National eHealth Collaborative

National HIE Governance Forum

Final Report
For the Office of the National Coordinator for Health Information Technology

December 2013

Staff

- National eHealth Collaborative (NeHC)
  - Kate Berry
  - Matthew Hager
- Office of the National Coordinator for Health Information Technology (ONC)
  - Edna Boone (contractor)
  - MaryJo Deering
  - Kory Mertz
  - Chris Muir

Contents

- Background and Goals
- Forum Participants
- Process
- Work Products
- HIE Governance Landscape
- Value of Work
- Areas in Need of Further Collaborative Effort
- Work Product Details
- Appendix

Background and Goals

Overarching Goal of Health Information Exchange

The goal of health information exchange is for information to follow a patient where and when it is needed, across organizational, vendor, and geographic boundaries.

ONC's Health Information Exchange Governance Goals

- Increase interoperability
- Increase trust among all participants to mobilize trusted exchange to support patient health and care
- Decrease the cost and complexity of exchange

The National HIE Governance Forum is a Key Component of ONC's Non-regulatory Approach to HIE

- Cooperative Agreements
- Framework of Principles
- **HIE Governance Forum**
- Monitor Exchange Progress

ONC's Definition of HIE Governance

HIE governance refers to the establishment and oversight of a common set of behaviors, policies, and standards that enable trusted electronic health information exchange among a set of participants.

National HIE Governance Forum Focus

Health information exchange at a national level, understanding commonalities in approaches, identifying ongoing challenges, and working collaboratively to address challenges to exchange between different exchange organizations and across state boundaries.

National HIE Governance Forum Participants

National HIE Governance Forum Participants

- 35 participants from national, state and regional exchange entities including CMS, SSA, VA
- Steering committee:
  - Marc Chasin, MD - Care Everywhere Usergroup (EPIC)
  - David Kibbe, MD - DirectTrust
  - John Mattison, MD - Care Connectivity Consortium/Kaiser Permanente
  - Paul Uhrig, JD - Surescripts
  - David Whitlinger - EHR | HIE Interoperability Workgroup/New York eHealth Collaborative
  - Mariann Yeager - eHealth Exchange/HealtheWay

National HIE Governance Forum Participants

- Arizona Health Care Cost Containment System
- Care Connectivity Consortium *
- Care Everywhere/Epic *
- Chesapeake Regional System for Our Patients
- CMS
- Colorado's Governors Office of IT
- Commonwell/Cerner
- Commonwell/RelayHealth
- Community Health Information Collaborative
- Delaware Health Information Network
- DirectTrust *
- eHealth Exchange/HealtheWay *
- EHR/HIE Interoperability Work Group/New York eHealth Collaborative *
- Geisinger Health System/KeyHIE
- HealthBridge
- HealtheLINK
- HealthShare Bay Area HIE
- Hudson Valley NY HIE
- Indiana HIE
- Inland Northwest Health Services
- Kansas Department of Health and Environment
- Maine HealthInfoNet
- MA eHealth Institute
- MN Department of Health
- National Association for Trusted Exchange
- NC Health Information and Communications Alliance
- Quality Health Network
- Rhode Island Quality Institute
- Rochester RHIO
- Social Security Administration
- Southeast Regional Collaborative for HIE
- State of Indiana Family and Social Services
- Surescripts *
- Utah Health Information Network
- VA/DoD Interagency Program Office
- WV Health Information Network

Note: * indicates steering committee member

National HIE Governance Forum Privacy and Security Work Group

- Cheryl Stephens, Community Health Information Collaborative, Work Group Chair
- Mariann Yeager, eHealth Exchange/HealtheWay
- Steve Allen, HealtheLINK
- Dave Minch, HealthShare Bay Area HIE
- Aaron Seib, NATE
- Tia Tinney, SERCH
- Stephania Griffin, Veterans Health Administration

National HIE Governance Forum
HIE Accreditation and Certification Work Group

- Michael McPherson, Kansas, Co-Chair
- Andy Vanzee, Indiana, Co-Chair
- Alisa Ray, CCHIT
- Cheryl Stephens, CHIC
- David Kibbe, DirectTrust
- Eric Heflin, eHealth Exchange/HealtheWay
- Mariann Yeager, eHealth Exchange/HealtheWay
- Lee Barrett, EHNAC
- Aaron Seib, NATE
- Tia Tinney, SERCH
- Paul Calatayud, Surescripts

Benefits and Goals for Forum Participants

✓Listening

Provide a neutral non-competitive collaborative environment to interact with other HIE leaders

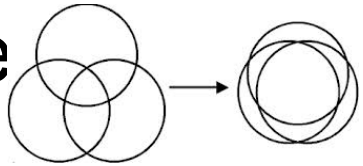
✓Learning

Share lessons learned and gain common understanding of key governance components, what is working and not working

✓Networking

Introduction and interaction with other HIE leaders

✓Convergence



Work toward greater consensus on trust framework, common scalable elements of trust, select business principles

National HIE Governance Forum Process

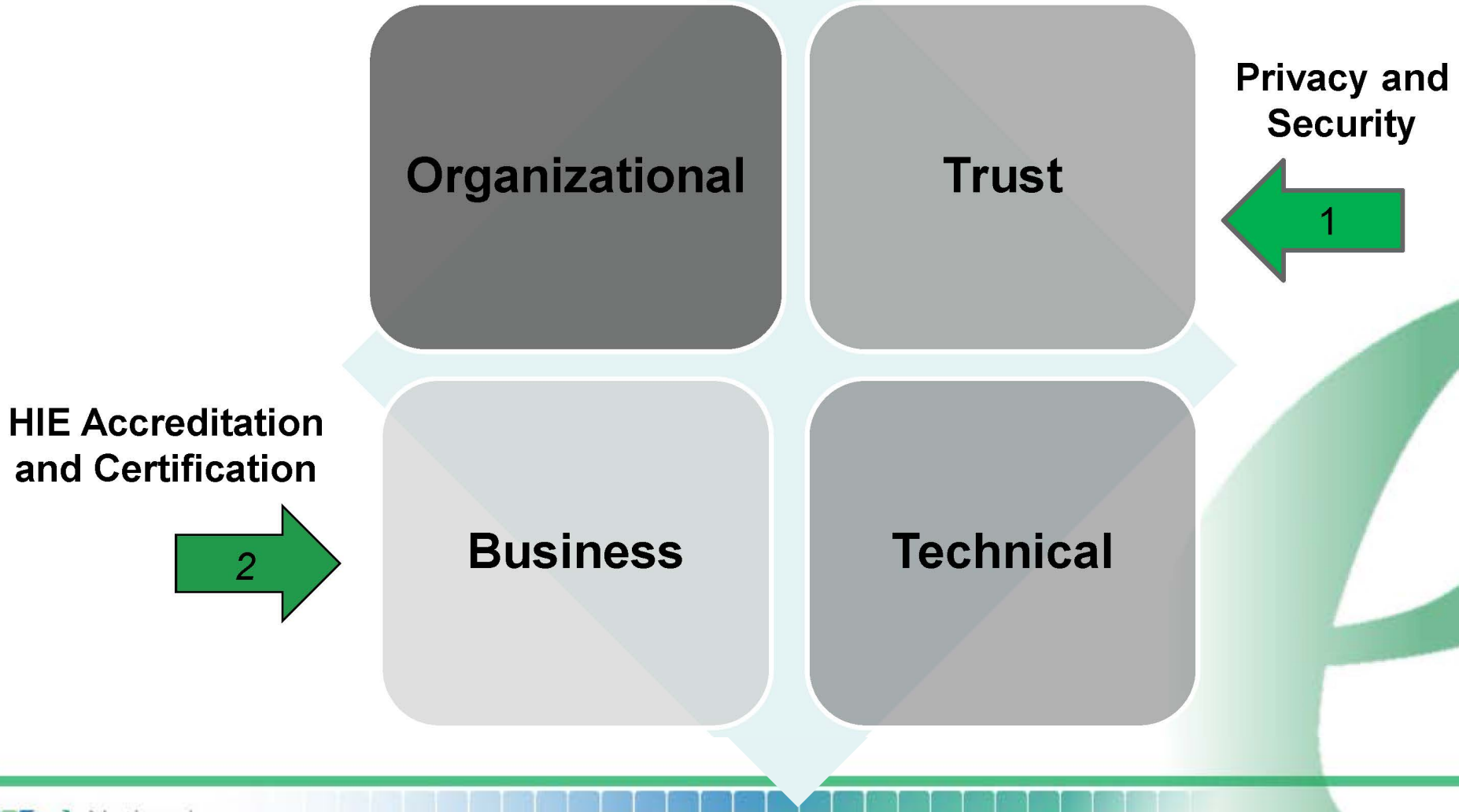
Forum Scope and Process

- Principles from the Governance Framework for Trusted Electronic Health Information Exchange served as a guide for topics to address
- Identified challenging areas within the Governance Framework for Trusted Electronic Health Information Exchange to address concepts such as challenges, gaps, landscape, promising practices, etc.
- Forum participants prioritized issues to work on
- Work groups were created to develop deliverables for review and discussion with Forum
- Steering Committee provided ongoing oversight and input

Governance Framework for Trusted Electronic HIE Guided Topics Participants' Desired to Address

- Trust Principles
  - Trust agreement components
  - Privacy and security components
    - Identity management at patient and provider level
    - Local autonomy - Access policies may differ as a result of varying Applicable Law and business practices
    - Consent - levels of consent, consent across multiple jurisdictions, meaningful consent
  - Alignment of DirectTrust and HealtheWay trust requirements
- Business Principles
  - HIE certification and accreditation landscape
  - HIE measurement and reporting
  - Competition and fees
- Technical Principles
  - Common framework for provider directories
  - Common framework for patient matching

Forum Prioritized Two Key Issues to Address Given Limited Time and Resources



Forum Work Products

Forum Work Products

- Access and identity management for HIE
- Trust Framework for HIE
- HIE Accreditation and Certification Landscape

Access and Identity Management

Background

- Growth in HIE is leading the need for a deeper understanding of security requirements.
- Forum participants identified the need for multi-stakeholder education on current Level of Assurance (LOA) requirements and how stakeholders are strengthening these assurances within and between their organizations.

Privacy and Security Access and Identity Management Workgroup Scope

- The resource examines LOA aspects of identity and access management, including evolving efforts from outside of healthcare, along with business and risk ramifications for stakeholders of moving up the LOA continuum to support secure exchange with a wider group of entities.

Full report available through the ONC website www.healthit.gov/hiegovernance

Trust Framework for HIE

Background

- Achieving an increase in trust among potential exchange participants to support patient health and care requires an understanding of what an organization needs to know about another organization in order to exchange data.

Privacy and Security Access Trust Framework Workgroup Scope

- Develop a whitepaper for consideration by governing entities, organizations, vendors, and providers engaged in health information exchange proposing:
  - A conceptual framework of identity, policy and contractual trust requirements, including attributes and definitions, to facilitate inter-entity exchange and reduce barriers to exchange through transparency into trust policies and practices.

Full report available through the ONC website
www.healthit.gov/hiegovernance

HIE Accreditation and Certification

Background

- Growth in HIE efforts appears to be leading several states and various national entities to develop voluntary or required accreditation and/or certification requirements
- There is concern that this may create duplicative cost and operational hurdles for HIE

HIE Accreditation and Certification Workgroup Scope

- The Forum HIE Accreditation and Certification workgroup will develop an inventory of national, regional, and state accreditation and certification programs, providing a landscape of these efforts including their purpose, scope and source of authority
- This landscape will provide stakeholders with an understanding of the categories of programs, where and why they are emerging, and what they are intended to address.

Full report will be available through the ONC website
www.healthit.gov/hiegovernance

HIE Governance Landscape

Common Trust Elements for HIE

Developed in conjunction with the Governance Framework for Trusted Electronic Health Information Exchange and National HIE Governance Forum Steering Committee

- Agreed Upon Technical Requirements
- Privacy Obligations
- Security Obligations
- Identification & Authentication of users
- Permitted purposes
- Future use of data received
- Role of the intermediary
- Meaningful choice
- Local autonomy
- Reciprocal duty to respond
- Responsibilities of party submitting data
- Authorizations
- Breach notification
- Chain of trust
- Warranty
- Allocation of liability risk

Common Trust Elements for Entity to Entity HIE

Identified by the National HIE Governance Forum Steering Committee , the Privacy and Security Workgroup, and Forum members as common trusts elements regardless of governance model

- Privacy obligations
- Security obligations
- Identification and authentication of users
- Permitted purposes
- Chain of trust
  - Responsibilities and obligations of participants flow down to all participants and users
- Agreed upon technical requirements
- Allocation of liability and risk

Common Privacy and Security Components for HIE

Developed by the the National HIE Governance Forum Steering Committee , the Privacy and Security Workgroup, and Forum members as a sub-set of overall trust elements.

- Local autonomy
- Identity management – proofing and authentication
- Policy assertions within the messages
- Mobile electronic device controls
- Encryption protocols
- Chain of trust
- Breach notification
- Cloud-based storage of PHI
- Email and messaging
- Audit controls and audit log

Current HIE Governance Landscape

Landscape generated from discussions with Forum members, opinions of thought-leaders, and evaluation of current practices:

- Governance implies that there is a group of people that have been empowered to establish mandatory and/or voluntary rules and that rules can be imposed and/or enforced upon a larger group of people or entities
- The challenge with governance in HIE context is that there is no single group empowered to come up with the rules across all exchange activity, and there is no authority to impose and enforce mandatory rules on others.
- In current non-regulatory environment, HIE governance entails consensus building, involving potentially thousands of entities which may or may not have conflicting or competitive business interests.
- HIE governance is an ongoing challenge and will remain so as HIE and stakeholder needs and expectations continue to evolve. However this is does not appear to be an impediment to progress.
- As experience in HIE grows, there will be new issues on which the community will need consensus as well as a mechanism or mechanisms for dispute resolution.
- There are some agreements and mechanisms in place that state that there will be no charges for HISP to HISP transactions within a given community.

HIE Governance Landscape: Key Themes

- HIE is growing but remains relatively immature
- HIE approaches and governance models are heterogeneous and often duplicative
- Forum participants believe it is important to enable trusted information exchange across governing entities, which requires some level of compatibility in HIE governance approaches
- Market requires Forum participants to use push (Direct), query and response, and hybrid models; they need to be able to implement each of these approaches as efficiently as possible for exchange to become widespread
- HIE governance requirements may vary depending on the type of information exchange
- There is confusion about which HIE accreditation and certification requirements HIE entities need to comply with
- Importance of local autonomy requires flexibility in governance
- HIEs will continue to evolve and consolidation is likely.

Value of Work

Value of Forum to Date

- Reduction of silos
- Open communications between HIE governing entities
- Understanding of different HIE approaches enabling various approaches to co-exist
- Understanding of governance at governing entity level
  - Requirements for participation
  - How requirements are established, communicated, monitored, enforced
- Education on how HIE entities address key trust components (e.g., provider identity proofing and authentication)
- Landscape of current accreditation and certification requirements
- Understanding from each other what is working and what isn't working.
- Workgroup interaction and problem-solving

Additional Work on HIE Governance Needed

Additional Work on HIE Governance Needed

- **Coordination**
  - Improve coordination among the many programs and strategies related to HIE to achieve better results (e.g., CMS Innovation grants, ACO programs, bundled payments). HIE is fundamental to improving quality, containing costs and improving health.
  - Enable exchange among participants across HIE governing entities
  - Include vendor-based exchange in governing entity discussions and solutions
  - Build understanding of jurisdiction issues related to legal, regulatory and other issues
- **Technical principles**
  - Develop standard framework for provider directories
  - Develop standard framework for patient matching
  - Expand current work to include patient identity management
  - Incorporate promising practices that include patient engagement and patient mediated exchange
  - Understand issues posed by multiple public and private HIOs operating within states

Additional Work on HIE Governance Needed

- **Trust principles**
  - Develop national baseline of approaches to trust requirements
  - Convene best practices on meaningful choice
  - Expand Forum's work regarding chain of trust
  - Define role of Intermediaries & vendor-based interconnecting networks
  - Understand certification and accreditation requirements and the costs and barriers they present to HIE growth
  - As HIE matures, get ahead of emerging issues with policies and protocols in order to protect trust.
- **Business principles**
  - Measure and report on HIE progress
  - Develop understanding of secondary uses of data and related best practices
  - Understand business practices such as competition and fees and their implications to hinder or accelerate widespread exchange.
  - Understand HISP to HISP charges within basic connectivity agreements.

Work Product Details

HIE Accreditation and Certification Landscape

Full report available through the ONC website
www.healthit.gov/hiegovernance

Content

- Welcome and Roll Call
- Accreditation and Certification Workgroup Final Report
- Final Report Review – key discussion questions
  - What next steps should we add?
  - What conclusions can we draw from these early results?
  - What additional information should be included in the final report?

Content

- Definitions
- Workgroup Purpose
- Workgroup Information Gathered and Analysis
- Summary of Conclusions and Next Steps

Forum HIE Accreditation and Certification Workgroup

Workgroup Charge

- Develop an inventory of national, regional, and state accreditation and certification programs, providing a landscape of these efforts including their purpose, scope and source of authority

Workgroup Purpose

- This landscape will provide stakeholders with an understanding of the categories of programs, where and why they are emerging, and what they are intended to address

Definitions

**As determined by the Accreditation & Certification workgroup*

Accreditation

- A process in which evidence of competency, authority, or credibility is presented
- The accreditation process ensures that their policies and practices are acceptable, that organizations behave ethically and employ suitable quality assurance and, if appropriate, that they are competent to test and certify third parties

Certification

- The process of certifying that a certain product has passed performance tests and quality assurance tests, and meets qualification criteria stipulated in contracts, regulations, or specifications

Accrediting and Certifying Organizations Data Request

- Key accreditation and certifying bodies, including state designated entities, were invited to share information to provide understanding of the HIE accreditation and certification landscape
  - Purpose of Accreditation/Certification program:
  - Who is this accreditation/certification relevant to? Who is the target audience?
  - What is the scope (technical, policy, etc.)?
  - What are the issues that are addressed?
  - What are the types of assurances that are gained?
  - What is the source of the authority; i.e. state, regional, national organization?
  - Is the program voluntary or required?
  - Is it an evaluation or a registry?
  - Are there any standards that are being used as a baseline for their certification or accreditation?
  - Are you aware of any overlap in the industry regarding HIE accreditation and certification? If yes, please provide details on overlap.
  - What are the gaps in current HIE accreditation or certification activities; i.e. what other matters would be best served by receiving an accreditation or certification by a third party?
  - What type of entity is best suited to perform this additional verification?

Organizations Who Provided Information

National	***Statewide***
- Surescripts - EHNAC - CCHIT - DirectTrust - Healtheway	- State of Indiana - State of Kansas - State of Pennsylvania - State of Vermont - Minnesota Dept. of Health - State of Texas

Initial Conclusions from Information Gathered from Accrediting and Certifying Organizations

- A continuing theme around these efforts is that to increase trust and interoperability.
- Much of the target audience consists of HISPS, HIOs, providers, vendors, or HIEs.
- The scope of the accreditation & certifications center around:
  - Technology
  - Policy/Legal including trust agreements
  - Security
  - Financial Sustainability including fee structures
- Approximately half are required and half are voluntary with some – Texas – being voluntary unless you would like to be listed as a trusted entity.
- The majority of accreditation & certifications are evaluations
- Many states are using national sources like EHNAC, DirectTrust, Healtheway, and CCHIT as a basis for their accreditation and certification efforts but some – Vermont, Indiana mostly, and Pennsylvania – pull from other sources as well.

Secure Messaging vs. Query-Based

- Accrediting and certifying bodies that address secure messaging:
  - DirectTrust
  - EHNAC
  - State of Rhode Island
  - State of Indiana
  - Minnesota Department of Health
- Accrediting and certifying bodies that address query-based exchange:
  - Healtheway
  - State of Indiana
  - CCHIT
  - State of Pennsylvania
  - Minnesota Department of Health

Purpose of Accreditation and Certification Programs

- Many cite the need to ensure HIOs, HISPs and providers exchanging information in a state have been reviewed and approved by an impartial certifying body and establish trusted relationships with each other for exchange
- Surescripts states that their purpose is “to provide HIE services related to Direct HIE products as well as to support the exchange of HIE information between HIEs within our network ecosystem”
- ENHAC states their purpose is to “develop standard criteria and accredit organizations that electronically exchange healthcare data”

Target Audiences and Scope

Target Audiences

- HISPs
- HIOs
- Providers
- Vendors
- HIEs

Scope

- Technology
- Security
- Financial sustainability including fee structures, plans for charging providers, long-term care facilities, etc.
- Policy & Legal Implications including trust agreements

Required vs. Voluntary Programs

Required

- Minnesota
- Pennsylvania
- Vermont
- Kansas

Voluntary

- DirectTrust
- Rhode Island
- CCHIT
- Surescripts
- EHNAC
- Indiana
- Texas
- Healtheway

Potential Gaps

- What are the gaps in current HIE accreditation or certification activities; i.e. what other matters would be best served by receiving an accreditation or certification by a third party?
  - We do not yet have a reliable and comprehensive testing and certification service unique for HISP/STAs. These entities may be partially tested and certified when using specific EHR vendor modules as "relied upon software" within the context of the 2014 Edition Certificate Criteria. However, not all HISPs have these partnerships.

Additional Verification

- What type of entity is best suited to perform this additional verification?
  - Initially at this early stage, state programs are adequate; however ultimately a public/private non-profit should be responsible
  - Verification standards and other criteria should be set by a community entity or government
  - Verification against criteria should be performed by an independent third party

Data Request of Non-Accrediting and Certifying Organizations

- Invited non-certifying bodies to provide information about accreditation and certification programs they are subject to.
  - Organization Name:
  - What HIE accreditation and certifications are you required to comply with?
  - What voluntary HIE accreditation and certifications do you currently comply with?
  - Are they evaluation or registries?
  - Are you aware of any overlap in the industry regarding accreditation and certification requirements?
  - What are the gaps in current HIE accreditation or certification activities; i.e. what other components would be best served by receiving an accreditation or certification by a third party?
  - What type of entity is best suited to perform needed accreditation or certification?

Non-Accrediting and Certifying Organizations Who Provided Information

- Great Lakes HIE (GLHIE)
- Brooklyn Health Information Exchange (BHIX)
- Rhode Island Quality Institute (RIQI)
- Oregon Health Authority/CareAccord (OR HIE)
- ConnectHealthcare
- Advanced Answers on Demand, Inc.

Initial Conclusions from Non-Accrediting and Certifying Organizations

- The majority of respondents are not required to comply with any accreditation or certification programs although states (OR, NY) are slowly developing these programs that may be required in the future.
- Many are voluntarily certified and accredited with EHNAC and CCHIT.
- Many did not understand the question about registries vs. evaluations so we did not receive a good sense of their answer.
- Most were not aware of any overlap in the current requirements.
- Meaningful Use and HIE was cited by two respondents as a potential gap that could be filled by a third party.
- Two respondents cited an “independent” organization as the best one to administer the needed certification and/or accreditation. Some cited EHNAC or CCHIT. One suggested a government agency or accreditation commission. One suggested an entity who was fluent in the laws of the specific state.

Required Programs

- **What HIE accreditation and certifications are you required to comply with?**
  - The GLHIE Security Plan identifies several laws and standards with which GLHIE and GLHIE users are required to comply, as stated in Data Use Agreements and BAAs. GLHIE's system partner, Optum, is contractually required to comply with state and federal laws and national standards related to privacy and security. The following laws and standards are cited in the GLHIE Security Plan:
    - The Privacy Act of 1974
    - Computer Security Act of 1987
    - Federal Information Processing Standard (FIPS) 199
    - Federal Information Processing Standard (FIPS) 200
    - The Health Insurance Portability and Accountability Act of 1996
    - OMB Circular A-130
    - National Institute of Standards and Technology (NIST) Guidance
  - New York State Regulations are expected in 2014 that would require Certification of all RHIOs.
  - None

Voluntary Programs

- **What voluntary HIE accreditation and certifications do you currently comply with?**
  - Currently BHIX – like all RHIOs in New York -- is voluntarily undergoing a "provisional" certification assessment by a vendor contracted to provide such certification services through the New York eHealth Collaborative (NYeC). This provisional certification will provide information and a gap analysis that will allow authorization for sharing of data between the state RHIOs (QEs) and will highlight areas for improvement in 2014-15, when full certification is expected to be required.
  - ONC 2011 Edition, ModularEHR, CC-1112-833360-1 and CCHIT LTPAC EHR 2011 +Home Health +Skilled Nursing Facility
  - GLHIE is fully accredited by the Electronic Health Network Accreditation Commission (EHNAC), in the HIE Accreditation Program.
  - EHNAC

Evaluations, Registries, & Overlap

- **Are they evaluation or registries?**
  - Fully certified, functional, and in production.
  - Evaluation of self- assessment and site visit.

- **Are you aware of any overlap in the industry regarding accreditation and certification requirements?**
  - There is overlap between the two certifications above, with the LTPAC being more comprehensive and specific to our industry, long-term and post-acute care. There is some concern that a new edition may not be available.

Potential Gaps

- **What are the gaps in current HIE accreditation or certification activities; i.e. what other components would be best served by receiving an accreditation or certification by a third party?**
  - It is expected that funding, with State funds flowing through DOH and NYeC, will be dependent upon achieving certification, which, in turn, will allow a RHIO to become “qualified” (i.e. a “Qualified Entity”) in the new New York regulatory framework for the SHIN-NY
  - Meaningful Use certification for HIEs.
  - Current ONC Meaningful Use certifications have limited value to testing a system for real-world use in ACO or HIE implementations as relates to transitions of care between acute or ambulatory settings and the quite different world of long term care. The S&I Framework has addressed some of this by including some elements of care planning, but more needs to be done. However, the largest gap exists in the functionality that is offered by the various HIE, and there appears to be no standardized approach to content or communication protocols.

Entities to Perform Needed Programs

- **What type of entity is best suited to perform needed accreditation or certification?**
  - Independent. *Comment: It is too early to be working on accreditation and certification. New HIEs are fiscally fragile. The need some time to become functional before adding a layer of requirements
  - An independent organization, such as the Electronic Healthcare Network Accreditation Commission (EHNAC). Please note: RIQI and the Rhode Island HIE rely on the compliance of others. RIQI's Direct efforts are built upon the HISP accreditation program run by DirectTrust and EHNAC. (The DirectTrust accreditation is replacing our self-grown accreditation process). Also, RIQI relies upon the Meaningful Use certification of EHRs, since our interoperable processes lever components dictated by the certification process (e.g. Direct capabilities, CCDs/CCDAs).
  - Government agency or accreditation commissions currently engaged in the activity.

Entities to Perform Needed Programs *(continued)*

- **What type of entity is best suited to perform needed accreditation or certification?**
  - An entity best suited to perform accreditation or certification of Qualified Entities in New York State would be one that comprehends the complexity of the HIE environment from many perspectives, including but not limited to technical applications, policy and privacy concerns, overall operations as well as the business community. The entity would also need to be well versed in Federal Law, New York State Law as well as emerging New York State Policy Guidance which governs health information exchange.
  - We believe the current ATCB process with entities like CCHIT are the best.

Suggested Next Steps

- Continue to inform and educate the community on the types of accreditation and certification programs, status, and progress.
- Raise awareness of the value proposition and business case for accreditation and certification.
- Identify a neutral, credible third-party organization and encourage them to keep track of current accreditation and certification programs for community reference.
- Encourage above organization to build on current landscape work and collaboratively identify gaps and consider how best to fill them.

LOA Resource Overview

Full report available through the ONC website
www.healthit.gov/hiegovernance

LOA Resource Overview

- Background
  - Section One: Forum Background
  - Section Two: Identity Management Overview
  - Section Three: Identified Gaps
- References
  - Section Four: Definitions
    - Identity Proofing
    - Electronic Authentication

LOA Resource Overview

References (cont.)

- Section Five – HIPAA
  - Security Rule requirements
- Section Six - National Efforts and Policy Recommendations
  - HITPC
  - NIST
  - NSTIC
  - Kantara
  - OASIS

LOA Resource Overview

References (cont.)

- Section Seven - NIST 800-63-2 (Finalized 9/5/2013)
  - Table 1 provides an overview of the NIST guideline for implementing electronic authentication and defines requirements for four levels of assurance. Key requirements for identity proofing, token usage, and authentication protocols are summarized.
  - Table 1 has been reviewed by several security experts

NIST Electronic Authentication Guideline 800-63-2 Table 1

	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	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

LOA Resource Overview

Level of Assurance Continuum

- Section Eight
  - Table 2 provides a snapshot of the benefits of moving to higher LOA levels.
  - Consistent with the HIPAA Security Rule, each organization should use the results from their own 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.

Level of Assurance Continuum of Benefits Table 2

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	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 the asserted identity's validity
Federal Agency Exchange			Required for Organizational and Individual participants*	
Direct			Required for Direct Trust participants (Organizational and Individual	
HealtheWay			Required for HealtheWay participants (Organizationl)	

Level of Assurance Continuum of Benefits Table 2

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
MU		Required for MU2 for providers	Proposed for MU3 for providers	
eRX		Required for e-RX	Required for e-RX of controlled substances	
Risk Mediation Cyber Insurance			Potential reduction in premiums**	Potential reduction in premiums**

LOA Resource Overview

Level of Assurance in Practice

- Section Nine - Provides sample use case and Forum participant practices for consideration at your organization

1. Require participants to follow recommended operational practices for Identity Proofing and Authentication and provide Checklists and Education in order for participants to do so
2. Require participants to perform a risk assessment and prescribe the minimum LOA sufficient to counter the identified risks.
3. Adopt the Office of Management and Budget's (OMB) 5-step process for reviewing and setting LOA requirements.
   - Conduct a risk assessment of their systems
   - Map identified risks to the appropriate assurance level
   - Select technology based on e-authentication technical guidance
   - Validate that the implemented system has met the required assurance level
   - Periodically reassess

LOA Resource Overview

Level of Assurance in Practice

– Section Nine – Cont.

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. Ex: 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

LOA Resource Overview

Level of Assurance in Practice Section Nine (Cont.)

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 with security policies. (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
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

LOA Resource Overview

Trust Models

- Section Ten - Provides views of trust models and organizational LOA considerations when exchanging health information

Appendix

- Section Eleven – Additional Resources
- Section Twelve – Attribution
- Endnotes

Trust Framework Overview

Full report available through the ONC website
www.healthit.gov/hiegovernance

Trust Framework

Who is the audience for a trust framework?

- Governing entities, organizations, vendors, and providers engaged in health information exchange.

What is the intended purpose of the trust framework?

- A whitepaper for consideration by governing entities, organizations, vendors, and providers engaged in health information exchange proposing:
  - A conceptual framework of identity, policy and contractual trust requirements, including attributes and definitions, to facilitate inter-entity exchange and reduce barriers to exchange through transparency into trust policies and practices.

How is the trust framework organized?

- Based on a conceptual framework of Identity, Policy and Contractual elements.

Trust Framework (cont.)

Satisfies the need to explicitly express obligations and assertions:

- A consistent approach to describing components of identity assurance including LOA for digital certificates across all levels of the exchange hierarchy
- A consistent approach to the classification of trust attributes including identity, policy, and contract elements defined by various governing entities such as Direct, HealtheWay, CCC, and other regional jurisdictions
- A consistent method for each trading partner to expose their own trust elements and transparently access those of their trading partners

Trust Framework Use Case

Two organizations without a common top-level trust anchor point (different trust and policy environments) have a need to exchange data, and wish to do so electronically.

- **Assumption:** Each organization has flow down trust obligations from their anchor point as well as local autonomy to vary certain trust requirements and exchange policies.
- **Issue to Resolve:** What does each organization need to know about the other in order to exchange without establishing one-off trust agreements or contracts?
- **What is Involved:** Each organization must gather information supplied by the other or that is otherwise publically available. The organization sending data must decide according to its own policies and procedures.

Trust Framework in Practice

- The anchor point for each trust group (chain of trust) would construct their trust elements and assert them in a way that is discoverable by others.
- Organizations would share their anchor point and local trust elements in computable technical expressions of trust (a digital handshake) between the ultimate sender and ultimate receiver, across domains, end points and intermediaries throughout chain of trust.
- Sharing trust elements in this way allows both the sender and receiver to compare those elements to their individual requirements, and for each to determine whether their baseline requirements are met for exchange to occur.

Evaluating the Chain of Trust

Without regard to the mechanics of how the trust attributes are published and shared, assume that each organization can "see" the attributes of each intermediary point between themselves and the endpoint who will be receiving the data.

- Since each organization within the trust chain of the data sender is already vetted for their trust elements (they are all part of the same chain of trust), the data sender starts with the top level of the chain where data is going.
- The credentials and trust assertions for each organization that may have access to the data will be examined against the sending organizations requirements.
- Once all organizations in the chain to the endpoint have been examined, the data sharing decision can be made.

Trust Framework - Technical Details

Taxonomy Axes (subsets):

- **Identity** - attributes used to confirm identity and provide adequate technical level of assurance of that identity and its authorization.
- **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.

Identity Axis Data Elements

- 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, HISP, Connector, etc.)
- Proofing Level (how was this identity established and “proofed”) – for individuals, NIST has levels of proofing: for organizations, the individual representing the organization is proofed, and then the organization identity is established through records search.
- Certificated? (Y/N)
- Issuing CA – if there is a chain, the full chain back to the root organization 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.)
- Contact person information (this is information on a live person who “represents” this identity if the identity is not a real person): Name; Address; Contact Number
- End Point (Y/N)
- Others…

Policy Axis Data Elements

- Identity (name)
- 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 MPI
- Requirements for Consent Elements (several)
- Privacy Policies
- Security Policies
- Audit log review policy
- Standards supported
- Profiles supported
- Permitted purposes for request / use
- Others…

Contract Axis Data Elements

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

Appendix of Presentations

Available through the ONC website
www.healthit.gov/hiegovernance