LINKING HEALTHCARE COMMUNITIES

FHA Directed Exchange Guidelines

Consensus Recommendations of the FHA Federal Directed Exchange Working Group

May 2015

Office of the National Coordinator for Health IT

Scope of the Guidelines

Guidelines are recommendations, each agency is free to determine their own policies

"The recommendations of the FHA Work Group have been developed in consultation with NIST, ONC and Federal PKI subject matter experts and industry leaders and represent our best understanding of best practice in accordance with our risk, current technology and law as applicable to federal agencies.

As such the recommendations are intended as workable guidelines for federal agency policy makers. Nothing in the guidelines are intended to be prescriptive or binding in nature. It is ultimately left to each agency to consider the guidelines in the context of their own policies."

Who Do You Trust?

Guideline 1:

Accept only Federal Bridge Certification Authority (FBCA) or FBCA cross-certified certificates or other trust framework certificates as approved by the federal partners in consultation with FBCA

Recommended Activities:

- Support federal participation in maturing DirectTrust frameworks.
- Continuously re-evaluate this guideline with assistance of *FICAM, *FPKIPA.

Safe harbor, stay the course with FBCA

Who Do You Trust? *Continued…*

- Direct is still in its infancy and not widely deployed in federal agencies.
- Emerging non-federal trust frameworks express a goal of consistency with the Federal Bridge but have not yet been validated for compliance.
- It is possible that non-federal trust frameworks could reach maturity, compliance or equivalence with the Federal Bridge within two years.
- Federal agencies currently have no real method to verify these emerging frameworks or their assertions.

Security Through Certificates

Guideline 2:

Provide data origin authentication and non-repudiation through trusted credentials maintained under the continuous control and possession of the credential owner.

Recommended Activities:

- Consistent with Guideline 1, federal agencies can trust individual signing certificates that chain to the Federal Bridge.
- Monitor adoption of Centers for Medicare & Medicaid Services esMD policies for Federal Bridge cross-certified certificates used for document signing purposes.

STA/HISP Certificates used to secure the S/MIME transmission path do not provide end user authentication or non-repudiation.

Individually-owned digital signature for non-repudiation

Federal Trust Bundles

Guideline 3:

Accept credentials that include Trust Framework Object Identifiers (OID) and trust bundle policies meeting HIPAA, FISMA, National Institute of Standards and Technology and applicable federal jurisdictional policy.

Recommended Activities:

- Within emerging trust frameworks, develop proposed federal common trust bundles.

Some trust frameworks' (e.g. DirectTrust.org) Certification Authorities can assert OIDs for both the Federal Bridge and the commercial trust framework.

This approach can be used to leverage federal and Direct certificate policy frameworks and possibly future Direct Federal Common Trust Bundles.

Minimum Level of Assurance (LOA) Policies

Guideline 4(a) Organizations and/or healthcare related professionals: Adopt LOA3

Guideline 4(b) Patients and/or consumers: Adopt LOA2 and begin transition planning for multi-factor authentication (See Executive Order 13681/Slide 15)

Recommended Activities:

- Consistent with Guideline 3, include LOA requirements within scope of developing a Federal/Patient Common Trust Bundle policy.

Trust in the binding of a real person to a Direct address rests in the CA certificate policy (CP). Consequently:

a)End users not in possession of Direct private keys associated with Direct certificates are potentially more weakly bound, hence trust may be less assured.

b)Technical mechanisms to verify level of identity assurance are not ubiquitously deployed within Direct.

c)Please see Certificate Issuance and Assurance in Direct Messaging White Paper http://healthit.gov/sites/default/files/certificate_issuance_and_assurance_in_direct_messaging_final_4915.pdf

HISP Considerations

Guideline 5:

Federal agency policy should ensure Personal Health Information (PHI) is only sent to/received from endpoints managed by HISPs where both sender and receiver have a Business Associate Agreement with their respective HISP.

Recommended Activities:

- Consistent with Guideline 3, include BAA requirements within scope of a Federal Common Trust Bundle policy.

HISPs have possession of both encryption/decryption keys of all users/organizations; meaning that they have access to unencrypted sensitive personally identifiable healthcare information. Policies need to be in place so that federal agencies can be assured that their HISP meets minimum standards of trust and governance in this case.

Always remember HIPAA applies

Domain-Bound Certificates

Guideline 6:

Adopt policy to require S/MIME header protection of domain-bound certificates to avoid possible substitution attacks.

Appropriate implementation of Direct security standards for domain-bound certificates reduces the need for individual patient certificates.

Recommended Activities:

- Support universal adoption of S/MIME header protection/verification for integrity.
- Ensure STA/HISP policy requires use of header protection for transmit/receive.
- Support trust frameworks such as DirectTrust that incorporate S/MIME header protection policy.
- Implement Direct Implementation Guide header protection features.
- Adopt FHA Federal Common Trust Bundle policy specifying S/MIME header protection.

Patient Directed Exchange (1 of 3)

Guideline 7:

Support patient use of Direct as a user. Provide MU2 View, Download, Transmit (VDT) as a service.

Common Guidelines

- Ensure that patients are aware of all risks and agency rules, and accept full responsibility for VDT "transmit" as a condition of use (Model Disclaimer included in notes. Adapt as needed).
- Consult with Agency Office of the General Council for additional guidance on patient VDT conditions of use.

Provide patients meaningful access and use of VDT to any endpoint of their choice as allowed by policy

Patient Directed Exchange (2 of 3) *Continued…*

Option 1: Agency Managed (sent on behalf of):

Agency sends Personal Health Information (PHI) per patient request. Agency uses federal agency supported trust bundles and policies, i.e., continues to apply federal security standards and policies when acting "on behalf of" a patient. Ensure patient signs a written understanding and acknowledgement of conditions and limitations of use.

Federal agencies acting to assist the patient to send their own information are responsible for delivery and federal policies apply. The patient may not be able to send to destinations not consistent with the federal policy.

Patient Directed Exchange (3 of 3) *Continued…*

Option 2: Patient Managed

(Patient Right of Access):

Patient sends their own information using federal agency provided equipment. Patient managed means that the patient is in possession of their information upon "Download" and thereafter controls "Transmission" exclusively under patient right of access policies.

- Ensure patient signs written understanding and acknowledgement of conditions of use and acceptance of liability.
- Ensure General Council approval.

When patients take possession of their own information, they choose what they send and to whom they send it. Federal policies do not apply.

Acknowledgements

- **FHA Directed Exchange Project Manager**
  Eric Larson, Eric.Larson@hhs.gov

- **FHA Directed Exchange Work Group Chair**
  Glen Crandall, Glen.Crandall@va.gov

- **FHA Directed Exchange Security Sub-Work Group Chair**
  John “Mike” Davis, Mike.Davis@va.gov

- **FHA Directed Exchange Implementation Sub-Work Group Chair**
  Robert Dieterle, rdieterle@enablecare.us

Supplementary Materials

Executive Order 13681, Improving the Security of Consumer Financial Transactions

Though this order refers to financial transactions, there is language in section 3 of the order that has implications for making personal data accessible to citizens through digital applications.

The following points should be considered when exchanging direct messages with federal agencies:

- Multi-factor authentication to provide stronger online security;
- An effective identity proofing process to validate citizen's identity; and
- Procedures consistent with the guidance set forth in the 2011 National Strategy for Trusted Identities in Cyberspace (NSTIC).

Please see https://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions **for more information.**

Model Disclaimer Patterns: *Sent on Behalf of*

Your Health Summary comes from your <Org> medical record. If you choose, you may send your summary to a participating non-<Org> provider, organization, or other application. They must first agree to a set of policies to protect your information. By agreeing you understand:

- You have the right to access your Health Summary
- You are asking <Org> to act on your behalf. By doing so, <Org> will send a copy of your Health Summary somewhere else
- The recipient must have a trust agreement with <Org>

Once your health information is sent to another party, it may no longer be covered by state and federal privacy protections and could be re-disclosed by the person or organization receiving it.

I have read the Disclaimer and Agree.

Model Disclaimer Patterns:
Patient Right of Access

Your Health Summary comes from your <Org> medical record. If you choose, you may send your summary to a participating non-<Org> provider, organization, or other application of your choice. By agreeing you understand:

- You have the right to access your Health Summary
- You are sending you Health Summary to somewhere you choose
- <Org> bears no responsibility for the health information you chose to send. This includes the privacy, use or re-disclosure of your health information.

Once your health information is sent to another party, it may no longer be covered by state and federal privacy protections and could be re-disclosed by the person or organization receiving it.

I have read the Disclaimer and Agree.