicated in the "To" address in the message, must communicate with the Receiver's HISP by authentication, encryption, and digital signature for message (vs. content) confidentiality, and integrity, and finally message transmission. Once the message has arrived at the Receiver's HISP, it needs to be decrypted, verified, and delivered to the intended recipient.

Workflow:

a. Sender STA must authenticate to Receiver STA (S/MIME signature)
b. Sender STA verifies Receivers public key meets policy requirements (e.g. certificate has not expired, belongs to Trust Bundle accepted by Sender organization, etc.)
c. Sender STA encrypts message using Receiver's public key (S/MIME)

1.1.3. Receiver's HISP to Receiver

Dr. Aye doesn't have an EHR, but he already uses e-mail software that is capable of handling secure (encrypted) messages. Dr. Aye's e-mail software authenticates to the HISP that Dr. Aye is using to provide him with Direct Project services and gets the message, displaying it within an inbox of messages. Dr. Aye has chosen to keep multiple e-mail accounts to separate his Direct messages from his normal e-mail, so his inbox contains only clinical messages sent via the Direct Project. He sees the message from Dr. Wells which Dr. Aye's HISP had decrypted and verified that the digital signature used for message integrity during transmission. Dr. Aye uses the procedure that his e-mail software requires to open the e-mails, in order to open the attached clinical summary. He sees Dr. Wells' description of the patient's problems, medications, allergies, and recent diagnostic tests, and he is now well briefed for the patient's visit later today.

Workflow:

a. Receiver authenticates to Receiver e-mail client
b. Receiver verifies the Sender's credential used to sign the message (not the content) for transmission.
c. Receives message. The Receiver trusts the Receiver HISP that trusts the Sender STA that has authenticated the Sender EHR/e-mail client that has authenticated Dr. Wells.

2. USE CASE 2. NON-FEDERAL PROVIDER TO FEDERAL PROVIDER

Non-Federal e-Mail Client with Full Service HISP to Federal Web Portal with Full Service STA

2.1. Non-federal Sender to Sender's HISP

IHE Tribal Clinic Gastroenterology specialist, Dr. G. Aye, is a non-Federal Sender who initiates a Direct message using an email client with a full service HISP. In this example, Dr. G. Aye, would like to send referring federal provider, Dr. B. Wells, consult notes related to Dr. Wells' referred patient. He uses EHR to generate an electronic, encode consult note, and attaches this to an email addressed to Dr. Wells. His email client authenticates to establish his identity to his organization's HISP, which delivers his email message including his consult note to the HISP link encrypted with HTTPS/TLS.

Workflow:

a. Dr. Aye has authenticated to his email client as required.
b. Dr. Aye may optionally digitally sign the consult note using a PIV-I card and EHR signature serves for content data integrity/source authentication purposes (outside the scope of Direct specifications) (see Author of Record Level 2 Use Case for the S&I standard for digital signatures on documents).
c. Dr. Aye's email client authenticates to the organization's HISP, which trusts Dr. Wells' Receiver STA to authenticate the Receiver's EHR/web portal, which authenticates Dr. Wells when she logs on and downloads Dr. Aye's consult note.

2.2. Sender's HISP to Receiver's STA

Dr. Aye's HISP, after locating and verifying the address of Dr. Wells, the Receiver, as indicated in the "To" address in the message, must communicate with the Receiver's STA through similar steps of authentication, encryption, and digital signature for message (vs. content) confidentiality, and integrity, and finally message transmission. Once the message has arrived at the Receiver's STA, it needs to be decrypted, verified, and delivered to the intended recipient.

Workflow:

a. Sender HISP must authenticate to Receiver STA (S/MIME signature)
b. Sender HISP verifies Receiver's public key meets policy requirements (e.g. certificate has not expired, belongs to Trust Bundle accepted by Sender organization, etc.)
c. Sender HISP encrypts message using Receiver's public key (S/MIME)

2.3. Receiver's STA to Receiver

Dr. Wells authenticates to her EHR/Web portal integrated email client, which authenticates to Dr. Wells' organizational STA to provide her with Direct services. Dr. Wells receives Dr. Aye's message, which her STA has decrypted and verified the digital signature used for message integrity during transmission. Dr. Wells uses the procedure that her EHR/web portal requires in order to open the attached consult notes from Dr. G. Ayes about his clinical findings related to the patient she had referred.

Workflow:

a. Receiver authenticates to Receiver e-mail client
b. Receiver's STA verifies the Sender's credential used to sign the message (not the content) for transmission.
c. Dr. Wells receives Dr. Aye's message. The Receiver trusts the Receiver STA, which trusts that the Sender's HISP has authenticated the Sender's e-mail client, which authenticated Dr. Aye.

3. USE CASE 3. PATIENT DIRECTED EXCHANGE FACILITATED BY FEDERAL AGENCY STA TO NON-CE PHR

Federal Web Portal with Full Service STA to Non-Federal PHR e-Mail Client with Full Service HISP.

3.1. Federal Sender to Sender's STA

Primary care IHS physician, Dr. B. Wells, is a Federal Sender who facilitates her patient's (Major Betty) request to transmit Dr. Wells' clinical summary and Dr. Aye's consult notes to the patient's non-federal PHR. Using her EHR's patient web portal, Dr. Wells enables her patient, Major Betty, to transmit the requested information via her organization STA to Major Betty's non-federal PHR Direct address via the PHR HISP.

Major Betty, authenticates to Dr. Wells' EHR patient portal, selects the records to be transmitted to her designated PHR Direct address, consents to the disclosure, and pushes the "send" button. The patient portal authenticates to establish the patient's identity to Dr. Wells' organization managed STA, and then delivers the patient's message with the attached clinical summary from Dr. Wells and the consult notes from Dr. Aye to the STA (link encrypted with HTTPS/TLS if separate from the EHR or Portal).

Workflow:

a. Dr. Wells' patient authenticates to Dr. Wells' organization Direct patient portal as required.
b. Dr. Wells' Direct patient portal authenticates to the organization STA.
c. Dr. Wells' Direct patient portal delivers the message (over a HTTPS/TLS encrypted link if required) to the organization's STA.
d. Dr. Wells' organization Direct patient portal trusts the Sender's STA, which trusts that the Receiver's HISP has authenticated the Receiver e-mail client, which has authenticates the patient when he/she logs into his/her PHR account.

3.2. Sender's STA to Receiver's HISP

Dr. Wells' organization Direct patient portal STA, after locating and verifying the address of Major Betty's PHR Direct address, as indicated in the "To" address line in the email , and after signing/encrypting Major Betty's transmitted payload, must communicate with the Receiver's HISP (Major Betty's PHR HISP) via SMTP/SMIME. Once the message has arrived at the PHR HISP, it needs to be decrypted, verified, and delivered to the intended recipient – i.e., the Major Betty's PHR account.

Workflow:

a. Sender STA must authenticate to Receiver HISP (S/MIME signature)
b. Sender STA verifies Receiver's public key meets policy requirements (e.g. certificate has not expired, belongs to Trust Bundle accepted by Sender organization, etc.)
c. Sender STA encrypts message using Receiver's public key (S/MIME)

3.3. Receiver's HISP to Receiver

Major Betty's PHR uses e-mail software that is capable of handling secure (encrypted) messages. Major Betty's PHR e-mail software authenticates to the HISP that Major Betty is using to provide her with Direct services, and gets the message, displaying it within an inbox of messages.

Major Betty authenticates to her PHR account, and uses the procedure that her e-mail software requires to open the e-mail. Major Betty's PHR allows her to incorporate a decrypted copy of the clinical summary from Dr. Wells and Dr. Aye's consult notes into her PHR overall clinical summary while persisting the encrypted inbound clinical summary and consult notes, i.e., by selecting this option, Major Betty does not "break the seal" on the provider-sourced information.

Workflow:

a. Receiver authenticates to Receiver e-mail client.
b. Receiver verifies the Sender's credential used to sign the message (not the content) for transmission.
c. Receiver trusts the Receiver HISP, which trusts that the Sender's STA has authenticated the Sender's e-mail client, which authenticated Dr. Wells.

Appendix D: FAQ

- to be inserted -