

National HIE Governance Forum

# Identity and Access Management for Health Information Exchange

**The Level of Assurance (LOA) Continuum: A resource for governing entities and their participants to examine identity management and progress along the LOA continuum to support secure exchange with a wider group of entities while reducing risk.**

**December 2013**

## Contents

I.	National HIE Governance Forum .....	2
II.	Forum Report on Identity Management and the Level of Assurance Continuum .....	2
III.	Identity Management Overview.....	3
IV.	Identified Gaps.....	3
V.	Identity Management Definitions.....	3
	a) Identity Proofing.....	3
	b) Electronic Authentication.....	4
VI.	HIPAA Requirements .....	4
VII.	DEA Requirements.....	5
VIII.	National Efforts and Policy Recommendations .....	5
	a) Office of National Coordinator.....	5
	b) NIST.....	6
	c) National Strategy for Trusted Identities in Cyberspace.....	7
	d) Other Identity Management Efforts.....	8
IX.	NIST Electronic Authentication Guideline 800-63-2 .....	8
X.	Level of Assurance (LOA) Continuum .....	11
XI.	LOA in Practice.....	12
XII.	Trust Models: Organizational LOA Considerations.....	16
XIII.	Conclusion.....	18
XIV.	Additional Resources .....	19
XV.	National HIE Governance Forum Participants .....	20

## I. National HIE Governance Forum

The National eHealth Collaborative (NeHC) has convened the [National HIE Governance Forum](#) at the Office of the National Coordinator for HIT's (ONC) request through ONC's cooperative agreement with NeHC. The forum convenes leading health information exchange (HIE) governance entities to address governance issues that cross cut various exchange approaches with the goal of cultivating consistency where possible and compatibility when necessary to enable entity to entity exchange. 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 key issues and common problems in the governance of health information exchange and the best ways to address them.

The forum has utilized the ONC's [Governance Framework for Trusted Electronic Health Information Exchange](#) to guide their discussions and work. The Governance Framework reflects the principles in which ONC believes when it comes to the policy set for HIE governance. This framework is intended to provide a common foundation for all types of governance models. The four key categories of principles discussed in the Governance Framework include: Organizational, Trust, Business and Technical Principles. Forum participants decided to focus on the Trust Principles for their initial discussions and work. A Steering Committee of the Forum was created to provide strategic oversight and guide the overall process. Additionally, a Privacy and Security Workgroup was established to develop specific work products for review and approval by the Forum with the intention to bring value to privacy and security aspects of health information exchange governance. Outcomes of the National HIE Governance Forum will be disseminated widely and are intended to accelerate entity to entity exchange in support of enhanced patient care<sup>1</sup>.

## II. Forum Report on Identity Management and the Level of Assurance Continuum

Through discussions on common aspects and challenges of privacy and security issues, the National HIE Governance Forum participants prioritized provider identity management, specifically identity proofing and electronic authentication, as an important element of trusted exchange needing industry education.

This report is intended to help HIE governing entities, organizations, vendors, and providers engaging in health information exchange understand fundamental identity management issues, practices, and resources; examine Level of Assurance (LOA) aspects of identity management, including evolving efforts from outside of healthcare, along with business and risk ramifications of moving up the LOA continuum and shared experiences for doing so. Our definitions and references to LOA are based on NIST guidance 800-63-2.

As identity management is highly reliant on technology, it is important to note that this field is rapidly evolving as technologies mature and innovations become established in the market. This Forum report is, necessarily, a snapshot of current policies and practice.

---

<sup>1</sup> The views expressed in Forum work products do not necessarily represent the views of the participants' organizations.

### **III. Identity Management Overview**

Strengthening identity proofing and authentication controls increases confidence and assurance in an identity's validity, and provides greater protection from unauthorized access, which creates a strong foundation for trusted exchange. Identity proofing and authentication are the first line of security defense at both the provider and organizational level and have the potential to be the weakest link in the security chain as they are the primary control which opens the 'door' to access management on which many aspects of security rely. All manner of access stems from the application of a user's credentials, if identity proofing and authentication are not implemented effectively, there is a negative downstream effect as exchange organizations and providers make numerous decisions based on identity within several security controls including access, encryption, auditing, and non-repudiation (digital signatures and authentication). As electronic health information exchange between different organizations and providers grows, it is essential to focus on these key building blocks of security and how trust with respect to identity controls can be improved.

This overview will attempt to simplify and address the key elements of identity proofing and authentication for organizations and providers through the eyes of the National Institutes of Standards and Technology (NIST) and the Office of the National Coordinator (ONC) as well as volunteer experts from the private sector. This should assist governing entities and their participants with understanding of the need for and the process of adapting these recommendations to the health care industry.

### **IV. Identified Gaps**

Forum members agreed there is a wide disparity among their participants', end users', and vendors' knowledge of identity proofing and authentication methods, and the impact a choice of method may have on the overall level of assured protection. These disparities create gaps in trust fabrics, potential security and patient-safety risks, and barriers to exchange. They saw a need for a common understanding of identity proofing and authentication policies and methods of implementing such policies to support efforts for exchange among trusted communities to improve patient care and more effective cost management.

### **V. Identity Management Definitions**

#### **a) Identity Proofing**

Identity proofing is the process of collecting and verifying information about a person for the purpose of proving that a person who has requested an account, a credential, or other special privilege is indeed who he or she claims to be, and establishing a reliable relationship

that can be trusted electronically between the individual and said credential for purposes of electronic authentication. This process may include, for example, in-person evaluation of a driver's license, passport, birth certificate, or other government-issued identity, as well as other factors specified in the individual certificate policy of the organization issuing the certificate. Identity proofing is performed before the account is created (e.g., portal, email), the credential is issued (e.g., digital certificate) or the special privilege is granted.<sup>i</sup> Identity proofing is more complex and lengthy the first time an account is created and in most cases need not be repeated in its entirety during subsequent access, depending on the details of the relying party policy and the sensitivity and criticality of actions performed using the account.

## **b) Electronic Authentication**

Electronic authentication (e-authentication) is the process of establishing confidence in user identities electronically presented to an information system.<sup>ii</sup> It is the process of establishing confidence that an individual/organization using a credential that is known to the system (e.g., login name, digital certificate) is indeed the person/organization to whom the credential was issued. There are three types of authentication factors: something you know (e.g., password, PIN), something you have (e.g., smartcard, hard token, mobile phone), something you are (e.g., biometric characteristic such as a fingerprint or voice pattern). Authentication is performed each time a user logs into an account (e.g., portal, email) or otherwise uses a credential.<sup>iii</sup> Multi-factor authentication, which requires more than one type of authentication to be used at the point of system login is sometimes used to achieve a higher level of assurance.

## **VI. HIPAA Requirements**

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that an individual or entity accessing electronic personal health information (PHI) be authenticated before such access is granted. Although the Rule does not mandate a specific framework or specify how to implement the standard, it does require that each covered entity “conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate” and to then to “implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.”<sup>iv</sup> The Security Rule cites several NIST publications as potentially valuable resources for users with specific questions and concerns about IT security and practices. The Security Rule risk analysis is to serve as the basis for deciding how to implement the technical measures that HIPAA requires:

- 1) Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed,<sup>v</sup>
- 2) Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network,<sup>vi</sup> and

- 3) Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the Privacy Rule.<sup>vii</sup>

## VII. DEA Requirements

The Drug Enforcement Administration (DEA) requires that clinicians engaged in e-prescribing of controlled substances must adhere to strict requirements including undergoing identity proofing. Once the identity-proofing process is complete, the clinician will be issued a two-factor authentication credential provided by an organization approved by the General Services Administration Office of Technology Strategy/Division of Identity Management.<sup>2</sup>

In addition, clinicians are permitted the option to use a private cryptographic key. A digital certificate associated with the key must be obtained from a certification authority that is cross-certified with the Federal Bridge Certification Authority (FBCA). The private key associated with the digital certificate must be stored on a hard token. This hard token containing the cryptographic key would be one of the two required authentication credentials. The clinician has the responsibility to safeguard his or her authentication credentials, and may not share them with any other individual.

Clinicians are required to electronically sign and authorize transmission of the e-prescription by applying their two-factor authentication protocol. The act of applying two-factor authentication constitutes the legal electronic signature on the prescription. Hence, it is critical for clinicians to safeguard their two-factor credentials to prevent forgeries. The DEA implemented a two-factor authentication requirement to reduce the risk of diversion of controlled substances.<sup>viii</sup>

## VIII. National Efforts and Policy Recommendations

There are several commonly referenced Levels of Assurance (LOA) guidelines (NIST, Kantara OASIS and ISO) which are used to inform security risk mitigation in healthcare. Although designed for different frameworks, all leverage the NIST assurance levels.

### a) Office of National Coordinator

#### **HIT Policy Committee Privacy and Security Tiger Team Recommendations for Identity Management for Providers:**

In September 2012, the Tiger Team of the HIT Policy Committee focused on trusted identity and identity proofing for the issuance of credentials to be used for authenticating the identity of provider users in the context of electronic health information exchange and provided the following recommendations:<sup>ix</sup>

1. By Meaningful Use Stage 3, ONC should move toward requiring multi-factor authentication (meeting NIST Level of Assurance (LOA) 3) by provider users to remotely access protected health information. Remote access includes the following scenarios:

- A. Access from outside of an entity's private network.
  - B. Access from an IP address not recognized as part of the organization/entity or that is outside of the entity's compliance environment.
  - C. Access across a network any part of which is or could be unsecure (such as across the open Internet or using an unsecure wireless connection).
2. Organizations/entities, as part of their HIPAA security risk analysis, should identify any other access environments that may require multiple factors to authenticate an asserted identity.
  3. Organizations/entities should continue to identify proof provider users in compliance with HIPAA. (The Tiger Team did not see a need to establish identity proofing requirements for different types of access scenarios).
  4. Such policies should extend to all clinical (provider) users accessing/exchanging data remotely.
  5. Technology options for authentication continue to evolve; ONC should continue to monitor and update policies as appropriate to reflect improved technological capabilities.
  6. ONC's work to implement this recommendation should continue to be informed by National Strategy for Trusted Identities in Cyberspace (NSTIC) and aim to establish trust within the health care system, taking into account provider workflow needs and the impact of approaches to trusted identity proofing and authentication on health care and on health care quality and safety.

## b) NIST

### NIST 800-63-2<sup>x</sup>

The [National Institute of Standards and Technology's \(NIST\) Electronic Authentication Guideline SP 800-63-2](#) recommends technical guidelines for implementing electronic authentication consistent with the four levels of assurance (LOA) defined by the Office of Management and Budget.<sup>xi</sup> Changes from version 1 are not major, though it does specifically recognize healthcare organizations as one of the regulated entities that issue credentials to "professions", e.g. "providers" as long as the institution accepts the "Conditions of Participation in Medicare" and rigorously follows the Medicare credentialing policy. For each LOA, the NIST guidance describes a coordinated set of identity-proofing and authentication methods that, when used together, can provide specific levels of confidence that the entities involved in electronic transactions are who they claim to be. Each assurance level describes the degree of certainty that the user has presented a valid identifier (a credential) that refers to his or her identity. NIST 800-63-2 outlines four levels of assurance in the areas of identity proofing, registration, tokens, management processes, authentication protocols and related assertions which have been cited by the HIT Policy Committee & HIT Standards Committee for adoption in health information exchange.

Assurance is defined as (1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and (2) the

degree of confidence that the individual using the credential is the individual to whom the credential was issued. Assurance answers the question, "How sure am I that you are who you say you are?" LOAs are determined through the use of varying technologies, processes, and policies associated with credentials, tokens, and authentication procedures.

Again it is important to note that advances in biometrics, GPS, social media, metadata and smartphones have the potential to both alter and revolutionize this space. One example is the ubiquity and technical sophistication of smartphones carried by providers which are changing token definitions and functionality. Today these phones represent "soft tokens", but with special modifications to the subscriber identity module (SIM) card and/or biometric scanners they could easily fit the FIPS 140-2 or higher cryptographic definition. Through its position within the U.S. Department of Commerce, NIST closely monitors these developments and will periodically update its guidance.

### **c) National Strategy for Trusted Identities in Cyberspace<sup>xii</sup>**

The National Strategy for Trusted Identities in Cyberspace (NSTIC) is a White House initiative to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the privacy, security, and convenience of sensitive online transactions. In President Obama's introduction of NSTIC, the president called for a "strategy to make online transactions more secure for businesses and consumers alike ..." and "...foster growth and innovation online and across our economy ..."<sup>xiii</sup> NSTIC has laid out a vision of an ecosystem in which individuals and organization utilize secure, efficient, easy-to-use and interoperable solutions that promote confidence, choice, privacy and innovation.

Governance is a key component of the NSTIC vision. At its core, is the establishment of an online environment that fosters trust through commonly agreed upon standards and processes developed over time by different online communities and sectors, including healthcare. This creates an identity ecosystem that provides a common identity framework, administrative steering group, sector/community based trust frameworks that adhere to a common baseline, accreditation authority and Trustmark scheme.

NSTIC<sup>xiv</sup> cites the following guiding principles with respect to authentication:

- Identity solutions will be secure and resilient via:
  - Trusted third-party provider integration
  - Identity risk assessed via minimal personally identifiable information (PII) submission
- Identity solutions will be interoperable via:
  - Flexible integration options across multiple platforms and processes
  - Unique and tailored process flow and decision making capabilities
- Identity solutions will be privacy enhancing and voluntary for the public via:
  - Level of authentication treatments based on and commensurate with the level of the subject's desired access
- Identity solutions will be cost-effective and easy to use via:



- Behind-the-scenes authentication supported by subject-facing questions
- Multilayered services that translate to multilayered cost structures

#### d) Other Identity Management Efforts

Other national and international identity management efforts may inform health care identity management practices. The banking industry and intelligence and commerce entities have been guiding practices with respect to authentication for several decades. Key organizations which are informing health care identity management are listed below. As the availability and exchange of electronic health and health care data continues to grow, it is expected that the health care industry will assume a more active role in the development of identity management solutions and practices. Key organizations which are informing health care identity management include:

- [Kantara Initiative](#) activities focus on requirements gathering for the development and operation of Trust Frameworks as well as verification of actors within Trust Framework ecosystems. The Kantara Initiative accredits assessors, approves credential service providers services and recognizes service components (Identity Proofing and Credential Management).<sup>xv</sup> Kantara has also authored the Identity Assurance Framework which several organizations have adopted.
- [International levels of assurance \(ISO 29115\)](#) - provides a framework for managing entity authentication assurance in a given context. It specifies four levels of entity authentication assurance, criteria and guidelines for achieving each of the four levels of entity authentication assurance, guidance for mapping other authentication assurance schemes to the four LOAs, guidance for exchanging the results of authentication that are based on the four LOAs, and guidance concerning controls that should be used to mitigate authentication threats.
- [OASIS \(Organization for the Advancement of Structured Information Standards\)](#) is currently analyzing survey methods used to authenticate identities in which these methods of trust elevation are systematically evaluated for vulnerabilities. This analysis is intended to inform ways of combining methods to further elevate trust to achieve desired levels of assurance.

## IX. NIST Electronic Authentication Guideline 800-63-2

The NIST Electronic Authentication Guideline 800-63-2 provides technical guidelines for implementing identity proofing, electronic authentication, cryptographic capabilities, and defines requirements for four levels of assurance. LOAs are part of a set of security policies that increase the security of data primarily directed at preventing those outside the “system” from breaking in. The table below outlines some of its key requirements for identity proofing, token usage, and authentication protocols.

**TABLE 1- Overview NIST Electronic Authentication Guidelines 800-63-2**


	LOA1	LOA2	LOA3	LOA4
Identity Proofing				
Claim of Identity	Must be a unique identification (not already in records)	In-person or remote presentation of credentials (presentation)	In-person or remote presentation of credentials (verification)	In-person presentation only
Proof Artifacts	No requirement. The claim itself is relied on without proof	Current government-issued picture ID w/ nationality, address, DOB. If remote, a bank account, credit card, and/or taxID	Same as LOA2 but includes 2 forms of ID, and if remote, a utility bill with address	Same as LOA2 but requires 2 forms of picture ID (e.g. license and passport), and may also require a financial account
Verification	Unique ID in records	If in person, verify picture, call or send to phone or address of record. If remote, also use verification of accounts. Crowd-source proofing	Same as LOA2 but also requires a means of proof (nonrepudiation) which can be a recorded voice print or response from primary address	Same as LOA2, visual check on both picture IDs. Verification of account holder and address through database or government record checks
Verification Example	Setting up a personal email account ➤ Hotmail, Gmail	Possessing valid government issued picture ID or financial account number Driver's license, bank account number	Possess valid government issued picture ID (or financial account number) <u>plus</u> verification of such ID	Possess valid government issued picture ID (or financial account number) <u>plus</u> verification of such ID <u>plus</u> second ID and verification of second ID

	LOA1	LOA2	LOA3	LOA4
<b>Authentication</b>				
Factors Required	Single	Single	Two	Two or more
Factors Allowed	Hard or Soft token Password One-time Password Device Strong Password PIN Bio-metric Out-of-Band secret delivery	Hard or Soft token Password One-time Password Device Strong Password Bio-metric Out-of-Band secret delivery	Hard or Soft token Strong Password One-time Password Device Bio-metric Out-of-Band secret delivery	Hard token only
Token Requirements	Must prove control of token	Must prove control of token	Must prove possession of a key by either: a) Using a password or biometric to activate a cryptographic key that is then used in a secure authentication protocol, or b) Manually entering a cryptographically generated one-time code plus a password	Proof of possession of a private key thru a crypto protocol – such as user authenticated TLS or Holder of key assertions
Threat Resistance	Prevention of: On-line guessing Replay	Prevention of: LOA1 threat + Eavesdropper Session hijacking	Prevention of: LOA2 threat + Verifier impersonation Direct Man-in-the-middle attacks	Prevention of: LOA3 threat + Man-in-the-middle attacks
Cryptographic Capabilities				
Requirement	None (however, passwords may not be sent “in the clear”)	Approved cryptographic module required	FIPS validated cryptographic module required for all operations	FIPS 140-2 or higher cryptographic strength with at least FIPS 140-2 Level 3 physical security

## X. Level of Assurance (LOA) Continuum

The LOA continuum table depicts the benefits of moving to higher LOA levels to mitigate risk. Forum participants noted that, consistent with the HIPAA Security Rule, each organization should use the results from their periodic risk assessments to measure security and privacy risks to HIE operations and health information in order to determine the LOA necessary for various use cases and high risk security points.

**TABLE 2 – LOA Continuum Benefits**

Moving through Level of Assurance (LOA) continuum strengthens incrementally the security of health information exchange and permits access to more sensitive data at both the federal and private level.				
				
	LOA1	LOA2	LOA3	LOA4
Confidence <sup>xvi</sup>	Little or no assurance in the asserted identity's validity	Some confidence in the asserted identity's validity	High confidence in the asserted identity's validity	Very high confidence in asserted identity's validity
Federal Agency Exchange			Required for Organizational and Individual participants*	
Direct			Required for Direct Trust HISPs submitting trust anchors to Direct Trust Anchor <sup>xvii</sup> Bundle & organizational & address level end-entity Direct certificates.	
HealtheWay			Required for HealtheWay participants to be issued eHealth Exchange digital certificates (Organizational)	
MU		Required for MU2 for providers remote access	Proposed for MU3 for providers remote access	
eRX		Required for e-RX	Required for e-RX of controlled substances <sup>xviii</sup>	
Risk Mediation Cyber Insurance			Potential reduction in premiums**	Potential reduction in premiums**

\*The Federal Information Security Management Act (FISMA) 800-53 requires federal agencies to perform a risk assessment to determine LOA. For bi-directional information exchange between agencies, it is required that each agency ensure the other has same level of protections in place. Example: If “high” information system is exchanging data with a “moderate” information system, the moderate information system would be required to put extra controls in place. For one directional data flow, an agency may allow this without implementation of additional safeguards since data is only flowing one way. Example: Data flow from moderate information system to high information system. It is encouraged that systems exchanging information both meet the requirements for the same LOA for data protection during exchange and at rest.

\*\*Michigan Health Information Network Shared Services (MiHIN) has noted that organizations may be able to lower their cyber liability insurance rates by minimizing their exposure to certain data security issues and adopting higher levels of security measures such as compliance with NIST LOA3.<sup>xix</sup>

## XI. LOA in Practice

LOA is determined by a number of factors: the detail to which the identity proofing is performed, the strength of the token used to authenticate, and the protection and management of the token. A key understanding is that any given LOA results from the use of the complete set of methods defined for that LOA. Selecting an appropriate LOA is not a matter of picking and choosing elements from more than one level; if any single element included a LOA set is omitted or weakened, that level of assurance cannot be achieved. Forum participant organizations are implementing identity management methods in a variety of ways. For any given HIE transaction several LOA levels and activities may come into play such as network to network authentication, individual to network authentication, issuance of identity credentials, authentication of trusted agents in a chain of trust, and also to the individual user or her organizational network. Understanding the nuances of obtaining and maintaining a given LOA level can be difficult.

### Sample Use Case:

A hospital may perform in person identity proofing (included in the LOA 4 set of protections) as the basis for issuing a username for an account. The hospital then asks the individual to select a strong password, which is used to authenticate the user when he/she logs in. Although the identity-proofing method is part of the LOA 4 definition, because the hospital uses single-factor authentication (password), the overall LOA can be no higher than LOA 2. However, if the hospital utilizes a knowledge-based authenticator (KBA) or a cell phone is added as an action required for authentication, the overall assurance level becomes LOA 3. If the hospital uses a smartcard or biometric as a second authenticator they may achieve LOA 4. It is important to note that NIST 800-63-2 has purposefully excluded the use of biometrics as biometric technology matures. That being said, it is important to a rapidly emerging practice that has become standard in many industries.

## Specifying LoA



Desired Overall LoA	Credential Issuance and Management	Identity Proofing	End User Authentication	Credential Management
			Credential Management	
<b>2</b>	2, 3, or 4	2, 3, or 4	2, 3, or 4	2, 3, or 4
<b>3</b>	3 or 4	3 or 4	3 or 4	3 or 4
<b>4</b>	4	4	4	4

## Determining LoA



Credential Issuance and Management	Identity Proofing	End User Authentication	Credential Management	Overall Level of Assurance
		Overall Level of Assurance		
LoA 3	LoA 3	LoA 2	LoA 3	<b>2</b>
LoA 3	LoA 2	LoA 3	LoA 3	<b>2</b>
LoA 3	LoA 4	LoA 3	LoA 3	<b>3</b>
LoA 4	LoA 4	LoA 1	LoA 4	<b>1</b>

## Forum participant practices for consideration at your organization:

The list below provides examples of how forum participants strengthen the LOA practices of their participants. This list should not be construed as a list of recommendations and does not express the views of all forum participant organizations. We recommend reviewing these items with your privacy and security officer(s) as well as legal counsel and operational teams in order to determine if appropriate for your organization and/or exchange model.

- 1) Require participants to show evidence of performing a risk assessment and prescribing to the minimum LOA sufficient to counter the identified risks.
- 2) Adopt the Office of Management and Budget's (OMB) 5-step process for reviewing and setting LOA requirements.
  1. Conduct a risk assessment of their systems
  2. Map identified risks to the appropriate assurance level
  3. Select technology based on e-authentication technical guidance
  4. Validate that the implemented system has met the required assurance level
  5. Periodically reassess
- 3) Require participants to follow recommended operational practices for Identity Proofing and Authentication and provide Checklists and Education in order for participants to do so. Sample education and training modules include: Risk management, Identity management, Security control testing, Threat management, etc.
- 4) Require "flow down" of identity proofing and authentication obligations to participants in participation, legal and/or user agreements.
- 5) Include LOA requirements for specific use cases within your HIE/HISP security policies. For example, require at least LOA3 for all query based access to information in the exchange.
- 6) Require participants utilizing single sign-on and/or single portal access (with multiple application access) to strengthen the initial authentication method to require at least two factors, since all subsequent assertions are dependent upon it.
- 7) Ensure participation agreements/contracts include a termination notification clause which requires participants to notify the HIO or HISP, within a very short timeframe, when a registered user in their system is discontinued (terminated, quits, exhibits inappropriate/dangerous behavior, etc.).
- 8) Ensure participation agreements/contracts include a process for periodically reconciling designated HIO/HISP participant/user list.
- 9) Include the establishment of processes to alert participants of the expiration date of any given security credentials so that participants understand when they expire, and the steps to take to renew with ample notice to not allow a gap in security. (Certificate Authority)

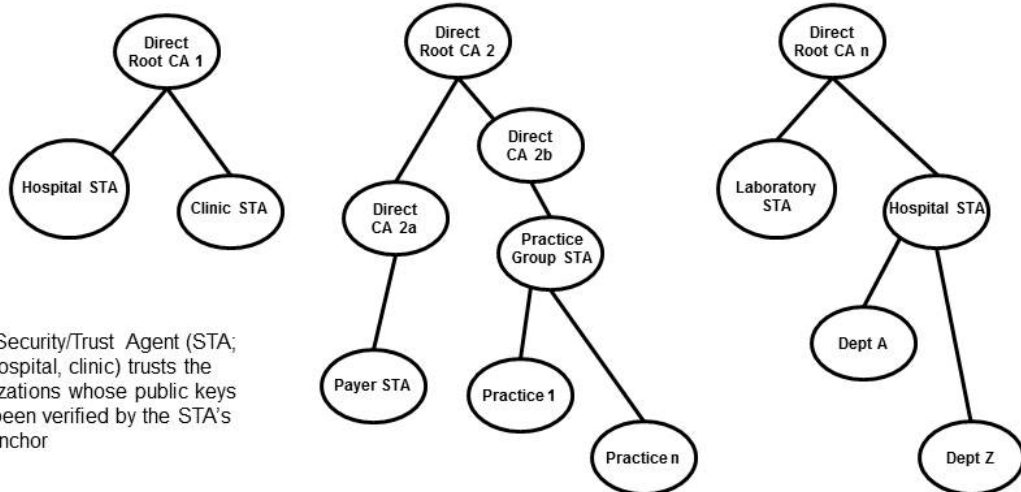
- 10) Include the establishment of processes to maintain an active certificate list used to authenticate servers. (HIOs and Providers).
- 11) Require physical meeting at the member site for signing of the Participation agreement. When a physical meeting is not possible an alternative is to require the use of a notary service.
- 12) Require verification of corporations by checking the state's corporate filings database to verify that their corporate filings are valid and up-to-date.
- 13) Create an organizational risk assessment program and offer to participants.
- 14) Clearly state your Identity Proofing and Authentication policies when soliciting cyber insurance.



## XII. Trust Models: Organizational LOA Considerations

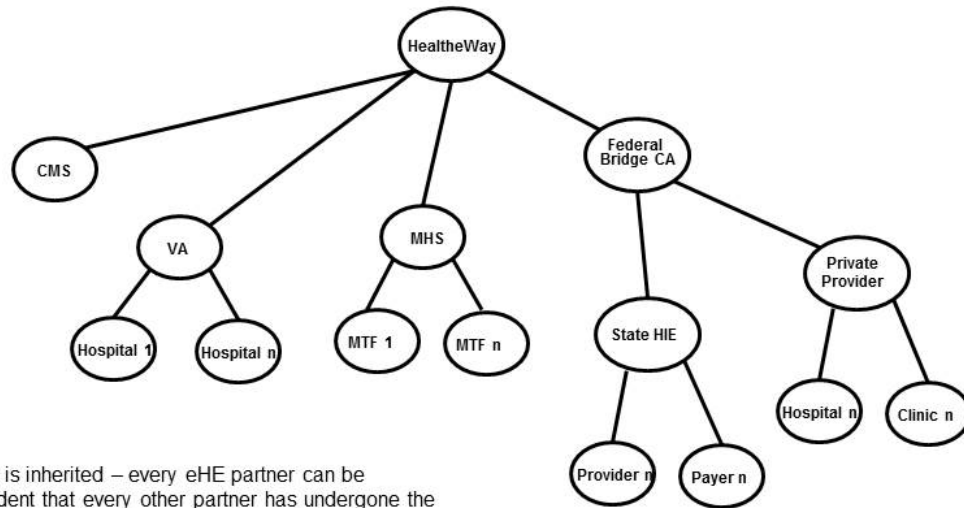
The models below indicate key exchange points between entities for organizations to review and consider when setting the strength of their LOA requirements for health information exchange.

### Multi-Root Trust Model – Direct



The Direct protocol uses a multi-root (PKI) certificate authority model. Direct addresses utilize certificates which are assigned to entities such as departments, clinics, or practices. Each organization is responsible for verifying the trustworthiness of the public keys used. This is quite similar to how secure email works in practice: an organization maintains a list of trusted public keys and distributes that list to its employees, and each employee can then add individual public keys that he/she trusts.

## Hierarchical Trust Model – eHealth Exchange (eHE)



Trust is inherited – every eHE partner can be confident that every other partner has undergone the same LOA of identity-proofing before being issued a digital certificate recognized by eHE

The eHealth Exchange (eHE) uses a traditional, hierarchical public key infrastructure (PKI), where trust is inherited from the “root” or trusted certificate authority (CA) – which for eHE is the Federal Bridge Certificate Authority (FBCA).

## Cloud-based Trust Model



Service in cloud authenticates users, passes verification of authentication to EHR and translates between different protocols (open ID, PKI, SAML, etc.). Patients and providers can re-use credentials across multiple Health IT services.

### XIII. Conclusion

The forum privacy and security workgroup hopes you find this resource valuable and encourage you to share it with your exchange partners and participants. Our goal was to develop a tool to assist in bringing us all to a similar level of basic understanding of LOA. Additionally, the tools can be used to ascertain what LOA is required for the type of exchange you are involved in and when you need to move up the scale.

We note again the importance to which LOA can strengthen trusted national exchange and of the technological advances which have the potential to revolutionize identity management in healthcare. We encourage forum participants to monitor new solutions and engage with organizations cited in order to be informed on new developments and their potential use in health care.

Thank you to all who contributed to this work. Through their expertise and willingness to share, we all benefit.

## XIV. Additional Resources

- a. Direct Trust Digital Certificate Policy [www.directtrust.org/digital-certificate-policy](http://www.directtrust.org/digital-certificate-policy)
- b. Federal Financial Institutions Examination Council Authentication in an Internet Banking Environment [http://www.ffeic.gov/pdf/authentication\\_guidance.pdf](http://www.ffeic.gov/pdf/authentication_guidance.pdf)
- c. HIPAA Administrative Simplification:  
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf>
- d. ID Management.GOV <http://www.idmanagement.gov/identity-credential-access-management> Glossary <http://www.idmanagement.gov/glossary>
- e. Kantara Initiative: Identity Assurance Framework  
<http://kantarainitiative.org/confluence/display/GI/Identity+Assurance+Framework>
- f. National Institute of Standards and Technology (NIST):
  - i. Federal Information Processing Standards  
<http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>
  - ii. Special Publication Assurance Level  
Guidance <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>
  - iii. An Introduction to Computer Security - The NIST Handbook  
<http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter16.html#107>
  - iv. Recommended Security Controls for Federal Information Systems and Organizations, security control family: Identification and Authentication (IA)  
[http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final\\_updated-errata\\_05-01-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf)
  - v. Security Architecture Design Process for Health Information Exchanges (HIEs)  
<http://csrc.nist.gov/publications/nistir/ir7497/nistir-7497.pdf>
  - vi. SP 800-30, Risk Management Guide for Information Technology Systems  
[http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final\\_updated-errata\\_05-01-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf)
  - vii. Managing Risk form Information Systems: An Organizational Perspective  
<http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>
- g. Office of National Coordinator
  - i. Direct: Implementation Guidelines to Assure Security and Interoperability  
May, 2013:  
[http://www.healthit.gov/sites/default/files/direct\\_implementation\\_guidelines\\_to\\_assure\\_security\\_and\\_interoperability.pdf](http://www.healthit.gov/sites/default/files/direct_implementation_guidelines_to_assure_security_and_interoperability.pdf)
  - ii. Health Information Technology Policy Committee, Privacy and Security Tiger Team, Trusted Identity of Providers in Cyberspace:  
[http://www.healthit.gov/sites/default/files/transmittal\\_092512\\_pstt\\_recommendations\\_provider\\_authentication.pdf](http://www.healthit.gov/sites/default/files/transmittal_092512_pstt_recommendations_provider_authentication.pdf)
  - iii. Guide to Privacy and Security of Health Information (June, 2012):  
<http://healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf>

## XV. National HIE Governance Forum Participants

Affiliation	Participant
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 Kelley
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

\*Steering Committee Member

## Forum Privacy and Security Workgroup and Contributors

Affiliation	Contributor
Care Connectivity Consortium/Kaiser Permanente	John Mattison, MD
Care Everywhere Usergroup (EPIC)	Marc Chasin, MD
Center for Democracy and Technology	Deven McGraw
Community Health Information Collaborative	Cheryl Stephens, PhD
DirectTrust	David Kibbe, MD
Dr First	Thomas Sullivan, MD
eHealth Exchange/HealtheWay	Eric Heflin
eHealth Exchange/HealtheWay	Mariann Yeager
HEALTHeLINK	Drew McNichol
HealthShare Bay Area HIE	Dave Minch
Independent Healthcare Consultant	Stephen Kelleher
Martin, Blanck and Associates	Dixie Baker, PhD
Michigan Health Information Network Shared Services	Helen Hill
National Association for Trusted Exchange	Aaron Seib
National eHealth Collaborative	Kate Berry
National eHealth Collaborative	Matthew Hager
National Institute of Standards and Technology	William Burr
Office of National Coordinator for HIT	Edna Boone
Office of National Coordinator for HIT	Wahida Bhuyan
Office of National Coordinator for HIT	Debbie Bucci
Office of National Coordinator for HIT	MaryJo Deering, PhD
Southeast Regional Collaborative Health Information Exchange	Tia Tinney
Surescripts	Paul Uhrig
VA/DoD Interagency Program Office	Elaine Hunolt

<sup>i</sup> <http://www.healthit.gov/sites/default/files/2012dec19-pswg-hearing.pdf>

<sup>ii</sup> <http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf>

<sup>iii</sup> <http://www.healthit.gov/sites/default/files/2012dec19-pswg-hearing.pdf>

<sup>iv</sup> 45 CFR §164.308(a)(1)(ii)(A) and (B) Implementation specifications.

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf>

<sup>v</sup> 45 CFR §164.312(d) Standard: Person or entity authentication

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf>

<sup>vi</sup> 45 CFR §164.312(e)(1) Standard: Transmission security (2013).

<sup>vii</sup> 45 CFR §164.308(4)(i) Standard: Information access management (2013).

<sup>viii</sup> U.S. Department of Justice, Drug Enforcement Administration. Electronic prescriptions for controlled substances. Interim final rule. *Fed Reg.* Volume 75, number 61. March 31, 2010; 16236 – 16319.

[www.deadiversion.usdoj.gov/fed\\_regs/rules/2010/fr0331.pdf](http://www.deadiversion.usdoj.gov/fed_regs/rules/2010/fr0331.pdf). Accessed December 12, 2012.

<sup>ix</sup> [http://www.healthit.gov/sites/default/files/transmittal\\_092512\\_pstt\\_recommendations\\_provider\\_authentication.pdf](http://www.healthit.gov/sites/default/files/transmittal_092512_pstt_recommendations_provider_authentication.pdf)

<sup>x</sup> <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>

---

<sup>xi</sup> Office of Management and Budget Memorandum M-04-04. E-Authentication Guidance for Federal Agencies. December 16, 2003.

<sup>xii</sup> [http://www.dhs.gov/xlibrary/assets/ns\\_tic.pdf](http://www.dhs.gov/xlibrary/assets/ns_tic.pdf)

<sup>xiii</sup> <http://www.whitehouse.gov/the-press-office/2011/04/15/administration-releases-strategy-protect-online-consumers-and-support-in>

<sup>xiv</sup> [http://www.dhs.gov/xlibrary/assets/ns\\_tic.pdf](http://www.dhs.gov/xlibrary/assets/ns_tic.pdf)

<sup>xv</sup> <http://kantarainitiative.org/about/>

<sup>xvi</sup> [http://csrc.nist.gov/publications/drafts/800-63-2/sp800\\_63\\_2\\_draft.pdf](http://csrc.nist.gov/publications/drafts/800-63-2/sp800_63_2_draft.pdf)

<sup>xvii</sup> Trust Anchor and Bundles defined @ <http://wiki.directproject.org/Direct+Project+Security+Overview>

<sup>xviii</sup> DEA's Interim Final Rule of Electronic Prescribing of Controlled Substances (Federal Register: *Electronic Prescriptions for Controlled Substances; Final Rule 21CFR Parts 1300, 1304, 1306, and 1311*. 2010 Mar 31 75(61):16236-16319) , and 2) the DEA's clarification of the requirement that the third party audit address the both "processing integrity" and "physical security." (Federal Register: *Electronic Prescriptions for Controlled Substance Clarifications; 21CFR Parts 1300, 1304, 1306, and 1311*. 2011 Oct 19 76(202):64813-64816)

<sup>xix</sup> <http://mihin.org/security-and-privacy/>