Directed Exchange Workgroup: Public Comments and FHA Responses for Directed Exchange Documents

In November 2013, the Directed Exchange Workgroup completed and released four key documents highlighting the results of their efforts including a Patient Identity in Directed Exchange recommendation, Risk Assessment, Frequently Asked Questions and Directed Exchange Guidelines presentation.

This document is a subset of the feedback received for these documents and responses from the Directed Exchange Security Sub-Workgroup. For questions or concerns, please contact Eric Larson at eric.larson@hhs.gov.

Patient Identity in Direct

Description	Response
Page 18 says, "Depending upon particular application LOA 2 and LOA 3 are currently considered to be the minimum levels of assurance appropriate for patient access to their own health records contained in a data holder's EHR." These two levels of assurance are different and both cannot be considered the minimum.	Agreed to make the change.
If providers must be identity proofed at LoA 3 and the defined HISP ISSOs will be identity proofed at LoA 3 (page 22), how can it be concluded that LoA 2 is sufficient for people (page 16)? The minimum LoA required for exchange of patient private health information should be LoA 3, so as to maintain the level of trust within the system at this achievable level. To lower the minimum required in one part of the exchange, causes the whole system to have less integrity.	LOA is determined by assessment of risk, policy, the scope of information that the user has access to, role and needs as described in the use paper.
Page 12 says, “Using Data Holder credentials provides assurance of provenance of the medical record. First it is the provider ‘vouching for’ the information and its relationship to the patient. The receiver may also have greater assurance that the transmission is exactly what was in the provider EHR or what was sent from PHR	We have modified this for clarity. If you need assurance of the content, DirectTrust doesn’t provide that so you need a signature under the content to trace back to the source.

Description	Response
entries for a specific patient. Second, the recipient is not dependent upon the level of assurance provided by the Direct Cert for the content but rather by the credential used by the data holder to sign the payload. What is this paragraph actually saying? Might there be higher levels of assurance that the information exchanged is accurate when a patient "vouches for" their own, actual, information? Who has a more accurate picture of what medications the patient is actually taking, the person taking the medications, or the person who prescribed them? Who has more accurate information about a patient's allergies and intolerances, family history, social history, symptoms, etc., the person whose life it is, or a physician who sees the person a couple times a year or less for a few minutes? What evidence supports these assertions?	
Page 12 says, "This OPTION eliminates many of the complexities and risks of OPTION 1 and 2, however, the concern regarding patient directed communication to an endpoint not in the sender's trust bundle remains." What is the concern? This statement is made twice in the document, but is not explained anywhere. The nature of this concern and rationale for it being a valid concern needs to be documented.	It is a policy matter. A DoD example is, "end to end system security is a must." Inserted comment in document for clarity
Page 15 says, "This paper establishes e-Authentication LOA 2 as the minimum for patient exchange of private healthcare information with federal agencies using Direct." This conclusion is not strongly supported with evidence or logical argument.	This conclusion is based on the risk assessment performed by the FHA Directed Exchange Security SWG. The statement was added in the document
Page 16 includes the following conclusion, "Source authentication methods provide another standard security approach to assuring permanent record of trust in the message content." This conclusion seems outside the scope of the paper.	The paper consists of two parts, first addresses the specific issue of patient assurance and the second part considers the related part of patient use of direct which the conclusion documents.
Page 16 asserts, "Trust can be established in advance or at the time of message delivery." It also seems possible	This was re-worded in the paper, first bullet under Conclusions as: "Yes.

Description	Response
that the trustworthiness of the information can be established after receipt and before action is taken to incorporate or act upon the information. Was that possibility considered?	Information trust or source authentication is included in the context of actions by the recipient upon "message delivery" meaning that the information is in the possession of the recipient. The section on Trust Frameworks also includes the broader concept of technical, operational and legal conditions for trustworthy exchange which may be established statically (e.g. DURSA, Trust Bundle) or potentially negotiated dynamically at runtime. The latter represents policy about how the sender can trust the recipient's behavior with the information (not to further re-disclose to unauthorized recipients in the case of 42 cFR Part II information for instance) rather than simple non-repudiation or source authentication of the information."
Page 17 includes definitions. Shouldn't Trust Bundles, Trust Frameworks, and "full service" HISP be explained in this appendix?	Made the change. Thank you
Pages 21-23 describe patient directed exchange under a full-service HISP. What are the expected or predicted costs to providers, provider organizations, and individuals to obtain the Direct e-mail services via this model, on an annual basis?	This is an economic assessment outside of the scope of the policy domain of the FHA Directed Exchange activities. That said, the federal approach closely follows development in the public space and the requirements for Meaningful Use.
Page 22 describes a step where the person's private key is installed in the HISP services protected key database. This is not safe. One's private key should not be shared with anyone. Why would someone want their private key to be installed in a HISP database? Private keys are meant to be controlled by the personal they are issued to, and kept private. Why would you want to design a system that requires them to be shared with the parties	Direct supports the notion of STAs and HISPs. The model is principally one of providing transport security to the exchange. End user authentication is not provided and end user assurance is provided second hand via RA, CA, HISP and organizational policy. It is for this reason that the Non-repudiation bit in

Description	Response
managing the HISP?	a Direct credential is turned off. Refer to the Direct Applicability Statement for further details.
Page 22 says, "The HISP ISSO will receive tokens (certificates) for all domain users and will be responsible for installing them into the HISP. The HISP will manage and protect these tokens associated with domain Trust Circles and Trust Bundles according to the policies and practices of the Trust Framework for which they are a certified member." How will "regular people" understand and assess these policies to determine the risk of breech or unwanted sharing? Additionally, this design would seem to make large-scale breech a bigger risk. A breech could more easily affect a much larger number of individuals when many private keys are all contained in a single data base rather than residing with the individuals to whom the private keys had been issued.	This is a valid question. The trust in the HISP is dependent upon the policies of the CA and upon the governance framework of the HISPs themselves. Such frameworks are provided by DirectTrust, for example, which provides assurance to relying parties that keys and governing policies are in fact implemented in a trustworthy way. As for the PHI/HISP relationship vs. risk of breech, the risk is mitigated by a trust framework, governing policies and certifications.
Page 25 says, "In order to receive the patient's Direct mail: The Sender's certificates must be part of a Trust Bundle that the recipient accepts. The receiver's STA/HISP must decrypt the message using the recipient's private key, then verify the message using the sender's public key (additional verification of the integrity of the unencrypted message headers may also be required.) The "From" address DNS lookup must retrieve a credential that can be used to validate the message transmission integrity." Why would the system be designed to decrypt the mail message in the middle of the communication between the sender and the receiver? Doesn't the Direct standard define a point-to-point mechanism which does not require a system to intervene in the middle? Doesn't this specification alter the role of the full-service HISP, making it an organization that needs to be held accountable under HIPAA as a Business Associate? Further, how does patient identity assurance relate to this design choice to require the HISP to decrypt the message in the middle? Are the two really related at all?	The questioner is referred to the Direct Applicability Statement. The Federal Directed Exchange WG has no authority over the Direct specification. What this WG is doing is expressing policy and guidelines applicable to federal participants consistent with the existing Direct Applicability Statement. These may not be the same policies that a non-Federal entity would choose. The issue regarding the HISP as a business associate was addressed in a Federal Directed Exchange guideline stating that a BAA was required. The core requirement is that the HISP authenticate a patient at LOA2. This is part of an end-to-end Patient to HISP (SSL), ->HISP to HISP->HISP to Receiver (SSL) piecewise continuous by not end-to-end communication.

Risk Assessment

Description	Response
RISK 12a: In my role as treating clinician, I want to send PHI via encrypted e-mail to any other HIPAA covered entity at any time and with minimal risk and ensure that the PHI will be properly processed for the benefit of my patient. I don't need a third party (HISP) to control my private encryption keys, and act as a STA on my behalf when I can do it myself with less risk and no need for a BAA. The risk score should be high (15) for a conventional HISP because the opportunity for breach is 100%, whereas PHI sent via a conduit HISP is near 0% because the information is continuously encrypted in transit between sender and receiver. While the BAA acts as a legal contract to assign risk, no such contract is needed for a conduit HISP using STA to STA communication. The current risk score of 8 is an inadequate of actual risk represented by a known man in the middle attack; it represents a failed risk assessment that dictates a specific architecture that will harm patient privacy and safety.	The FHA Directed Exchange Working Group is focusing on the HISP to HISP communications as the most common approach. This approach is reflective of the architecture chosen by federal agencies. We concur that other approaches are possible and explicitly allowed by the Direct Applicability Statement. The purpose of the BAA within the HISP/HISP architecture is to meet legal requirements and to provide mitigating mechanisms applicable to this approach.

Guidelines Doc

Description	Response
The Massachusetts Medical Society, which represents over 24,000 physicians, medical residents and students, appreciates the opportunity to provide the following comments in response to the Federal Health Architecture Workgroup's document on Guidance for Directed Exchange. At its December 2013 meeting, the Massachusetts Medical Society adopted a resolution which stated that " all Direct secure e-mail systems... including health information exchanges and electronic health record systems, allow a licensed physician to designate any specified Direct recipient or sender without interference from any institution, electronic health record vendor, or intermediary	Thank you for your input. We agree that the model of PIV card user to FBCA compliant PIV card user (or LOA3 equivalent) along with an appropriate policy and governance environment using an email system is an acceptable approach (assuming the acknowledgement requirements of Direct are also met). This is generally consistent with federal policy but not consistent with the majority of Direct implementations today and is in fact considered to be limiting in practice. Nor does it adequately address patients as Direct users. The goal of the FHA Directed Exchange Working Group is to identify the policies and practices that would enable the greatest participation in Direct rather than

Description	Response
transport agent." We recommend that the FHA Directed Exchange Workgroup incorporate this thinking into these documents. Specifically: Any licensed physician holding a Federal Bridge conformant credential with a Direct address can use that Direct address to communicate with anyone anywhere having any Direct address in either direction without technical interference from the EHR, EHR vendor, HIE, or other trust intermediaries associated with the physician's Direct service. The Federal bridge conformant credential is by current definition strongly bound to a single real person. Any automated sharing or delegation would not be supported using this specific Direct email address but nothing prevents the physician or their institution from issuing other, less restrictive credentials as well. Take as an example a physician Dr. Pixel using an e-mail client that supports S/MIME encryption such as Microsoft Outlook. When Dr. Pixel has a Federal Bridge conformant credential linked to that client, he or she should be able to message other physicians using a Direct-capable EHR, or using a state health information exchange. Physicians, including FHA physicians, should also be able to message patients who have a Direct certificate and email address without interference by intermediate transport agents. The Physician's institution, EHR or Direct Trust agent can warn the physician if the other party is not trusted and why, but they cannot prevent the physician from overriding the warning.	specify a specific implementation, however, attractive. Specifically; the choice of the term "...without interference from any institution..." implies an environment in which end-users operate outside of the organizations policy framework. In fact, organizations are responsible for the safety, security and privacy of communications. Federal agencies are always responsible for the actions of their employees (including clinicians) and for the security and privacy of their information systems. In no case, would a federal agency delegate such responsibility to an end-user. In such a model, in the event of a breach or any other insecurity (e.g. unauthorized re-disclosure or disclosure not in accordance with a patient consent) who is legally responsible? While your proposal identifies Federal Bridge compliant credentials, it does not put similar restrictions on the recipient or the sender in the case of information received from external sources. From the federal agency perspective, this means that the trust in the sender-recipient exchange cannot be assured nor would it meet the requirements for a federally compliant Trust Bundle. Finally, Federal Bridge compliant credentials are just one aspect of a complete DirectTrust framework. We believe that policy approaches at such as DirectTrust provide the additional security needed to guarantee an appropriate policy environment for the exchange of protected health information within Direct as an exemplar for Direct implementations.