Governance Design Group

Meeting #1 - May 23, 2018
Meeting #2 – June 6, 2018

OHS CONNECTICUT Office of Health Strategy

CONNECTICUT HEALTH INFORMATION TECHNOLOGY OFFICE

Agenda

Agenda Topic	Lead	Duration
Welcome Remarks – Meeting Overview and Objectives	Jennifer Richmond	10 min
Introductions • 2-minute introductions of name, job (organization and title), brief summary of the role on Design Group and the sector perspective being represented by members	All Design Group members and support staff	20 min
Charter • Walk-through of Governance Design Group draft charter • Request approval of charter by group	Michael Matthews	20 min
Discuss planning process • Proposed meeting schedule • Proposed timeline of meeting topics	Michael Matthews	15 min
HIE Governance Basics • Principles • Trust • P&P • Organizational • National perspectives • State perspectives	Michael Matthews	20 min
Meeting Wrap-up and Next Steps	Michael Matthews	5 min

Project Structure

Executive Sponsor

Allan Hackney, Connecticut's Health Information Technology Officer (HITO)

Project Oversight

Health IT Advisory Council - Member Listing

Members

Lisa Stump, MS – Yale New Haven Health
Pat Checko, DrPH – Consumer Advocate and Public Policy Professional
Jake Star – VNA Community Healthcare & Hospice
Bruce Adams, JD - Office of the Lieutenant Governor
Pending- Office of the Attorney General (TBD)
Polly Bentley – DSS representative (on assignment from HealthTech Solutions)

Support Staff

HIT PMO
Jennifer Richmond
Sarju Shah
M.J. Lamelin
Grace Capreol
Kelsey Lawlor
Dino Puia

CedarBridge Group
Michael Matthews, Lead
Steve Gravely, SME
Chris Robinson, PM & Analyst

Consulted:

Victoria Veltri, Executive Director, Office of Health Strategy

Purpose of Governance Design Group

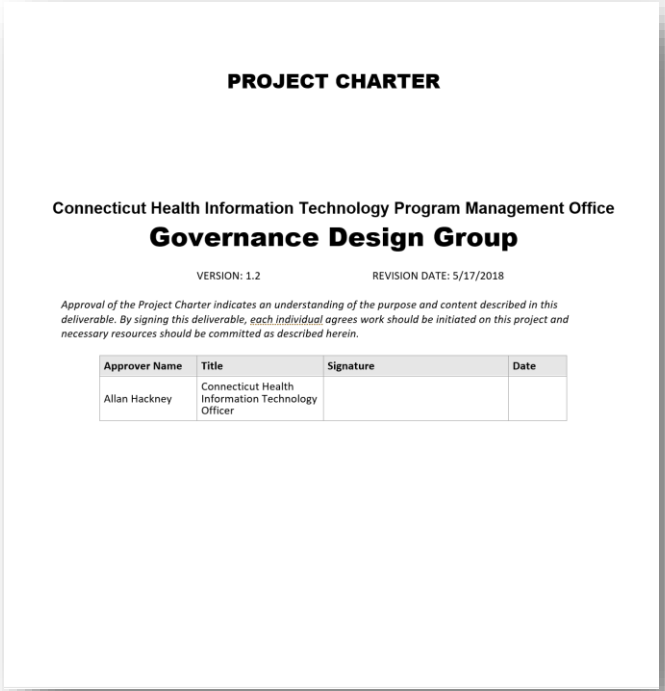
- Develop **recommendations for the Health IT Advisory Council to address:**
  - **Relationship of Health IT Advisory Council, the State of Connecticut, and the HIE entity**
  - Pros and cons of establishing a **new HIE entity or designating an existing entity with recommendations**
  - Baseline elements of **a trust framework and agreement**
  - Table of contents for HIE **Policies and Procedures**
  - **Critical success factors** in HIE governance

Goals and Objectives of Governance Design Group

- Develop **high-level requirements for the Connecticut HIE governance structure**
- Define **attributes of a "neutral and trusted entity"**
- Review **models of governance** used successfully by other state HIEs
- Review **state and national legislation and regulations** that should inform HIE governance
- **Review existing trust frameworks and trust agreements** commonly used for interoperability and HIE initiatives

Design Group Charter: Review

- Project Purpose
- Project Goals and Objectives
- Project Scope
- Critical Success Factors
- Project Milestones
- Project Structure



PROJECT CHARTER

Connecticut Health Information Technology Program Management Office

Governance Design Group

VERSION: 1.2 REVISION DATE: 5/17/2018

Approval of the Project Charter indicates an understanding of the purpose and content described in this deliverable. By signing this deliverable, each individual agrees work should be initiated on this project and necessary resources should be committed as described herein.

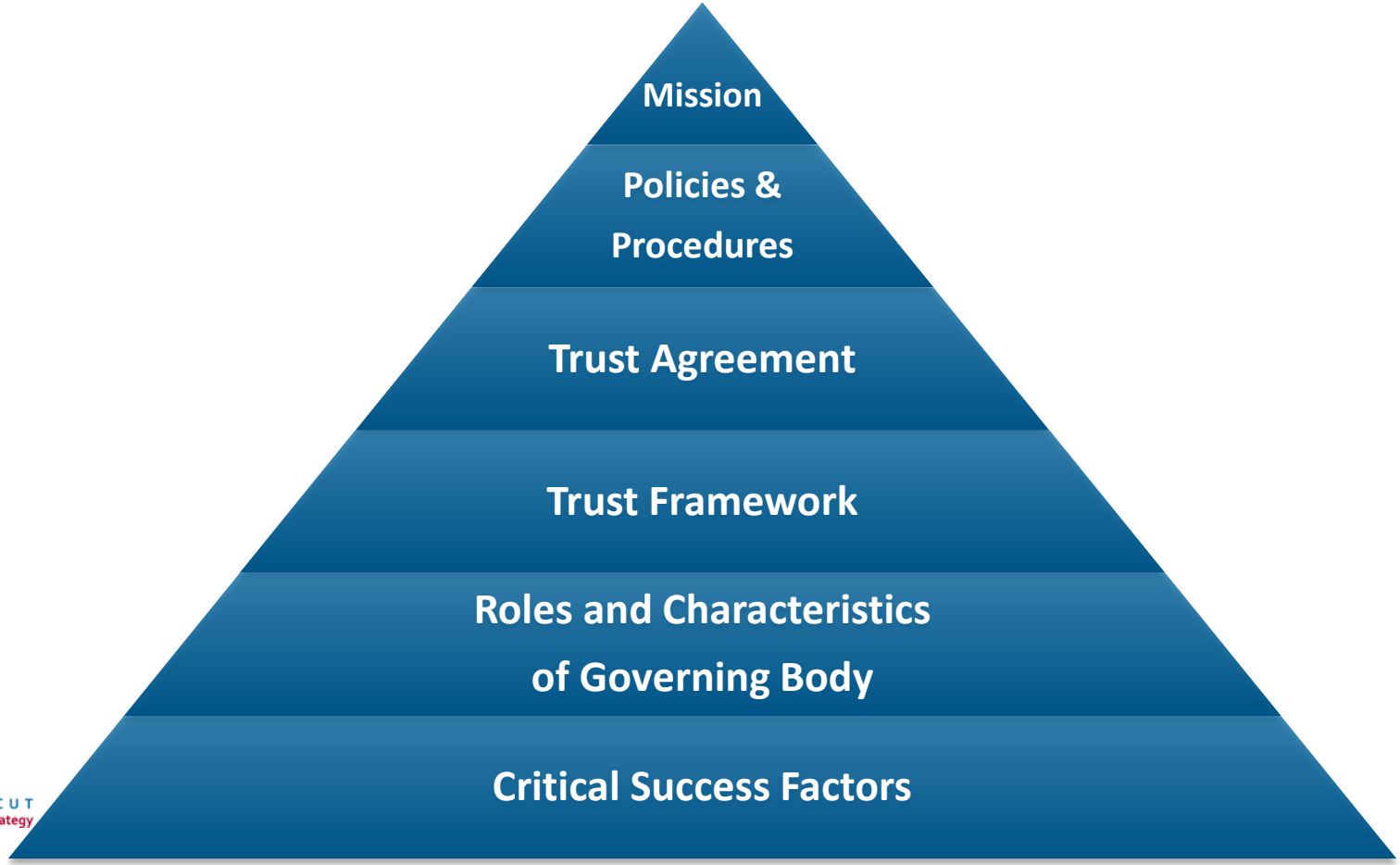
Approver Name	Title	Signature	Date
Allan Hackney	Connecticut Health Information Technology Officer		

Grounding Principles

"Health Information is exchanged at the speed of trust."

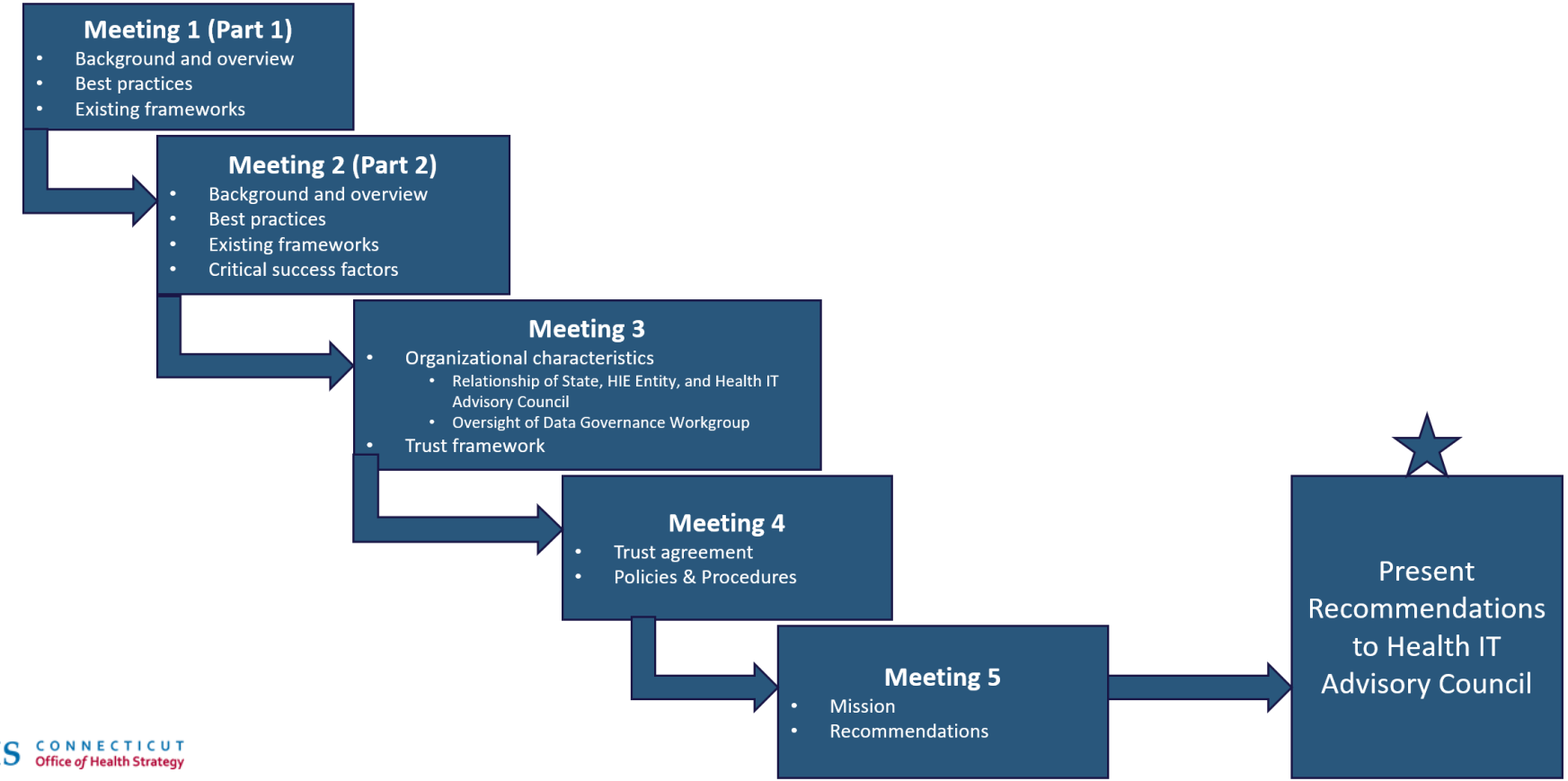
Farzad Mostashari

Governance Design Group Building Blocks



OHS CONNECTICUT Office of Health Strategy

Proposed Meetings and Topics



Health Information Exchange (Noun)

- Entity that provides services to enable exchange
- Policy and governance
- Trust Framework

Exchange of Health Information (Verb)

- Technology
- Exchange of health-related information

Data Governance

- Decision rights & accountabilities
- The how, when, with whom, and under what circumstance data is exchanged

Sustainable, successful HIE requires each level to work smoothly and work in tandem

Source: https://www.healthit.gov/

Governing Authority

- HIE entity established
- Governing authority codified
- “Rules of the Road” established for Participants
- *“Form follows function”*
  - Board
  - Board committee
  - Empowered council

Source: eHealth Initiative

Senate Bill No. 1502 June Sp. Sess., Public Act No. 17-2

- HITO and Secretary of OPM may establish or incorporate an entity to implement the program
- Such entity shall, without limitation, be owned and governed, in whole or in part, by a party or parties other than the state and may be organized as a nonprofit entity.
- Any entity established or incorporated shall have its powers vested in and exercised by a board of directors. The board of directors shall be comprised of the following members who shall each serve for a term of two years. One member who shall have expertise in the following areas:
  - advocate for consumers of health care, appointed by the Governor;
  - clinical medical doctor, appointed by the president pro tempore of the Senate;
  - hospital administration, appointed by the speaker of the House of Representatives;
  - corporate law or finance, appointed by the minority leader of the Senate;
  - group health insurance coverage, appointed by the minority leader of the House of Representatives;
  - The Chief Information Officer, the Secretary of the Office of Policy and Management and the Health Information Technology Officer, or their designees, who shall serve as ex-officio, voting members of the board; and
  - The Health Information Technology Officer, or his or her designee, who shall serve as chairperson of the board

Role of the Board for Statewide HIE Entity (1 of 2 example)

- Setting strategic direction
- Establishing goals, objectives, and performance measures
- Convening stakeholders to create trust and consensus
- Determining acceptable uses that are driven by value and considerations related to privacy and security of health information
- Managing and maintaining financial sustainability
- Providing oversight and holding customers accountable for complying with all participation requirements
- Interpreting and applying standards, policies, and agreements for health information exchanges that are recommended by the state and that apply both to public and private sector entities
- Approving the design, implementation, and administration of a certification process for customers to ensure compliance with state and national health information exchange standards, policies, and agreements
- Coordinating integration and use of HIE amongst other public and private sector health information technology related projects within the state

Role of the Board for Statewide HIE Entity (2 of 2 example)

- Recommending policy changes, as appropriate and necessary, to state executive, legislative, and judicial branches to reduce barriers to participation in HIE and enhance privacy and security protections for the health information that is exchanged through the HIE
- Providing recommendations for the resolution of issues of standards harmonization, interstate/national policy, technical interoperability and applicable current and future federal and state regulations
- Contracting with vendors to provide any additional services that are necessary to build, maintain, and operate the HIE
- Enforcing accountability with vendors contracted to the HIE for meeting designated service metrics and imposing penalties as contractually appropriate
- Determining how the HIE will be represented in dispute resolution

CONNECTICUT
HEALTH INFORMATION
TECHNOLOGY OFFICE

Introduction to Governance Models

OHS CONNECTICUT
Office of Health Strategy

Components of Governance Framework

Source: https://www.healthit.gov/

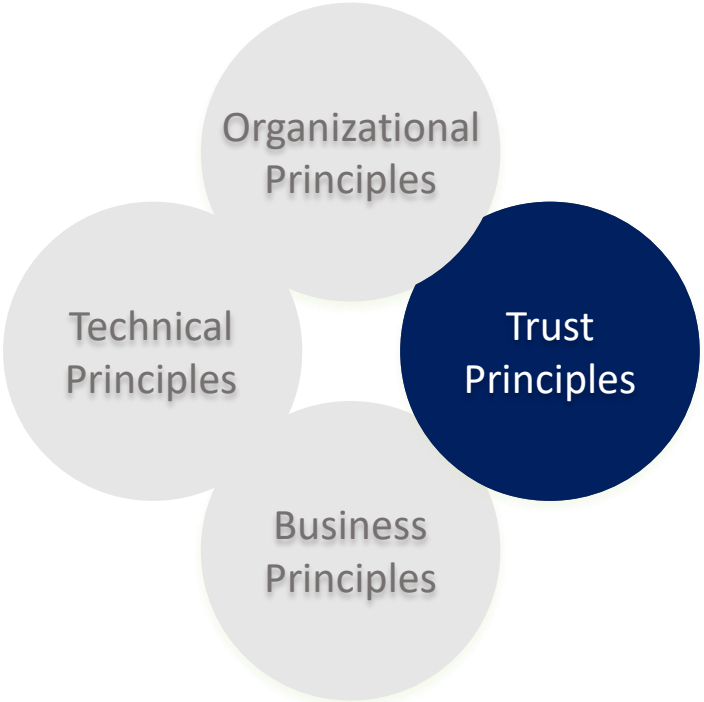
Organizational Principles

- Operate with transparency and openness
- Establish mechanisms to ensure that the entity's policies and practices and adherence to applicable federal and state laws and regulations
- Promote inclusive participation and adequate stakeholder representation, especially patients in the development of policies and practices
- Ensure oversight is consistent and equitable
- Provide due process to the stakeholders to which it provides oversight

Source: https://www.healthit.gov/

Trust Principles

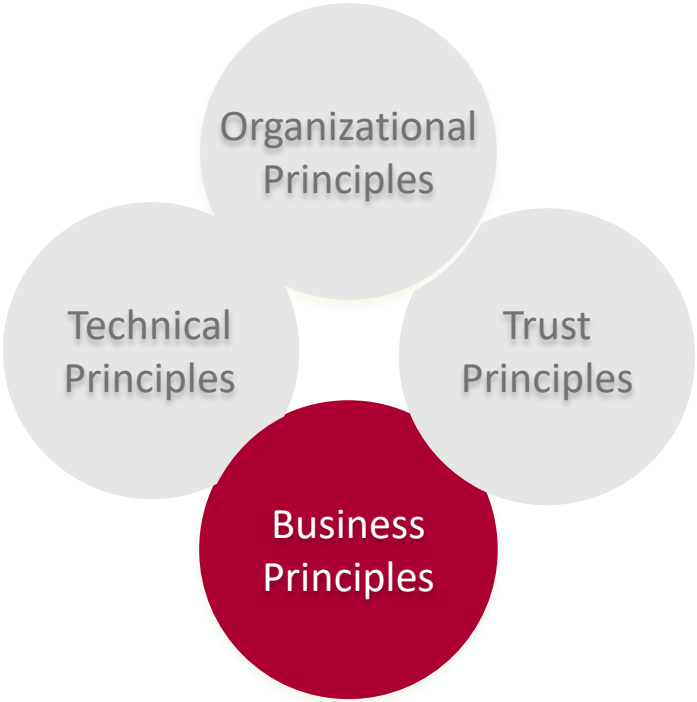
- Public access to “Notice of Data Practices,” including data use agreements
- Explanation of privacy and security policies
- Provide meaningful choice as to whether personally identifiable information can be exchanged
- Request data exchange limits based on data type or source (e.g. substance abuse treatment)
- Ability to access and request changes to personally identifiable information
- Assurance that personally identifiable information is consistently and accurately matched when electronically exchanged



Source: https://www.healthit.gov/

Business Principles

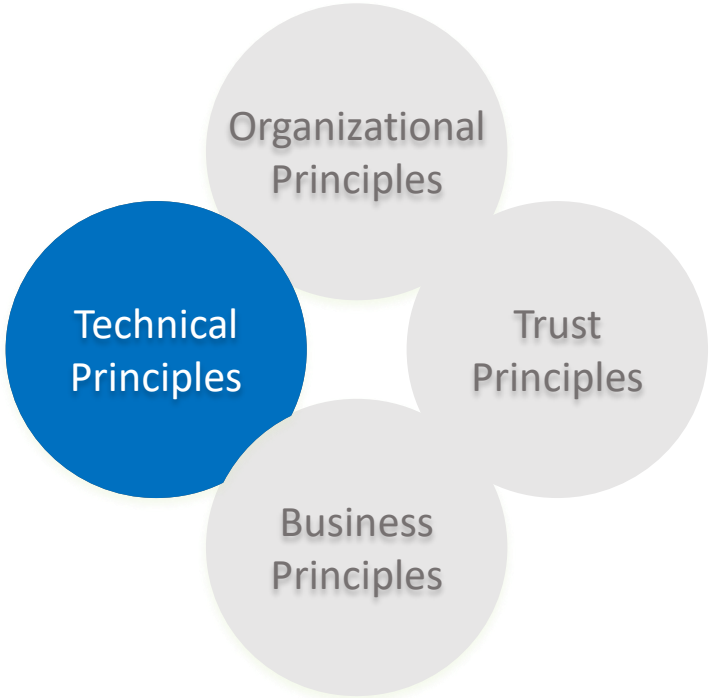
- Set standards of participation that promote collaboration and avoid differences in fees, policies, services, or contracts
- Provide open access to exchange services (e.g. directory data) that would enable partners to identify with whom they can electronically exchange information
- Publish statistics describing their electronic exchange capacity
- Maintain and disseminate up-to-date information about: compliance with relevant statutory and regulatory requirements; available standards; potential security vulnerabilities, and best practices developed for HIE



Source: https://www.healthit.gov/

Technical Principles

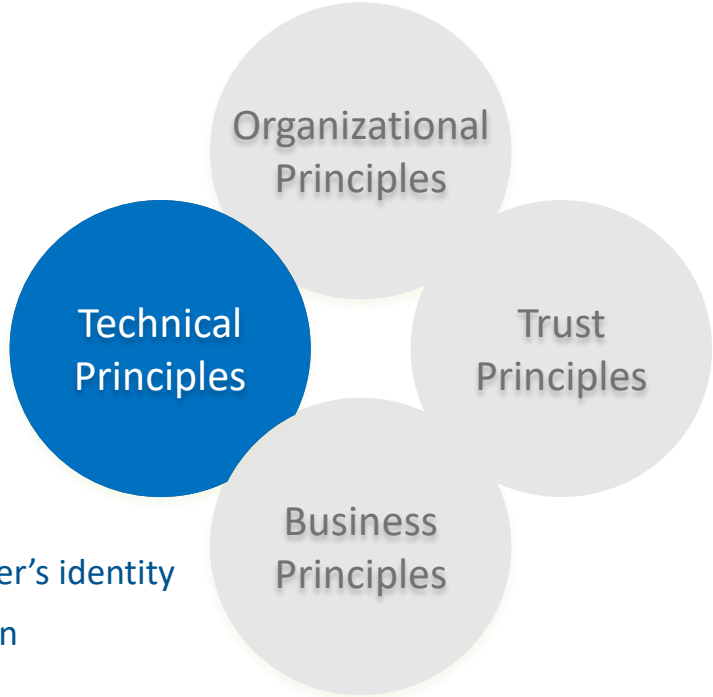
- Ensure that technology is implemented to support the Trust and Business Principles
- Encourage the use of vocabulary, content, transport, and security standards, and associated implementation specifications developed by voluntary consensus standards organizations (VCSOs) when federal standards have not been adopted
- Lead engagement in VCSOs and national efforts to accelerate standards development and consensus on the adoption of standards as well as the improvement of existing standards.
- Work with VCSOs to develop standards for specific use cases and volunteer to pilot and use new standards when no such standards exist
- Take an active role in development and implementation of conformance assessment and testing methods for HIE and utilize (or promote the use of) testing methods developed to assess compliance with federal standards



Source: https://www.healthit.gov/

Technical Principles: Securing Data

- Multi-factor authentication
- Utilizing data-encryption
- Digital Certificates
- Accreditation
- Public Key encryption
- Hardware/software tokens
- Secured sockets layer
- VPNs
- Mutual node authentication to assure each node of the other's identity
- Transmission integrity to guard against improper information modification or destruction while in transit
- Transmission confidentiality to ensure information in transit is not disclosed to unauthorized individuals, entities, or processes



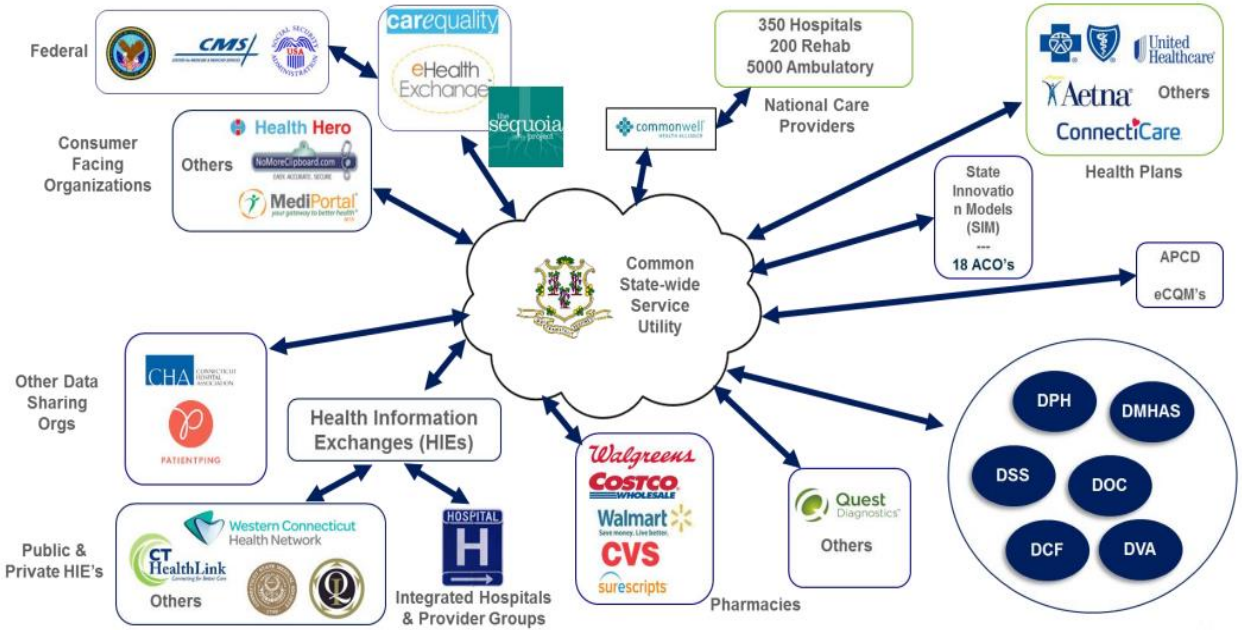
Source: Public Health Data Standards Consortium. "Data Standards." Health Information Technology Standards. 2013. http://www.phdsc.org/standards/health-information/d_standards.asp.

Technical Principles: Technical/Interoperability Standards

- **Health Level 7 (HL7) –** core standards-based interoperability, HL7 version 2 messaging most dominant, multiple sub-versions, complex, not always compatible. Most commonly used to exchange laboratory orders and results, patient admissions, discharges and transfers from in-patient facilities, and immunizations
- **Clinical Document Architecture (CDA)** — is sometimes confused with Version 3 messages but represents data in a different paradigm, that of clinical documents
- **Continuity of Care Document (CCD)** - supports clinical summaries which contain a wide variety of information about a patient encounter and/or history available for system-to-system transmission *and* viewing through a standard web browser with the aid of an external style sheet that helps define the aesthetic look of the document. Its flexibility has led to a number of efforts to limit, or constrain, what might appear in a CCD to focus its use on a particular need or set of needs.
- **Health Information Technology Standards Panel (HITSP) C 32 -** specification which is referenced by many HIE deployments and many organizations. Though HITSP has been eclipsed by other activities, many of its artifacts continue to be foundational for healthcare data interoperability
- **Consolidated CDA** - is a library of CDA templates bringing together the work of various organizations and is the basis for Meaningful Use clinical documents
- **Fast Healthcare Interoperability Resources (FHIR)** -provide another option for representing clinical content as either XML or JSON objects. FHIR resources are defined for most clinical content and can be assembled with as much or as little as is needed to fulfill a particular use case. While FHIR is simpler to use than any other data representations, it still needs to be consistently deployed among data trading partners to ensure compatibility.
- **Other Standards include:** USCDI, SMART, API, XCA, XCPD, SAML, SOAP, BPPC, NCPDP

Source: Public Health Data Standards Consortium. "Data Standards." Health Information Technology Standards. 2013. http://www.phdsc.org/standards/health-information/d_standards.asp; https://www.hln.com/knowledge/interoperability-standards/

Connecticut – “Network of Networks”



Contracted participants will include:

- Individual provider entities (clinics, hospitals, etc.)
- Orgs representing multiple entities (e.g. HIEs)

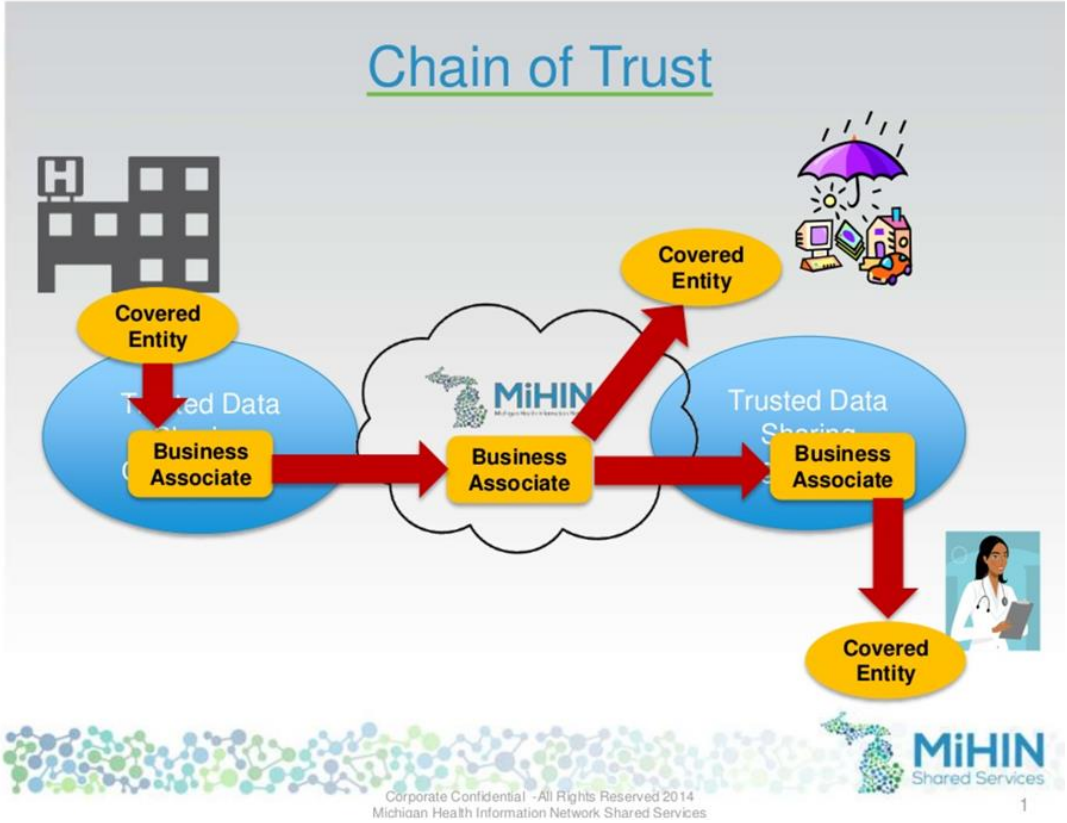
Uniform contract terms and “rules of the road” apply to all participants and flow down to exchange partners of participants

State Example - Michigan

- Michigan has a collaborative governance structure with the Health Information Technology Commission and Michigan Health Information Network (MiHIN) Shared Services.
- A not-for-profit and the State Designated Entity (SDE), MiHIN Shared Services is responsible for implementing the state's operational plan and has complete authority over its organization.
- The HIT Commission, created by the Michigan Legislature and a participant in the governance of the SDE, is responsible for recommending policies for HIT and HIE adoption, as well as for monitoring the progress of HIT and HIE statewide.
- MiHIN Shared Services has its own Board of Directors
- MiHIN Shared Services uses the network of networks architectural model.
- Providers will connect to HIE's that will in turn connect to each other as part of the Health Information Network

Source: https://truvenhealth.com/portals/0/assets/GOV_11558_0712_HIE_Governance_WP_WEB.pdf

MiHIN's Chain of Trust



MiHIN utilizes a modular, highly standardized legal framework by utilizing a Master Use Case Agreement (MUCA) that can incorporate multiple use cases. The MUCA includes language on:

- Definitions
- Basic Connection Terms
- Basic BAA Terms
- Minimal Operational Service Level Agreements
- Contracting & Payment
- Cyber Liability Insurance
- Termination

The MUCA and its 3 elements (Use Case Summary, Use Case Exhibit, and Implementation Guides) allow for conformance and validation reports, Statement of Work, PO from a Multi-purpose Legal Structure, and to support trust between the HIE and covered entities.

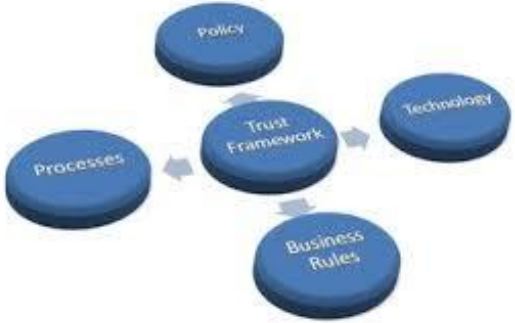
Source: Michigan Health Information Network Shared Services

CONNECTICUT
HEALTH INFORMATION
TECHNOLOGY OFFICE

Trust Agreements

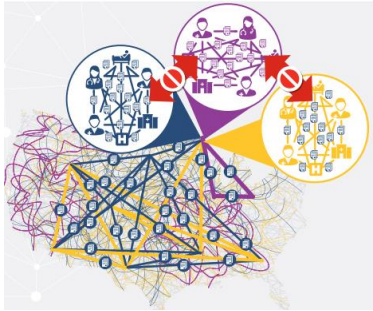
OHS CONNECTICUT
Office of Health Strategy

Trust Framework Purpose



- Common language, understanding, and agreement
- Promotes transparency, trust, and sharing
- Addresses requirements for data use and sharing among a variety of stakeholders
- Fairness
- Accountability
- Privacy & Security
- Minimized need for one-off trust agreements and contracts

Risk if Void a Common Trust



- Impact on data usage and interoperability
- Speed and efficiency scale our exchange efforts
- Healthcare organizations are currently burdened with creating many costly, point-to-point interfaces between organizations which are complex to create, provide oversight, stay in compliance, and maintain, and an inefficient use of provider and health IT developer resources
- Variations in the participation agreements that govern exchange
- No common method for authenticating trust health information network participants
- No common set of rules for trusted exchange
- Terms of non-compliance with an agreement vary, difficulty with oversight
- Many organizations have to join multiple Health Information Networks (HINs), and the HINs do not share data with each other

Roadblocks to a Single Agreement

- Federal Laws & Regulations
- Applicable / State Laws & Regulations
- Consent Models
- Local Policies and Procedures

Source: Johnson, et. al. (2016). Getting the Right Information to the Right Health Care Providers at the Right Time: A Road Map for States to Improve Health Information Flow Between Providers.

CONNECTICUT
HEALTH INFORMATION
TECHNOLOGY OFFICE

Trust Agreement Analysis

OHS CONNECTICUT
Office of Health Strategy

What is a Trust Agreement?

- Legal agreements that include Policies and Procedures, BAA's
- Multi-party agreement among participating HIEs that defines how the HIEs relate to each other
- Legal framework within which HIEs can exchange data electronically
- Assumes that each HIE has trust relationships in place with its participants

Trust Framework Analysis

State-Level

- Michigan (MiHIN)
- Massachusetts (Mass HIway)
- Rhode Island (CurrentCare)
- New York (SHIN-NY)
- Maine (HealthInfoNet)
- Delaware (DHIN)
- Maryland (CRISP)
- Virginia (ConnectVirginia)
- California (CAHIE)

National

- eHealth Exchange (eHEX), (The Sequoia Project)
- Carequality, (The Sequoia Project)
- Commonwell Health Alliance
- Trusted Exchange Framework and Common Agreement (TEFCA)

Major Components of a Trust Framework

- Purpose & Scope
  - Scope of Exchange
  - Approach to Establishing Trust
  - Governance Structure
  - Operational Policies/Procedures
- Permitted Purposes
- Permitted Participants
- Identity Proofing & Authentication
- Technical Approach and Infrastructure
  - Standards Used
- Cooperation & Non-Discrimination
- Allocation of Liability and Risk
- Accountability
  - Technical
  - Network Flow Down
  - Enforcement
  - Dispute Resolution
- Consent Model
  - States Consent Models
  - CT Consent Policy
- Transparency
- Privacy & Security
  - Breach Notifications
- Access

Key Differences Between Trust Agreements

- Consent Models
- Breach notification (time requirements)
- Participant Testing/certification/onboarding
- Types of policies and procedures that accompany the trust agreement
- Permitted Purposes
- Use Cases
- Trust agreements vary across end users and HINs forcing end users to join multiple HINs to share data
- Healthcare providers burdened with costs for point-to-point interfaces

CONNECTICUT
HEALTH INFORMATION
TECHNOLOGY OFFICE

Trust Exchange Framework and Common Agreement (TEFCA)

OHS CONNECTICUT
Office of Health Strategy

21st Century Cures Act

- Office of the National Coordinator for Health IT (ONC) has been working on the **Trusted Exchange Framework and Common Agreement (TEFCA) -** First Draft released January 5, 2018
- The common agreement includes:
  - A common method for authenticating trusted health information network participants;
  - A common set of rules for trusted exchange;
  - Organizational and operational policies to enable the exchange of health information among networks, including minimum conditions for such exchange to occur; and
  - A process for filing an adjudicating noncompliance with the terms of the common agreement.

Source: https://www.healthit.gov/sites/default/files/draft-guide.pdf

TEFCA

Why did Congress require the Trusted Exchange Framework?

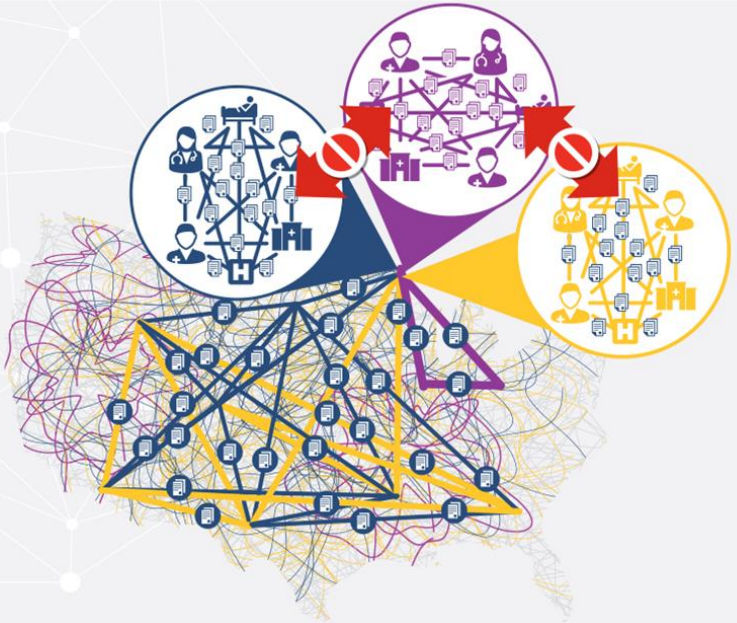
Need for the Trusted Exchange Framework – Complexity

Current Proliferation of Agreements

Many organizations have to join multiple Health Information Networks (HINs), and the HINs do not share data with each other.

Trusted exchange must be simplified in order to scale.

Each line color on the map represents a different network.
There are well over 100 networks in the U.S.



Source: https://www.healthit.gov/sites/default/files/draft-guide.pdf

Part A – Principles for Trusted Exchange

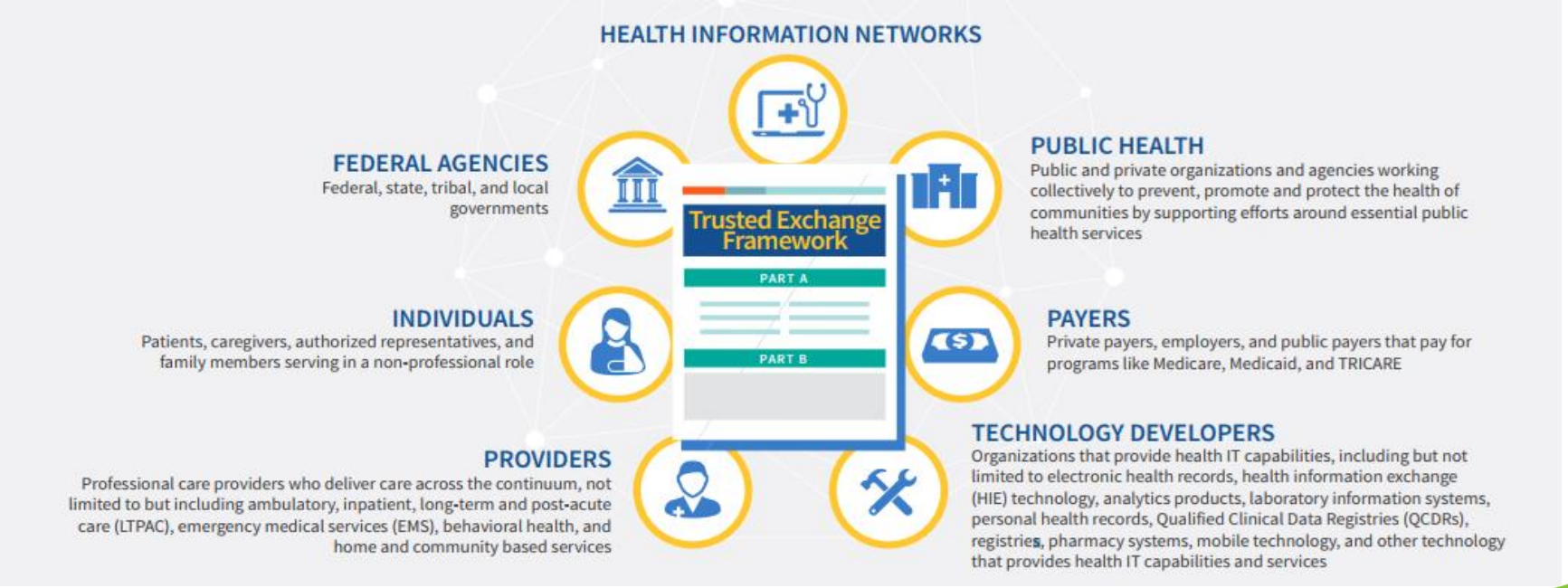
- Principle 1– **Standardization**: Adhere to industry and federally recognized standards, policies, best practices, and procedures
- Principle 2 – **Transparency**: Conduct all exchange openly and transparently
- Principle 3 – **Cooperation and Non-Discrimination**: Collaborate with stakeholder across the continuum of care to exchange electronic health information, even when a stakeholder may be a business competitor
- Principle 4 – **Security and Patient Safety**: Exchange electronic health information securely and in a manner that promotes patient safety and ensures data integrity
- Principle 5 – **Access**: Ensure that patients and their caregivers have easy access to their electronic health information
- Principle 6 – **Data-driven Accountability**: Exchange multiple records at one time to enable identification and trending of data to lower the cost of care and improve the health of the population

Source: https://www.healthit.gov/sites/default/files/draft-guide.pdf

Goals of the TEFCA

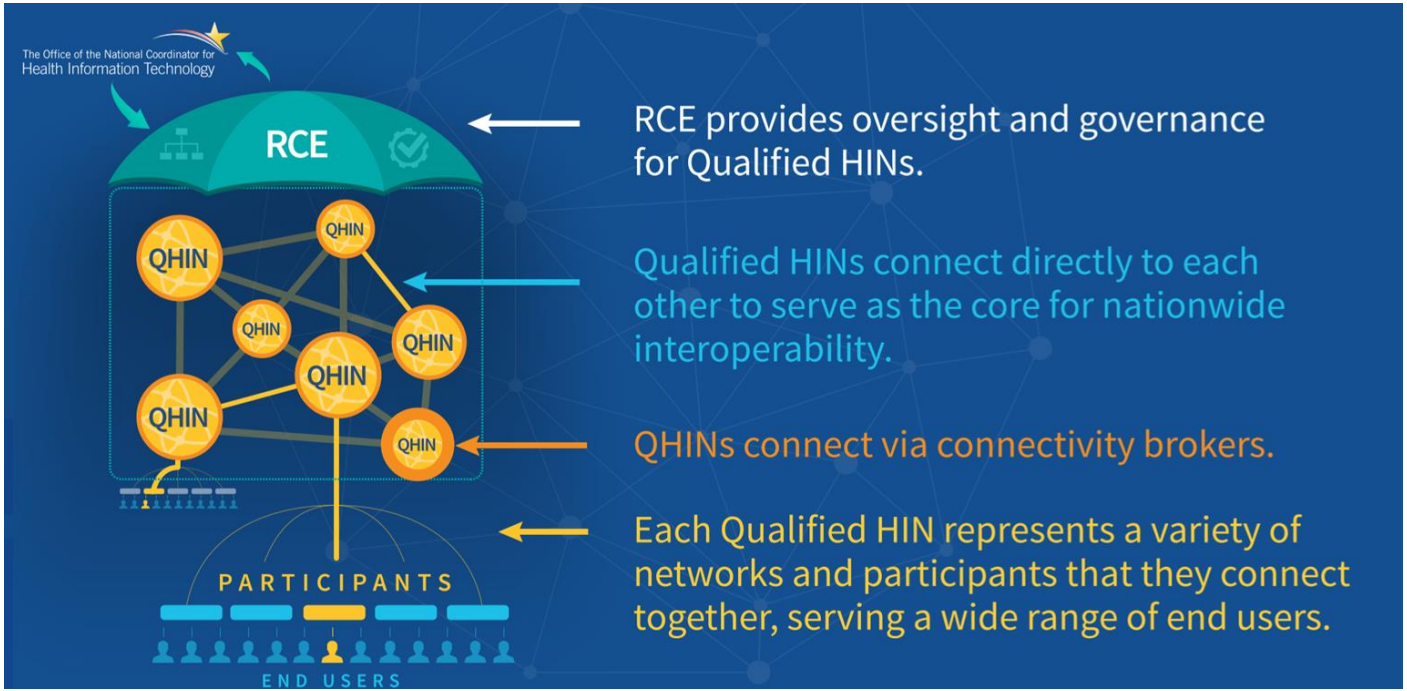
Source: https://www.healthit.gov/sites/default/files/draft-guide.pdf

Stakeholders Permitted to use TEFCA



Source: https://www.healthit.gov/sites/default/files/draft-guide.pdf

How will the Trusted Exchange Framework Work?

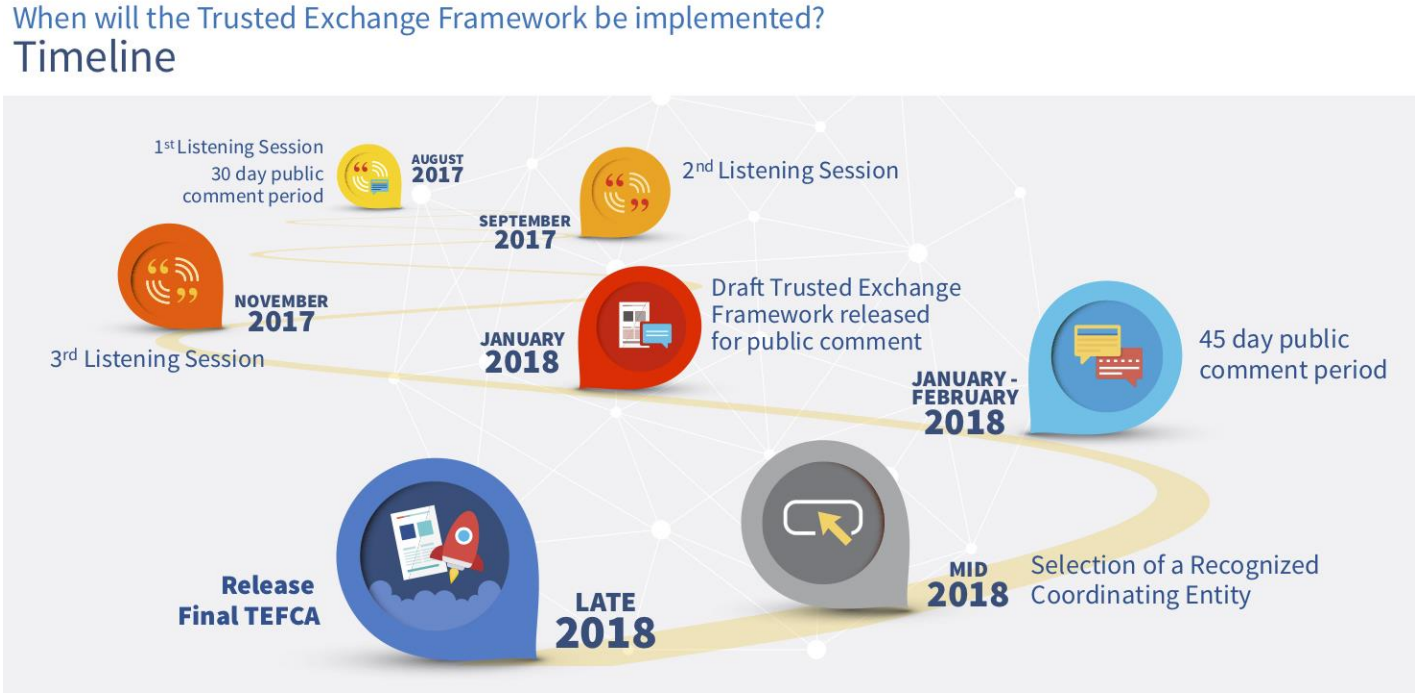


Source: https://www.healthit.gov/sites/default/files/draft-guide.pdf

TEFCA Permitted Purposes

Source: https://www.healthit.gov/sites/default/files/draft-guide.pdf

TEFCA Timeline



Source: healthit.gov

CONNECTICUT
HEALTH INFORMATION
TECHNOLOGY OFFICE

Federal Law, State Regulations & Legislation

Compliance with Applicable Federal Laws

- Health Insurance Portability and Accountability Act (HIPAA)
- Privacy Act
- Freedom of Information Act (FOIA)
- Family Educational Rights and Privacy Act (FERPA)
- Federal Torts Claims Act
- Federal Information Security Management Act

Health Insurance Portability and Accountability Act (HIPAA) 1996

- HIPAA ***does not*** create legal obstacles for sharing information through an HIE in that it ***does not require*** a covered entity to obtain member/patient consent prior to sharing or disclosing information with other covered entities through an HIE
- HIPAA ***contains exceptions*** that allow a covered entity to share information (without consent) for treatment, payment or healthcare operations
- The primary exception under HIPAA is the sharing of psychotherapy notes.
- There maybe consent requirements under other federal or state laws for “Sensitive” Data such as, behavioral health and substance abuse

HIPAA vs. State Law

- HIPAA preempts state laws that permit disclosure unless the state law is “more stringent” than HIPAA
- “More stringent” means the law provides a higher level of patient privacy protection
- HIPAA allows all disclosures required by state law
- Typical state law restrictions that go beyond HIPAA include laws governing genetic information, mental health records, substance abuse records, human immunodeficiency virus records, and informed consent
- These restrictions could lead to entire records being excluded from HIEs, as data-aggregating software used by HIOs does not always have the capability to redact only the sensitive information
- To combat these roadblocks, HIOs are working to:
  - Make granular data restrictions on the display of sensitive information
  - Engaging in lobbying and lawmaking efforts to soften certain state law restrictions that make HIE operation costly and burdensome

Source: https://www.mcguirewoods.com/news-resources/publications/health_care/HIT-News-April2014.pdf; https://www.hhs.gov/hipaa/index.html; https://www.hhs.gov/hipaa/index.html

Connecticut Statutes

- Disclosure of personally identifiable information by state agencies to the Connecticut Health Information Network - Conn. Gen. Stat. § 19a-25f
  - State agency participants in the Connecticut Health Information Network "may disclose personally identifiable information held in [their] databases to the administrator of the Connecticut Health Information Network and its subcontractor" in order to develop the network. Such disclosure must occur in compliance with state and federal laws (e.g. HIPAA and FERPA)
- Availability of patient information to certain agencies - Conn. Gen. Stat. § 17b-225
  - The Department of Public Safety, Department of Social Services, and the U.S. Department of Health and Human Services ("Departments") may access patient information from hospitals and facilities operated by the Department of Public Health, Department of Development Services, and Department of Mental Health and Addiction Services ("Agencies") to the extent that the information is necessary to pay for patient care, claim federal reimbursement, or conduct an audit of federally funded programs.
- APCD Statute Public Act No. 12-166
  - Allows for data in APCD to be available to any state agency, insurer, employer, health care provider, consumer of health care services, researcher or the Connecticut Health Insurance Exchange for the purpose of allowing such person or entity to review such data as it relates to health care utilization, costs or quality of health care services. Disclosure of APCD data shall be made in a manner to protect the confidentiality of health information, as defined in 45 CFR 160.103, and other information, as required by state and federal law (e.g., HIPAA, ERISA). Access to de-identified data or limited data set requires application for data, data use agreement, waiver, etc.
- Data submission requirements - Conn. Gen. Stat. § 19a-654
  - Short-term acute care general and children's hospitals must submit data to the Office of Health Care Access that the Office deems necessary to carry out their duties. Required data must include medical record abstracts and hospital bills. The Office must maintain the confidentiality of patient and physician data, but may release de-identified aggregate reports to the public.

Connecticut Statutes Continued

- Data submission requirements for the Office of Health Care Access (OHCA) - Conn. Gen. Stat. § 19a-654
  - The **[**office**]** unit may release patient-identifiable data (1) for medical and scientific research as provided for in section 19a-25-3 of the regulations of Connecticut state agencies, and (2) to (A) a state agency for the purpose of improving health care service delivery, (B) a federal agency or the office of the Attorney General for the purpose of investigating hospital mergers and acquisitions, or (C) another state's health data collection agency with which the **[**office**]** unit has entered into a reciprocal data-sharing agreement for the purpose of certificate of need review or evaluation of health care services, upon receipt of a request from such agency, provided, prior to the release of such patient-identifiable data, such agency enters into a written agreement with the **[**office**]** unit pursuant to which such agency agrees to protect the confidentiality of such patient-identifiable data and not to use such patient-identifiable data as a basis for any decision concerning a patient. **No individual or entity receiving patient-identifiable data may release such data in any manner that may result in an individual patient, physician, provider or payer being identified. The [office] unit shall impose a reasonable, cost-based fee for any patient data provided to a nongovernmental entity.**

Critical Factors for Success in Connecticut

- Support of Statutes – Statutory Agreement on Consent
- State Statutes not incompatible with Trust Framework Objectives
- Framework practical and fair – supports participation
- Data Compatibility with bidirectional statutes
- Stakeholders (patients/consumers, providers, payors, state agencies, etc.,) engagement, support, and participation
- Sustainability Model

References

Johnson, K., Kelleher, C., Block, L., & Isasi, F. (2016). ***Getting the Right Information for the Right Health Care Providers at the Right Time: A Road Map for States to Improve Health Information Flow Between Providers.*** Washington, DC: National Governors Association Center for Best Practices.

Covich, J., Jones, D., Morris, G., & Bates, M. (2011). ***Governance Models for Health Information Exchange.*** Truven Health Analytics.

https://www.healthit.gov/sites/default/files/draft-guide.pdf

https://dashboard.healthit.gov/apps/state-health-it-privacy-consent-law-policy.php

https://www.cga.ct.gov/

https://www.healthit.gov/sites/default/files/draft-trusted-exchange-framework.pdf

https://www.healthit.gov/sites/default/files/july24trustedexchangeframework.pdf; https://www.cga.ct.gov/current/pub/chap_669.htm#sec_36a-701b

https://www.healthit.gov/sites/default/files/State%20HIE%20Opt-In%20vs%20Opt-Out%20Policy%20Research_09-30-16_Final.pdf

https://truvenhealth.com/portals/0/assets/GOV_11558_0712_HIE_Governance_WP_WEB.pdf

Public Health Data Standards Consortium. "Data Standards." Health Information Technology Standards. 2013. http://www.phdsc.org/standards/health-information/d_standards.asp

https://www.hln.com/knowledge/interoperability-standards/

https://www.healthit.gov/

http://www.datagovernance.com/defining-data-governance/

Healthcare IT News

https://www.hhs.gov/hipaa/index.html

https://www.mcguirewoods.com/news-resources/publications/health_care/HIT-News-April2014.pdf

https://www.healthcare-informatics.com/blogs/david-raths/interoperability/what-will-tefca-mean-regional-hies

Contact Information

Health Information Technology Program Management Office

Allan Hackney, Allan.Hackney@ct.gov

Sarju Shah, Sarju.Shah@ct.gov

Kelsey Lawlor, Kelsey.Lawlor@ct.gov

M.J. Lamelin, MaryJane.Lamelin@ct.gov

Jennifer Richmond, Jennifer.Richmond@ct.gov

Dino Puia, Dino.Puia@ct.gov

Grace Capreol, Grace.Capreol@ct.gov

General E-Mail, HITO@ct.gov

CedarBridge Group

Michael Matthews, michael@cedarbridgegroup.com

Chris Robinson, chris@cedarbridgegroup.com

Health IT Advisory Council Website:
http://portal.ct.gov/Office-of-the-Lt-Governor/Health-IT-Advisory-Council

Please direct all questions to Jennifer Richmond