National HIE Governance Forum

Trust Framework for Health Information Exchange

Trust Framework for HIE: A framework for governing entities and their participants to share trust attributes to support exchange with a group of unaffiliated entities.

December 2013

This report was prepared under the auspices of the National eHealth Collaborative through its cooperative agreement with the Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services.

Contents

I. National HIE Governance Forum

The National eHealth Collaborative (NeHC) has convened the National HIE Governance Forum at the request of the Office of the National Coordinator for HITs (ONC) through ONC's cooperative agreement with NeHC. The Forum convenes leaders of health information exchange (HIE) governance entities to address governance issues that crosscut various exchange approaches with the goal of cultivating consistency where possible and compatibility when necessary to enable entity to entity exchange. The leaders of these entities, whose decisions establish policies and practices for a given community of exchange partners at the national, state, or regional level, are working to identify common approaches, issues and common challenges in the governance of HIE and ways to address them.

The Forum used ONC's Governance Framework for Trusted Electronic Health Information Exchange to guide their discussions and work. The Governance Framework reflects the principles ONC believes are important when it comes to HIE governance. This Framework is intended to provide a common foundation for all types of governance models. The four categories of principles set forth in the Governance Framework include: Organizational, Trust, Business and Technical Principles. Forum participants initially focused on the Trust Principles. A Steering Committee of the Forum was created to provide strategic oversight and guide the process. Additionally, a Privacy and Security Workgroup was established to develop specific work products for review and approval by the Forum with the intention of bringing value to the privacy and security aspects of HIE governance. Outcomes of the National HIE Governance Forum will be disseminated widely and aspire to help accelerate entity to entity exchange in support of enhanced patient care[1].

II. Introduction – Composition of a Trust Framework

One of ONC's governance goals for nationwide HIE is to increase trust among potential exchange participants to mobilize trusted exchange to support patient health and care.[2] An essential aspect of trust for national HIE is an understanding of what an organization needs to know about another organization in order to exchange data. The National HIE Governance Forum Privacy and Security workgroup has developed this Trust Framework white paper to initiate a discussion of trust requirements between many stakeholders and ultimately lead to the construction of a concrete, real world solution. This is a preliminary step in what will likely be an extended collaborative effort.

Although individual trust communities establish common requirements for their participants, the requirements and methods of verification necessary to be a member of that community are often not the totality of trust requirements that an individual organization follows when making a decision to exchange with unaffiliated organizations. The principle of local autonomy which allows for policy decisions about when to disclose what information, to whom, based on what evidence, is the role and responsibility of local policy makers i.e. Covered Entities and their patients and does not go away when an organization becomes a member of one or more trust communities. Trust communities simplify the process of determining who to exchange with but

[1] The views expressed in Forum work products do not necessarily represent the views of the participants' organizations.

[2] http://www.healthit.gov/providers-professionals/hie-governance

may not be sufficient in and of themselves to enable all forms of appropriate exchange. The unique considerations of every organization and the fact that the individual organization is accountable for the disclosures made by its authorized end users often creates the need to be able to discover additional trust attributes. The approach outlined in this white paper is of potential value to entities within a given trust community as well as entities in different trust communities whom are attempting to both disclose and learn of others' trust attributes as part of their business practices.

The white paper seeks to address the questions:

- What are the critical dimensions of trust that must be discussed and decided upon between parties to exchange?
- How do parties which do not already participate in a common trust community, or parties within a trust community that are subject to additional requirements, such as those imposed by different states, understand and map each other's trust requirements?
- How do parties in different trust communities discover and understand each other's trust attributes and requirements?

A common understanding and framework for the attributes of trust will minimize the need for one-off trust agreements and contracts and permit the extension of existing trust communities to handle more use cases in the future. Ultimately it will allow for interoperable trust profiles that can be automatically communicated among unaffiliated entities to aid in the decision to disclose in the context of who is exchanging what, for what purpose. Trust Attributes, a term used in this white paper to mean those conditions for trusted exchange that can be made discoverable, are becoming more and more familiar across the industry. Trust attributes can be asserted and verified through means including self-attestation, various forms of certification and accreditation, and contractually defined obligations.

This Trust Framework provides a common language to promote transparency into trust policies and practices based on Identity, Policy and Contractual attribute sets and thereby ease inter-entity exchange. When utilizing the concepts proposed by this paper, all trading partners would use a consistent approach to the classification of trust attribute definitions along with consistent representations as to how these trust attributes were verified.

This structured, common set of trust attributes would describe a "Trust Attribute Profile" that could include attributes evidenced by accreditation, certification, attestation or contract.

The Trust Attribute Profiles could be used by governing entities, HIE organizations, vendors, providers and patients or their advocates engaged in HIE to evaluate if a trading partner's profile meets or exceeds the local policy requirements of the user's organization. If fully automated, it would allow for each exchange partner to quickly and efficiently assess any differences in trust elements that might influence what type of information can be exchanged, if any.

The key is to identify those attributes that trusted exchange is dependent upon and allow a comparison of attributes among unaffiliated entities, including where those entities rely in part or in whole on third party service providers for exchange. The long term end goal is to explicitly identify all elements that would indicate whether or not the conditions for trusted exchange exist, so that one entity can sufficiently trust another, according to its local policy preferences, to appropriately share protected health information.

III. Working Definitions

Because the concepts being explored need further maturation, the working definitions below do not purport to be either authoritative of exhaustive. The use of these terms is intended to convey general understanding. Better terms may emerge in the future. Additionally, it is important to note that these terms may be defined differently in other contexts.

1. Access Management: A process control in which entities are granted or denied access to the resources of an organization ensuring that users can access only those resources for which the owner has given them approval. (include Identity, Authentication, Authorization, and other security features)
2. Authentication: The process of establishing confidence in the identity of users or information systems. (Process to gain trust that a claimant is who he/she/it claims to be)
3. Authorization: The processes of granting or denying specific requests for obtaining and using information processing services or data and to enter specific physical facilities.
4. Certificate: An electronic document that uses a digital signature to bind a public key with identity information such as the name of a person or an organization."
5. Certificate Authority: A trusted entity that issues and revokes public key certificates.
6. Chain of Trust: an ordered list of certificates, containing an end-user subscriber certificate and intermediate certificates that enables the receiver to verify that the sender and all intermediates certificates are trustworthy.
7. Identity Proofing: The process of providing sufficient information (e.g., identity history, credentials, documents, etc.) to a service provider for the purpose of proving that a person or object is the same person or object it claims to be.
8. Registration Authority: Act as an intermediary between users and certificate authorities, reviewing and approving certificate requests.
9. Trust Anchor: An authoritative entity for which trust is assumed and not derived.

IV. Trust Framework in Practice

Each participant in the trust framework would make the attributes of their trust requirements discoverable by others. Ideally, each organization would share their requirements in a computable way. Sharing requirements in this way would allow both the sender and receiver of health information to compare the trust attributes important to making a decision to share and for each to determine whether their baseline requirements for exchange are met.

The attributes that are required for specific use cases may vary, but generally several attributes, such as identity-related attributes, are required for all. Once these attributes are discovered in relation to the exchange partner, and the means by which purported trust attribute values associated with that partner can be considered reliable, an organization should be expected to trust any organization that meets or exceeds their local policy requirements. As an organization accepts the asserted values of these attributes reported by the "trust agent", they may reliably trust their assertions.

V. Use Case

One use case illustrates the intent of this paper without regard to the mechanics of how the trust attributes are published and shared. To simplify the discussion, it assumes that each organization is provided knowledge of the trust attributes of each intermediary point between themselves and the endpoint who will be receiving the data. Alternative technical mechanisms likely exist in the computer science domain, but the intent here is to shine a light on the policy considerations so that appropriate technologies may be selected for early piloting of this framework if deemed appropriate by the community.

USE CASE - Current State

HOMEBASE is a provider of medical services and is the medical home for George. FARAWAY is another provider of medical services in another community. George is traveling and finds that he must seek services at the FARAWAY clinic.

- FARAWAY calls and asks the health information management (HIM) department at HOMEBASE for George's summary clinical record.
- The HOMEBASE HIM department asks the requesting physician at FARAWAY questions regarding George to confirm the patient identity and consults the national provider database (or another resource that the relying party trusts) to verify that FARAWAY is a valid provider of services.
- The HOMEBASE HIM department then calls the FARAWAY management services organization (MSO) department to verify that the requesting physician actually works at the FARAWAY clinic and verifies the fax number.
- Having assured that the request is legitimate (established trust), the HOMEBASE HIM department faxes the records requested by FARAWAY.

USE CASE – Future State

To automate this exchange, both HOMEBASE and FARAWAY must have common terms and attribute values that would govern the exchange – a dataset of *exchange trust requirements*.

- FARAWAY sends a data request, and includes (or otherwise makes available) a standardized dataset with FARAWAY's encoded trust attributes (a dataset that is nationally recognized) and is also used by HOMEBASE to determine their ability to respond.
- The HOMEBASE application receiving the request compares the dataset (FARAWAY's trust attributes) to those that it was programmed to accept.
- The HOMEBASE application makes a determination that the dataset is valid, sufficient and appropriate to the request and sends back the records requested.

VI. Trust Axes – A conceptual categorization of Trust Framework components

The Trust Framework for HIE is proposed for use by governing entities (such as Covered Entities, Health Information Organizations (HIOs), and others) and their participants, to facilitate sharing trust attributes in order to evaluate decisions to permit exchange among unaffiliated entities.

The conditions for trusted exchange vary from entity to entity based on differences in local policy and applicable law. Establishing a static one-size fits all set of attributes and the prerequisite values to be met or exceeded by all is challenging. To reduce the burden of this challenge, pattern of like attributes has been identified and these attributes have been grouped into three axes to describe the initial framework. The attributes are based on the extensive experience of National HIE Governance Forum participants and cover most of the common considerations for trusted exchange. As entities gain experience with and test the framework over time, any entity could sufficiently describe a profile of itself (with supporting evidence where the attribute has been verified by a greater rigor then self-attestation) and the actors it is willing to trust based on the attributes in the three axes described below.

Framework "Axes" Identity, Policy, and Contract:

- Identity - attributes used to confirm identity and provide adequate technical level of assurance of that identity and its authorization and authentication.
- Policy - attributes used to determine relevant business practices of the organization which are sufficient to provide assurance of data maintenance and use.
- Contract - attributes used to determine specific obligations and policy statements flowing through bilateral or multiparty agreements. Note that the contract Axis is interrelated with the policy axis – that is, some policy terms may be included as contract terms in some agreements.

These three groupings were found to be useful when conversing with exchange governing entities. The groupings allow for the capture of local policy preferences, common contracted obligations placed on third parties involved in exchange, and some common community practices related to identity emerging in the domain. Although all three of these axes can be related to a policy-intent, it is beneficial to separate the universe of attributes for trusted exchange into these three vectors and present them here for further discussion across the community to discover which attributes are most critical to the automation of appropriate disclosure decisions.

So, why the three axes?

In order to support different use cases involving all types of stakeholders, a complete Trust Framework would likely need to represent many attributes of trust, not just those related to authorization or identity. These additional attributes are frequently focused on the business aspects of how an organization processes and maintains data, which may pass through third party facilitators on its way to an endpoint (frequently codified in contract), and how that endpoint does business (frequently codified in organizational policy).

Although these groupings are somewhat arbitrary, they are helpful when discerning what it will take to facilitate exchange among unaffiliated entities. Attributes listed in each axis represent the kinds of attributes typically evaluated today when making decisions to share information between two entities. They are presented here to illustrate the types of attributes that may be of value in working toward the proposed Trust Framework. To automate the concept, each element of each axis would need to be fully defined.

i. Identity Axis Data Components[3]

- Identity (name)
- Class of identity (individual or real person), pseudo identity, endpoint address, organization, service, <others>?
- Type of identity (hospital, IDN, Provider Org, Provider, HIE, Connector, etc.)
- Proofing Level (how was this identity established and "proofed") – for individuals, NIST has levels of proofing, for orgs, the individual representing the org is proofed, and then the org identity is established through records search. Not sure how apps (services) are proofed, or if that is even relevant, although it maybe should be.
- Certificated? (Y/N)
- Issuing CA – if there is a chain, perhaps the full chain back to the root org needs to be specified
- Accreditation (need to know what these values may be)
- Accrediting Entity
- User Authentication level (NIST)
- Remote user authentication level (NIST)
- User Authorization Type (e.g. RBAC, none, ABAC, ZBAC, etc.)
- Authorization Content
- Contact person information (this is info on a live person who "represents" this identity if the identity is not a real person):
    - Name
    - Address
    - Contact Number
- <Other fields?>
- Endpoint? (Y/N)

For the most part, attributes associated with the framework's Identity Axis are directly related to identity, authentication and authorization. "Accreditation" and "Accrediting Entity" are the only exceptions to this. As an aspect of establishing the Trust Framework, an understanding of what attributes are verified by the accrediting organization is essential. It is anticipated that some accreditations may address attributes that span all of the axes. The Identity Axis allows for a consistent approach to describing components of identity assurance including for example, levels of assurance (LOA) for digital certificates across all levels of the exchange hierarchy.

[3] The authors note that as listed here the "identity axis" conflates four aspects that are clearly understood as different in the security community (identity policy, authentication policy, authorization policy, and identity attributes) but commonly intermingled by business users and others.

ii. Policy Axis Elements

- Does the identity store a copy of the data as it passes through the HIE? (Y/N)
- Policy requirements around management of the provider directory
- Policy requirements around patient disambiguation
- Management of the Master Patient Index
- Requirements for Consent Elements (several)
- Privacy Policies
- Security Policies
- Audit log review policy
- Standards supported
- Profiles supported
- Permitted purposes for request/use
- Several others…

iii. Contract Axis Elements

- Reciprocal obligations such as the obligation to respond.
- Notification in the event of breach
- Explicit flow-down agreements and practices[4]
- Requirements for suspending trade and timely terminations
- Timely update of directories
- Availability of participant agreements for inspection
- Version of the agreement

VII. Application of Framework – Manual

To illustrate how the Trust Framework might work in a manual mode, assume that the framework has been fully fleshed out and established as a national standard with all attributes defined and allowed values delineated, and that participating organizations have agreed to populate their "Trust Attribute Profiles".

Using the HOMEBASE and FARAWAY use case again, imagine that the Clinic at FARAWAY finds out that the patient's records are at HOMEBASE. In place of calling and requesting a fax of records, FARAWAY instead faxes or sends via Direct a copy of its completed Trust Framework to HOMEBASE along with proof of identity of the patient (e.g. the patient's picture ID such as their driver's license). HOMEBASE then reviews FARAWAY's "Trust Attribute Profile[5]" or TAP against its requirements which have been determined through analysis of their policies and their contracts with others in their trust chain. Upon completion of the review of FARAWAY's TAP,

[4] Note: Flow-downs are very important because they can be used during the trust evaluation to determine that information may be shared with lower levels supported through that leg of the hierarchy without doing further evaluation.

[5] For convenience we use the phrase "Trust Attribute Profile" (TAP) to convey the notion of a representation of a set of key-value pairs or some other representation of those attributes necessitated for the transaction being considered.

HOMEBASE determines that FARAWAY meets their minimal trust criteria, and they also identify from the TAP the FARAWAY clinic's Direct address. HOMEBASE then sends a current CCD to FARAWAY's clinic.

It may also be the case that FARAWAY does not meet HOMEBASE's criteria. Perhaps FARAWAY automatically stores a copy of any records it receives from unrelated third parties in its local HIE which is a violation of HOMEBASE's policies. Since HOMEBASE's patients expect that their data would only be stored in their local HIE, HOMEBASE might then send an informing message to their patient at FARAWAY letting them know about this anomaly, and asking if they will approve transfer of their data to FARAWAY so that they may be treated appropriately, and informing the patient that if they approve, they should opt out of any sharing of data by FARAWAY excepting the transmission of a Transition of Care document back to HOMEBASE.

In either case, the facilitation of an electronic exchange of records has occurred between two unrelated parties who previously had no knowledge of each other. In the second case, even though the receiver of the records may not have met all of the criteria of the sender, the patient was provided an opportunity to decide whether to share their information for the improvement of their care, and was also given some instruction by their home provider of how to further protect their data.

A number of variants of this manual example could be imagined, including some form of a registry of trust attribute profiles (perhaps derivative of X.500), or the completed framework could be instantiated a number of other ways. On-going efforts – including the NSTIC project at NIST – will provide a wealth of input to how best to execute a technical solution. The goal of this paper is to initiate the healthcare domain discussion regarding these points to prioritize and prepare for these emerging capabilities.

VIII. Proposed Next Steps

The nation is experiencing a growth in HIE capabilities.   This acceleration is in part a result of the national efforts toward a standards-based approach to interoperability and governance principles that respect and support local autonomy. As health information exchange continues to grow, it is essential to begin the process of establishing a rational approach to inter-HIO exchange that preserves the local autonomy of the participants.

The proposed Trust Framework is a starting point and a call to begin a collaborative process of defining, developing, piloting and ultimately implementing a mechanism by which governing entities and their participants can share trust attributes within and across trust communities in order to support appropriate and trustworthy exchange between otherwise unaffiliated creators and users of health information.

The following next steps are proposed for consideration as part of the nationwide effort to address this ongoing need:

1) Broadly socialize this paper and its concepts with organizations such as state, community and enterprise HIOs and the organizations that enable them (such as HealtheWay, DirectTrust and the National Association for Trusted Exchange (NATE), their vendors, and related accreditation bodies (such as EHNAC and CCHIT) to solicit input, next steps and optimal ways to evaluate alternatives.
2) Perform an inventory of the landscape of existing methods of trust being employed in the environment today and further refine the details of the framework to include common definitions of axes, elements, and their related attributes and metadata.
3) Develop a pre-computable form for use in one or more innovative efforts to refine and prioritize common attributes critical to the vision.
4) Identify and promote efforts underway that are beginning to explore concepts similar to those proposed and support their collaboration where possible.
5) Determine best mechanisms to foster the concept of this whitepaper, in conjunction with similar initiatives such work being led by the ONC, NIST and numerous not-for-profit organizations focused on trusted exchange in healthcare.
6) Develop a Roadmap that is routinely updated by an inclusive committee of industry experts and leaders to champion and steer the initiative from this whitepaper to a nationwide tool set required to realize the full benefits of HIT and HIE at scale.

IX. Additional Resources

Data Use and Reciprocal Support Agreement (DURSA) used by eHealth Exchange participants http://www.healthewayinc.org/images/Content/Documents/Application-Package/2011.03.05-restatement-i-of-the-dursa-final.pdf

Direct Trust Policies http://www.directtrust.org/policies/

Federal Bridge Certificate Authority (FBCA) and Public Key Infrastructure (PKI) Policy Authority (FPKIPA)

FICAM Roadmap and Implementation Guidance

HIPAA Security Rule: 45 CFR 164.308(a)(1), Implementation Specification: Risk Analysis. http://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-sec164-308.pdf

HITSC NwHIN Power Team Final Recommendations for RESTful Exchange Standards (HL7 Fast Healthcare Interoperability Resources (FHIR), OAUTH and OpenID Connect)

HL7's Healthcare Privacy and Security Classification System (HCS) http://wiki.hl7.org/index.php?title=HL7_Security_Document_Library

Identity Ecosystem Steering Group (IDESG) – AHG terminology work https://www.idecosystem.org/wiki/Taxonomy_AHG_Catalog

ISO 22600

Kantara Trust Framework

ONC's Standard and Interoperability Framework Data Segmentation for Privacy (DS4P)

National Strategy for Trusted Identities in Cyberspace

NIST 800 special publication series http://csrc.nist.gov/publications/PubsSPs.html

PCAST HIT Report http://www.whitehouse.gov/administration/eop/ostp/pcast/docsreports

Security Assertion Markup Language (SAML) http://saml.xml.org/

X. National HIE Governance Forum Participants

Arizona Health Care Cost Containment System (AHCCCS)	Lorie Mayer
Care Connectivity Consortium	Jamie Ferguson, MD
Care Connectivity Consortium/Kaiser Permanente	John Mattison, MD*
Care Everywhere Usergroup (EPIC)	Marc Chasin, MD*
Chesapeake Regional System for Our Patients (CRISP)	Scott Afzal
Colorado Governor's Office of Information Technology	Liza Fox-Wylie
Commonwell/Cerner	David McCallie, MD
Commonwell/RelayHealth	Arien Malec
Community Health Information Collaborative	Cheryl Stephens, PhD
Delaware Health Information Network	Mark Jacobs
DirectTrust	David Kibbe, MD*
eHealth Exchange/HealtheWay	Mariann Yeager*
EHR HIE Interoperability Workgroup/New York eHealth Collaborative	David Whitlinger*
Geisinger Health System / Keystone Health Information Exchange	James Younkin
HealthBridge	Keith Hepp
HEALTHeLINK	Dan Porreca
HealthShare Bay Area HIE	Dave Minch
Hudson Valley (NY) Health Information Exchange	John Blair, MD
Indiana Health Information Exchange	Keith Kelly
Inland Northwest Health Services	Tom Fritz
Kansas Department of Health & Environment	Michael McPherson
Maine HealthInfoNet	Devore Culver
Maine HealthInfoNet	Shaun Alfreds
Massachusetts eHealth Institute	Laurance Stuntz
Minnesota Department of Health	Marty LaVenture, PhD
National Association for Trusted Exchange	Aaron Seib
North Carolina Health Information Communications Alliance	Holt Anderson
Quality Health Network	Dick Thompson
Rhode Island Quality Institute	Laura Adams
Rochester RHIO	Ted Kremer
Social Security Administration	Kitt Winter
Southeast Regional Collaborative Health Information Exchange	Tia Tinney
State of Indiana/Family & Social Services Administration	Andrew VanZee
Surescripts	Paul Uhrig*
Utah Health Information Network	Matt Hoffman, MD
VA/DoD Interagency Program Office	Tim Cromwell
VA/DoD Interagency Program Office	Elaine Hunolt
West Virginia Health Information Network	Kathy Moore
*Forum Steering Committee Member	

Forum Privacy and Security Workgroup and Contributors

Care Connectivity Consortium/Kaiser Permanente	John Mattison, MD
Care Everywhere Usergroup (EPIC)	Marc Chasin, MD
Community Health Information Collaborative	Cheryl Stephens, PhD
DirectTrust	David Kibbe, MD
eHealth Exchange/HealtheWay	Eric Heflin
eHealth Exchange/HealtheWay	Mariann Yeager
HealthShare Bay Area HIE	Dave Minch
Independent Healthcare Consultant	Stephen Kelleher
National Association for Trusted Exchange	Aaron Seib
National eHealth Collaborative	Kate Berry
Office of National Coordinator for HIT	Edna Boone
Office of National Coordinator for HIT	Debbie Bucci
Office of National Coordinator for HIT	Mary Jo Deering, PhD
Southeast Regional Collaborative Health Information Exchange	Tia Tinney
Surescripts	Paul Uhrig
VA/DoD Interagency Program Office	Elaine Hunolt
Veterans Administration	Stephanie Griffin