Recommendations for Establishing Trust Relationships

(last updated 05/21/2015)

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

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

Website: healthit.gov/fha

General Email: federal.health@hhs.gov

Purpose

It is recommended that the Healthcare Directory Work Group (HcDir Work Group) consider establishing internal and external trust relationships by utilizing Provider Electronic Service Information (ESI).

Introduction

Provider ESI includes the end point address that allows electronic communication with a recipient. It allows healthcare providers to send and receive a patient's medical information from his/her electronic health record. Examples of applications that utilize ESI are DIRECT (email) addresses and eHealth Exchange's Uniform Resource Identifiers (URI). This document envisions federal agencies using ESI in order to successfully send specific data from a healthcare directory to a particular recipient.

The efficacy of Health Information Exchanges (HIE) and its supporting methodologies are contingent upon the ability for a given recipient to retrieve accurate ESI information. For agencies that provide and support the payment for healthcare services, secure, robust, and scalable semantic ESI interoperability can lead to improvements in the quality of care and ultimately reduce costs in the long term. Based on specific recommendations constructed by the HcDir Work Group, an instantiation of a standard healthcare directory system would meet an agency's expectations for delivering ESI information in a secure and reliable manner.

The recommendations noted below are provisional and require further research and analysis by the FHA team and the HcDir Work Group.

Proposed Solution

A healthcare directory framework must have a baseline of collaborative ESI policies and definitive criteria in order to be effective for initial agency adoption. A few examples of the topics that may need to be addressed are authentication, access, security, and data quality (including validity and reliability). Providing a sense of flexibility for agencies to accommodate their needs without adversely impacting other agency's participation in the collaborative effort is essential for finalizing these policies. The recommendations focus on how a collaborative set of ESI policies can potentially accommodate the needs of the federal partners.

The recommendations also focus on specific trust and policy issues as it most closely relates to ESI integration. Addressing these issues will encourage future efforts and analyses that will also support the collaborative baseline policies and governance mentioned above. It will also support the underlying engineering and implementation standards and technologies as the HcDir Work Group develops a collaborative Healthcare Directory framework. Agencies that currently participate in the HcDir Work Group have come to a consensus that economies can be achieved through publishing information via inter-agency, intra-agency, and for external interoperability purposes.

The use cases below provide a detailed description of trust scenarios as it relates to a specific agency:

- Individual agency information (entries and/or data fields) that are not intended to be shared (individual agency use only).

- Individual agency information (entries and/or data fields) that are intended to be shared with authenticated agencies.
- Individual agency information (entries and/or data fields) that are intended to be shared with non-agency authenticated users.
- Individual agency information (entries and/or data fields) that are intended to be shared with non-authenticated users.

Trust Policies & Access Control for ESI

The following provides a detailed set of potential trust and access control policies.

Table 1. Trust Policies using Authentication & Access Control for ESI Use Cases

Enforce Trust Policies using Authentication and Access Control for Electronic Service Information (ESI)	
Referenced Use Cases	HL7 Security Use Cases S&I Frameworks Data Access Framework Use Cases
Pre-conditions	• Agencies may publish information for intra-agency, inter-agency, and non-agency ESI. • Agencies may store information for their internal use only. • Members of agency-trust-groups follow common baseline authentication and policy requirements similar to CONNECT users in a gateway to gateway trust. • Stewards of specific agency data may receive queries from agency trust groups which may or may not contain a security token and depend on implementation and underlying architecture to which they may or may not choose to reply. • An agency reserves the right to selectively respond to certain queries, (e.g. within its own agency, from agency trust groups, etc.) • An agency's data steward will have an Organizational Policy Resolution (OPR) function for resolving and enforcing specific rules based on specific agency policy. Rules will be as simple or as complex as required by that specific agency. • Although agencies publishing information and responding to queries are normally the authoritative source of that ESI, there may be exceptions to this policy as some organizations may have a need to publish ESI for which they are not the authoritative source. • Agencies can store copies of information for which they are not the authoritative source for their own agency use.

Table 2. ESI Sharing Classes

ESI Sharing Classes	**Description**
Scenario 1: ESI Consumer is granted access to an entire agency healthcare directory data store	• Without authorization, entire directory is restricted • OPR function determines authenticated ESI consumer's scope of access rights is an authenticated and only authenticated agency trust group ESI have access to its information

Scenario 2: ESI Consumer is granted access to individual or organization entries	• Without authorization, all individual and organizational entries for an agency are restricted • OPR function grants an authenticated ESI consumer access to a pre-defined group of individual and/or organizational entries (including relationships between individuals and organizations, where appropriate) for an agency which they have been granted access
Scenario 3: ESI Consumer is granted access to specific elements of an entry	• OPR function grants an authenticated ESI consumer access to a pre-defined group of elements for entries for which they have been granted access within an agency
General Requirement	• Scenario 2 and 3 occur within the context of Scenario 1 only. For example, the OPR grants access to entries and elements of a healthcare directory within an agency and based on each agency's access policies.
Post-condition	• Only information to which the OPR function indicates authenticated ESI Consumer should have access is returned by the Federal Healthcare Directory Service Provider. • Only information to which the OPR function indicates non-authenticated ESI should have access is returned by the Healthcare Directory user.
Actors	• ESI Consumer • Federal Healthcare Directory Service Provider

Recommendations

That the HcDir Work Group approves:

1) The above findings for establishing Trust Policies for Authentication & Access Control for ESI (Table 1).

2) The above findings for establishing ESI Sharing Classes (Scenario 1, 2, and 3) (Table 2).