The Office of the National Coordinator for Health Information Technology

21st Century Cures Act
Trusted Exchange Framework and Common Agreement
Kick-Off Meeting

Monday, July 24, 2017
9:30 am – 4:30 pm
Hubert H. Humphrey Auditorium

The Office of the National Coordinator for Health Information Technology

21st Century Cures Act
Trusted Exchange Framework and Common Agreement Kick-Off Meeting

WELCOME and INTRODUCTIONS

Donald Rucker, MD
National Coordinator, ONC

The Office of the National Coordinator for Health Information Technology

21st Century Cures Act Trusted Exchange Framework and Common Agreement Kick-Off Meeting

21st Century Cures Act Overview

Elise Sweeney Anthony, J.D.
Director, Office of Policy, ONC

21st Century Cures Act

- **Title IV – Delivery:**
  - Section 4001: Assisting Doctors and Hospitals in Improving Quality of Care for Patients (*Burden Reduction strategy, Specialty certification*)
  - Section 4002: Transparent Reporting on EHR Transparency, Usability, Security, and Functionality (*EHR Significant Hardship, Conditions of Certification, EHR Reporting Program*)
  - **Section 4003: Transparent Reporting on EHR Transparency, Usability, Security, and Functionality - Interoperability** (***Trusted Exchange Framework and Common Agreement***, *Health IT Advisory Committee, Provider digital contact information index*)
  - Section 4004: Information Blocking
  - Section 4005: Leveraging EHRs to Improve Patient Care (*registry/EHR information*)
  - Section 4006: Empowering Patients and Improving Patient Access to Electronic Health Information
  - Sections 4007, 4008: GAO Studies on Patient Matching, Patient Access to Health Information

Trusted Exchange Framework and Common Agreement

"Not later than 6 months after the date of enactment…the National Coordinator shall convene appropriate public and private stakeholders to develop or support a trusted exchange framework for trust policies and practices and for a common agreement for exchange between health information networks. The common agreement may include –

> **"(I) a common method for authenticating trusted health information network participants;**
>
> **"(II) a common set of rules for trusted exchange;**
>
> **"(III) organizational and operational policies to enable the exchange of health information among networks, including minimum conditions for such exchange to occur; and**
>
> **"(IV) a process for filing and adjudicating noncompliance with the terms of the common agreement.**

21st Century Cures Act - Section 4003(b)

Kick-Off Meeting Overview

- National Trust Frameworks and Network-to-Network Connectivity
  - Carequality – Dave Cassell
  - CARIN Alliance – Ryan Howells
  - CommonWell – Jitin Asnaani
  - Digital Bridge – Walter Suarez
  - DirectTrust – David Kibbe
  - DirectTrust – David Kibbe
  - NATE – Aaron Seib
  - SHIEC – David Kendrick, Richard Thompson
- Personal Perspective of Interoperability
- Panel Discussion and Audience Questions and Answers
- Alignment and Gaps Among Current Trust Agreements
- Public Comment (In Person and via Webinar)
- Going Forward

The Office of the National Coordinator for Health Information Technology

Thank You

Elise Sweeney Anthony , J.D.
Director, Office of Policy

Elise.Anthony@hhs.gov

@ONC_HealthIT HHSONC HealthIT.gov

The Office of the National Coordinator for Health Information Technology

21st Century Cures Act
Trusted Exchange Framework and Common Agreement
Kick-Off Meeting

National Trust Frameworks and Network-to-Network Connectivity

Carequality

Overview

Carequality is a national-level interoperability framework developed by public and private stakeholders for trusted exchange between and among health information networks

- Leverages existing investments to efficiently increase interoperability nationwide using:
  - A common set of rules and policy requirements for trusted exchange
  - A process for resolving disputes and questions of non-compliance with terms of the agreement
  - Technical specifications for each supported use case
  - Operational services for certificates and participant directory
- Framework and agreement are deliberately independent of specific architecture or data type, use cases
  - Current use includes clinical documents and patient-generated data.
  - Future use includes notifications, FHIR resources, images, and more

Participation

Carequality Implementers To-Date

HIEs

- Coordinate Care Health Network
- HIE Texas
- MiHIN
- Santa Cruz HIE
- Sun Coast RHIO

Technology Vendors

- athenahealth
- eClincalWorks
- Epic
- GE Healthcare
- Glenwood Systems
- Medicity
- Netsmart
- NextGen Healthcare

Service Providers

- Common Well Health Alliance
- Kno2
- Inovalon
- Mana Health
- Surescripts

PHRs

- Azuba
- Cartus Health
- OneRecord
- Womba

Exchange Metrics

- 2M Clinical Documents Exchanged in 1 year
- 260,000 Physicians
- 865+ Hospitals
- 23,000 Clinics

Carequality Community

- Physicians
- Consumers
- Government
- Public Health
- Vendors
- Data Sharing Networks
- Payers
- Behavioral Health
- Acute Care
- Hospice
- SDOs
- Pharmacies
- Long Term/ Post-Acute Care
- EMS Services

Support

Carequality was designed from its inception to serve as a framework for existing networks and services to connect their members to one another.

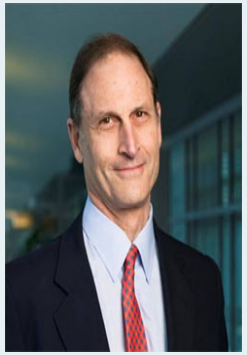
- Each participant knows its rights and obligations, and can trust that it understands the rights and obligations of all other participants.
- Technical specifications ensure that for each use case, participants can "speak a common language".
- Operational support in the form of certificate services and a participant directory combine with the other elements to allow each organization to ***implement once, and connect universally***.
- Accommodates independent and competing service offerings
  - e.g. Record Locator Services

CARIN Alliance

CARIN Overview

Creating Access to Real-time Information Now through Consumer-Directed Exchange

www.carinalliance.com
@carinalliance


David Blumenthal


David Brailer


Aneesh Chopra

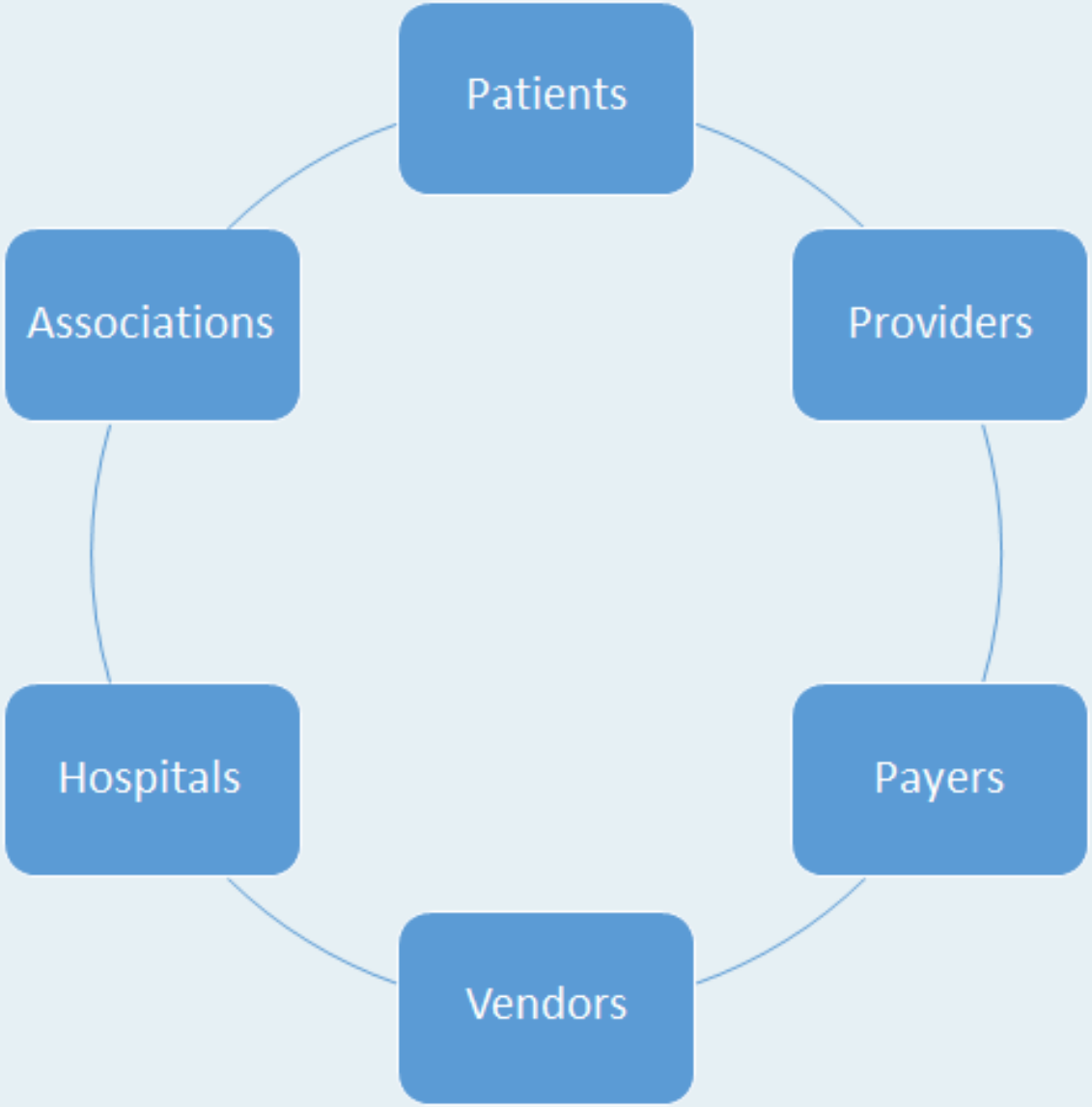

Mike Leavitt

VISION

To rapidly advance the ability for consumers and their authorized caregivers to easily get, use, and share their digital health information when, where, and how they want to achieve their goals.

CARIN Participants

Creating Access to Real-time Information Now through Consumer-Directed Exchange



CARIN Use Cases

Creating Access to Real-time Information Now through Consumer-Directed Exchange

Eliminate the business and policy barriers associated with the implementation of the FHIR APIs

CARIN Trust Framework

Creating Access to Real-time Information Now through Consumer-Directed Exchange

The CARIN Alliance has developed a document that lays out an open standards framework regarding the best practices and principles for consumer-directed exchange.

- The document is constructed to provide a set of tools for consumers, their authorized caregivers, covered entities, and third-party data stewards or applications to use to help implement digital consumer-directed exchange and includes the following sections:
  - A set of consensus-driven, industry guiding principles for trusted consumer-directed data exchange
  - Major topics related to consumer-directed exchange including questions industry feels needs to be addressed
  - Within each major topic, use cases that provide best practices for organizations who are facilitating consumer-directed data exchange

12 Trust Framework Principles

Creating Access to Real-time Information Now through Consumer-Directed Exchange

The Consumer – Our Governing Principle

- **Consumers Right to Access, Store, Share and Use:** Consumers or their authorized caregivers have a right to access, share and receive their available digital health information. They can provide access to any third-party data steward they authorize. The digital health information will be provided in any readily producible format they request, in as close to real-time as feasible, and at no cost.

Principles for Covered Entities

- **Access for consumers.** Covered entities have a responsibility to provide consumers or their authorized caregivers access to share their available digital health information with any third-party data steward when a consumer invokes their individual right of access.
- **Consumer authentication.** Covered entities authenticate the identity of the consumer or authorized caregiver requesting access to their digital health information before providing access.

12 Trust Framework Principles

Creating Access to Real-time Information Now through Consumer-Directed Exchange

Principles for Data Stewards including third-party applications and EMR/HIT vendors

This applies only to data stewards which are third-party applications provided by non-covered entities

- Openness and transparency
- Purpose specification
- Use limitation
- Data quality and integrity
- Security safeguards and controls
- Accountability and oversight
- Remedies
- Endorsement and Certification
- Openness and completeness of data sharing

Trust Framework Topics

Creating Access to Real-time Information Now through Consumer-Directed Exchange

Technology, Certification, Registration

- Consumer Identification
- Standards and Technology
- Registering Applications
- Certifications and Endorsements

Privacy and Security

- Privacy and Security Policies
- Limitations on Use and Sharing
- Establishing Conformance
- Accountability and Oversight

Consumer Access and Education

- Define Types of Entities
- Individual Right of Access Requests
- Consumer and Data Holder Education

CommonWell Health Alliance

Overview

- Description of CommonWell Health Alliance:
  - CommonWell Health Alliance is an independent, not-for-profit trade association
  - Our Vision is that (1) health data should be available to individuals and providers regardless of where care occurs, and that (2) access to this data must be built-in to HIT at a reasonable cost for use by a broad range of health care providers and the people they serve
  - To achieve this Vision, we have built and coalesced enabling infrastructure, services, policies, and governance
- Description of Exchange Services provided by CommonWell:
  - Today, CommonWell services are utilized for query/retrieve (“pull”) of person-centered data for the purposes of treatment and direct patient access:
    - Integrated Master Patient Index (MPI) + Record Locator Service (RLS) + Brokered Query that simplifies the user experience and eliminates point-to-point interfaces.
    - MPI+RLS grow smarter with usage and with end-user input.
    - Brokered query creates vendor and provider simplicity by fanning out requests and bundling the responses.
    - Focus on a “built in” approach with our user-facing vendor Members (EHRs, etc.)
    - Transparent integration with other interoperability modes, e.g., directed query with Carequality Implementers

Overview continued

- Participation in the CommonWell trust framework:
  - CommonWell Membership:
    - Is open to all organizations who share our vision.
    - Enables participation in the Alliance as an entity that facilitates collaboration around functional use cases and technical specifications.
    - Is currently largely driven by EHR and HIT vendors, serving 20+ care settings.
    - Also includes leading private data sharing networks, systems integrators, federal agencies, state authorities/HIEs, and other mission-driven interoperability non-profit organizations.
  - To access services, a CommonWell Member (e.g., an HIT vendor) "Subscribes" to CommonWell Services and enables its clients (i.e., end-users) to access those services through the HIT vendor's products.
    - The Subscriber passes through a set of End User Terms and Conditions encapsulated by a EULA that is included in the Member Services Agreement ("MSA"); the Alliance is a Business Associate of the Member, thus creating a trust fabric among all network participants.

Overview continued

- Exchange metrics as-of July 1, 2017:
  1. # of nodes (clinical sites) committed or live on the network: 8,488
  2. # of nodes already live on the network: 5,441

  3. # of non-distinct patient records in our database: 53,693,251
  4. # of enrolled (unique) individuals accessible: 17,609,390, growing at ~900K monthly
  5. # cross-vendor linked individuals: 1,199,599

  6. # queries sent by nodes: 98,557,091
  7. # of documents available from nodes for those queries: 7,703,213
  8. # of documents retrieved/viewed by the end-user for those queries: 105,148

  - Note that:
    - Note that CommonWell has been live since spring 2015.
    - All patient, query and document metrics (#3-#8) grew 10-75x over last year.

Overview continued

- CommonWell is creating pathways towards greater and more valuable interoperability within the network
  - Uniquely creates person-centered query & retrieve fabric today.
  - Introducing new services to query on a location-centric basis (“directed query”) and to proactively notify caregivers of clinical encounters.
  - Introducing new data usage models, e.g., optional (i.e., end-user opt-in/opt-out) models for population-based/bulk data exchange, data exchange for disability/life insurance coverage, etc.
  - Enabling other modes of interoperability through Network-Network agreements, e.g., Directed Query and (optionally) RLS-based exchange through our agreement with Carequality; other modes supported by other initiatives, frameworks and networks.

Overview continued

- CommonWell supports the goal of broader nationwide interoperability
  - Within the Alliance, the governance framework ensures representation and broad participation of industry stakeholders.
    - Formal documents and processes: ByLaws; Membership Agreement (obligations as Members, IP Contribution requirements/constraints, etc.); Use Case governance process; policy guidance; a non-discriminatory Member Services Agreement (obligations of Alliance, Subscribers and Service Providers; data usage obligations/restrictions; privacy & security policy; BAA; SLAs; EULA; etc.).
    - Established and evolving structures for participation: Board of Directors, Functional Committees, Workgroups, Advisory Committees.
  - Outside the Alliance, CommonWell supports organizations and initiatives with complementary missions:
    - Public endorsement of initiatives by CHIME, HIMSS, NATE, RSNA, The Sequoia Project, etc.
    - Membership in HIMSS, HL7, NATE, eHealth Initiative, and others.
    - Adoption and promotion of standards from HL7, IHE, W3C, and the Argonaut Project.

Digital Bridge

Overview

- Digital Bridge is a collaboration between health care, public health, and health information technology organizations to ensure our nation's health through improved information sharing across sectors.
- As its first project, the Digital Bridge has designed a nationally scalable, multi-jurisdictional approach to electronic case reporting (eCR). Objectives include:
  - improved public health surveillance of infectious diseases
  - decreased burden on providers for meeting public health reporting requirements
  - bidirectional information flow between providers and public health

Overview continued

- Participants (Governance):
  - Health care: HealthPartners, Kaiser Permanente, Partners HealthCare
  - Health IT: Allscripts, Cerner, eClinicalWorks, Epic, Meditech
  - Public health: ASTHO, APHL, CDC, CSTE, NACCHO
  - Funding: Robert Wood Johnson Foundation, de Beaumont Foundation
  - Project Management: Public Health Informatics Institute, Deloitte
- Exchange metrics
  - Initial electronic case reporting (eCR) implementation sites recruited (next slide)
  - Exchange will utilize a cloud-based decision support intermediary hosted by APHL

eCR Site Participation

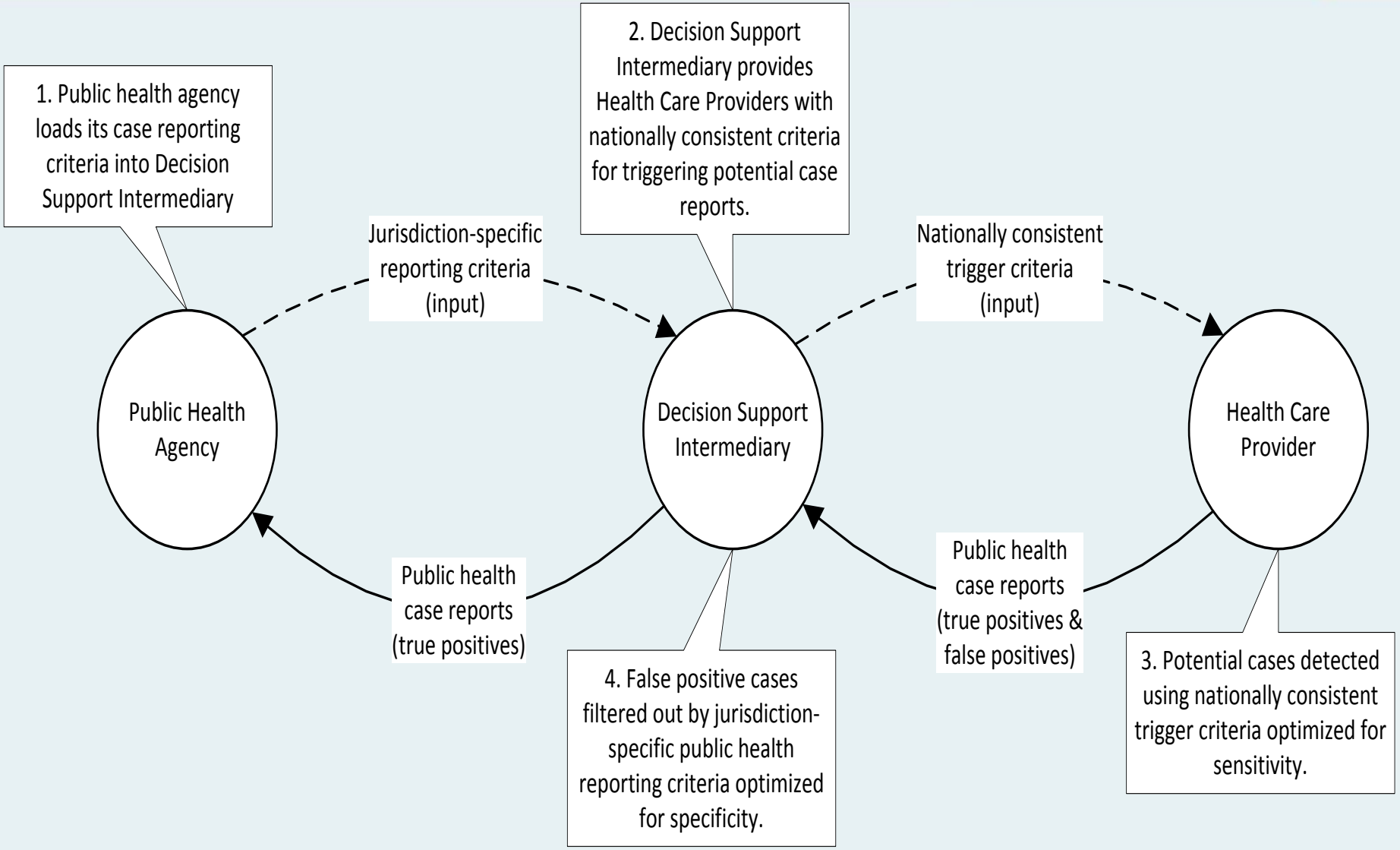
Wave 1

Public Health Agency	Health Care Provider	EHR Vendor
Kansas	Lawrence Memorial Hospital	Cerner
Michigan	a) Local Public Health Clinics b) McLaren Health Center	a) NetSmart b) HIE-MiHIN
Utah	Intermountain Healthcare	Cerner

Wave 2

Public Health Agency	Health Care Provider	EHR Vendor
California	UC Davis	Epic
Houston	Houston Methodist	Epic
Massachusetts	Partners HealthCare	Epic
New York City	Institute of Family Health	Epic

eCR Overview



Overview continued

- How does your organization support interoperability?
  - Use existing standards where they exist,
    - eCR uses new HL7 standard for 1) Public Health Case Report R2 and 2) Reportability Response
  - Recommend new standards where they don't exist

- What additional services, policies, infrastructure, etc. does your organization provide to do so?
  - Digital Bridge provides governance structure to facilitate collaborative decision-making between health care, public health, and health IT
  - Decisions include: use cases to prioritize, recommendations for technical implementation and standards development
  - Digital Bridge plans on adopting trusted framework to facilitate data exchange between health care providers and state/local public health agencies

The Office of the National Coordinator for Health Information Technology

BREAK

15 Minute Break

Meeting will Resume at 11:00 am

@ONC_HealthIT HHSONC HealthIT.gov

The Office of the National Coordinator for Health Information Technology

21st Century Cures Act
Trusted Exchange Framework and Common Agreement
Kick-Off Meeting

National Trust Frameworks and Network-to-Network Connectivity

DirectTrust

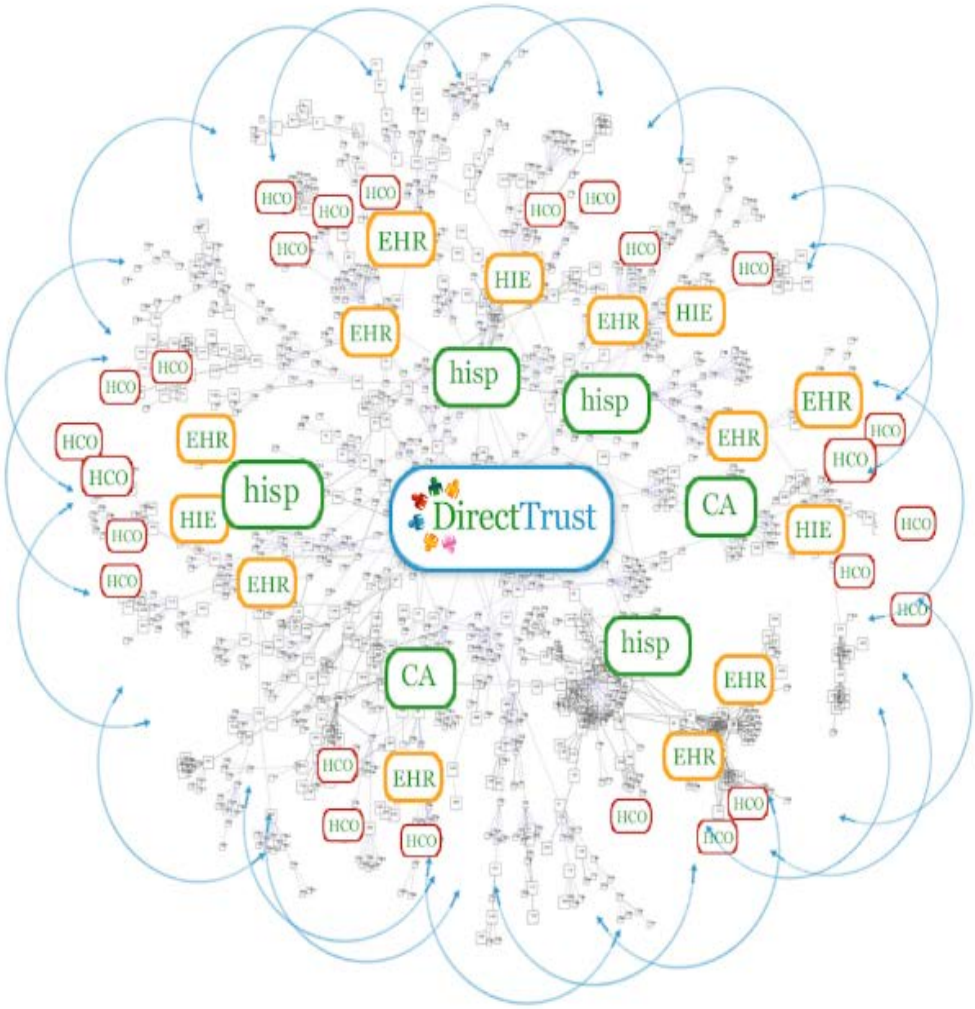
DirectTrust Overview

DirectTrust is a product of an ONC-private sector collaboration known as the Direct Project, created in 2010 to provide secure, interoperable, health information exchange among providers and patients. DirectTrust received a Cooperative Agreement from ONC from 2013-15.

The Direct standard is required to be implemented in all ONC-certified health IT products, including EHRs, and use of Direct message+attachments for transitions of care and referrals is encouraged in the Meaningful Use programs.

The DirectTrust network has roughly doubled each year since 2012, and now reaches almost all health care organizations whose providers have engaged in MU stage 2.

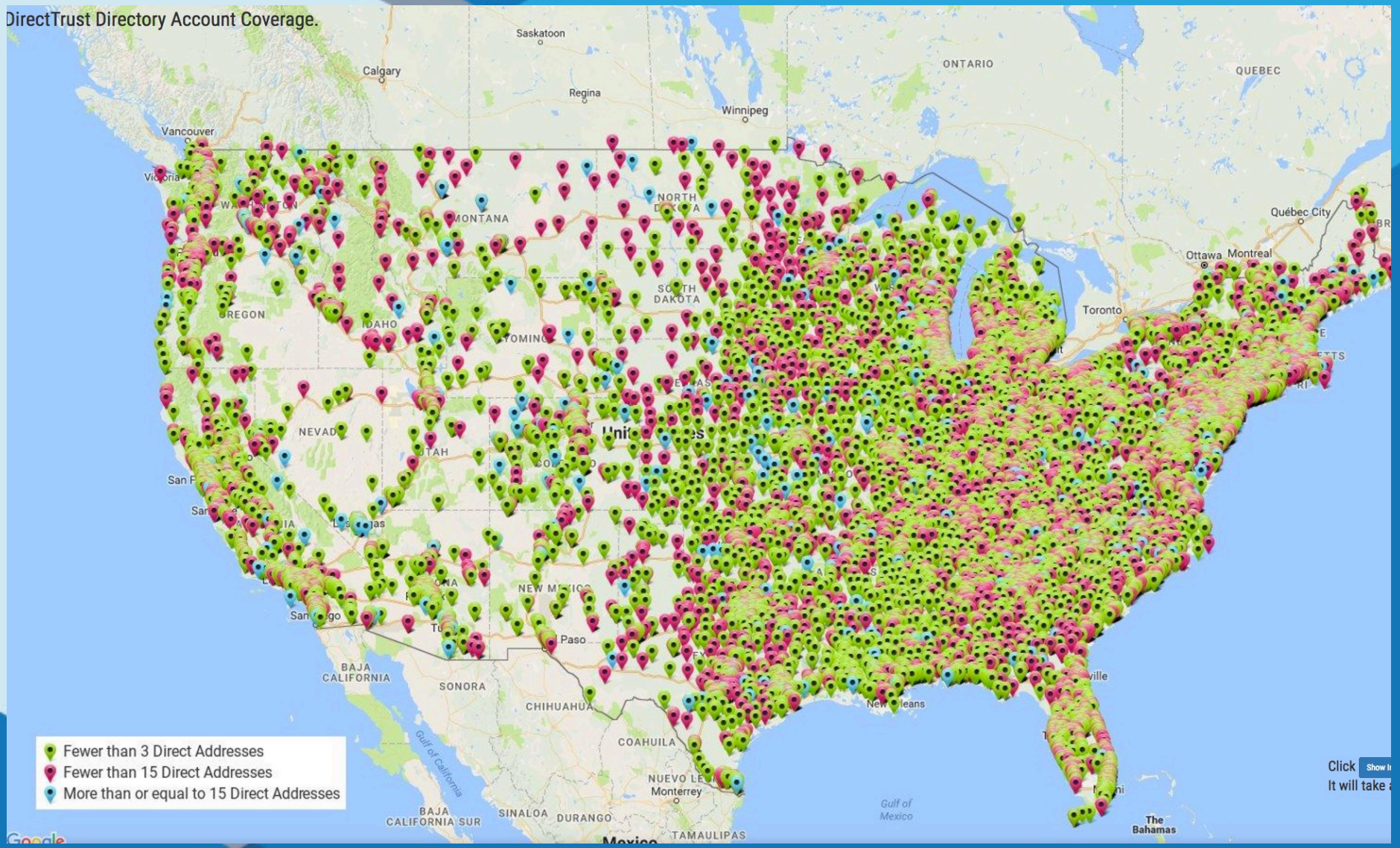
DirectTrust's Network: A National Platform for Secure Interoperable Exchange of PHI



The DirectTrust Network

- 40 HISPs, 15 CAs
- 400+ Direct-enabled, ONC certified EHRs & PHRs
- 100,000+ trusted health care organizations
- 1.5 million trusted Direct addresses
- 50+ HIEs in 20 states
- 2 Federal Agencies
- 67 million transactions in 2015, 98 million in 2016
- Adding 1 million+ transactions per month in 2017
- Estimated 130 million in 2017

DirectTrust's Network has 1.5 million Trusted Endpoints -- Direct addresses -- Supported by its Trust Framework



DirectTrust Trust Framework Description

- DirectTrust's Trust Framework is a dynamic and voluntary technical and human system, involving legal, policy, infrastructural and governance components.
- The primary purpose of the Trust Framework is to instill confidence in the security and identity controls all parties apply to their roles in exchange.
- The Trust Framework "scales" trust by making it unnecessary for relying parties to negotiate one-off agreements for trust. It creates a "network of trust."
- At the heart of DirectTrust's Trust Framework is its Public Key Infrastructure, PKI.

DirectTrust PKI Details

- A **Public Key Infrastructure** (**PKI**) is a set of rules, roles, policies, standards and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
- The DirectTrust PKI permits X.509 digital certificates bound to Direct addresses to assert that ID proofing of individual end-users has been performed at a high level of assurance, NIST Level 3 or higher.
- DirectTrust certificates are also used for encryption/decryption of Direct messages and attachments, and to sign the Direct package to ensure integrity of the contents during exchange.

Security and Trust Framework Details

- Federated Services Agreement, FSA
- Certificate and HISP Policies and Practices
- Accreditation and Audit Programs for Service Providers
- Public Key Infrastructure, PKI, for Identity Verification of all Participants in DirectTrust Network
- Standard Operating Procedure, SOP, documents for Trust Bundle inclusion
- Trust Anchor Bundles and operations
- Governance via collaboration, testing, enforcement, remediation, and legal contract

eHealth Exchange

eHealth Exchange Overview

eHealth Exchange Overview

- Public-private health information exchange network
- Developed by government and industry, supported by ONC
- 8 Years of exchange (primarily query and push)
- Enables federal agencies to share data between agencies and with private sector
- Federated-approach that does not depend on a technology or data hub

Types of exchange Supported

- Treatment/ Care Coordination
- SSA Benefits Determination
- Immunization
- Consumer Access to Health Info
- Encounter Alerts
- Prescription Drug Monitoring Program (PDMP)
- Electronic Lab Reporting for Public Health
- Syndromic Surveillance
- Life Insurance Determination

Dynamic legal agreement and governance can adopt additional use cases as market need arises

eHealth Exchange™ 8 Years of Exchange

Participants

More than 160+ exchange partners including:

- 4 Federal Government Agencies
- 65% of U.S. Hospitals
- 50,000+ Medical Groups
- 8,300+ Pharmacies
- 3,400+ Dialysis Centers
- 46 Regional / State HIEs

Exchange metrics*

eHealth Exchange support **109M patients**

Just one federal agency estimates **2 million exchanges** a month.

*Metrics are self-reported due to the federated nature of the network.

Supporting Interoperability

How eHealth Exchange supports interoperability:

- Enables de-centralized, federated exchange between signees of the DURSA
- Actively governed by Committee network participants
- Centralized security model based on X.509 digital certificates

Additional eHealth Exchange services:

- Healthcare directory of approved technical end points
- Onboarding Support – Due diligence, planning, etc.
- Testing – Security, transport, content (CCDA), "validated product"
- Performance Monitoring – Assessing system up time
- Security Testing – Verifying proper configuration of the x.509 certificate
- Specifications/ Technical Support – Interpretation, SME work
- Work Groups

Additional services as market need arises

What is DURSA?

The Data Use and Reciprocal Support Agreement (DURSA) is a comprehensive, multi-party trust agreement that:

- Establishes participants' obligations, responsibilities and expectations
- Creates a framework for safe and secure health information exchange
- Promotes trust among participants
- Expects participants comply with applicable law
- Protects the privacy, confidentiality and security of the health data that is shared
- Assumes that each participant has trust relationships in place with its agents, employees and data connections
- Evolves as a living document and modified over time

eHealth Exchange DURSA

Key Elements of the DURSA

- Governance
- Clear requirements applicable to all participants
- Uniform privacy and security obligations
- Equitable data sharing
- Exchange only for a permitted purpose
- Respect for local policies
- Future use of data received from another participant
- Well-defined technical specifications
- Participant directory
- Incident response and notification requirements
- Accountability
- Mechanism for updating agreement as legal and policy changes dictate

The agreement is flexible and can be easily revised by reference to technical specs, polices, and procedures as needed.

NATE

Overview

NATE NATIONAL ASSOCIATION FOR TRUSTED EXCHANGE

nate-trust.org

The **National Association for Trusted Exchange** (NATE) is a not-for-profit membership association focused on facilitating consumer access to information and enabling trusted exchange among organizations and individuals with differing regulatory environments and exchange preferences.

NATE is a 501(c)(3) mission driven organization focused on enabling trusted exchange that includes the patient. NATE's membership is open to government entities, non-government organizations, associations and individuals.

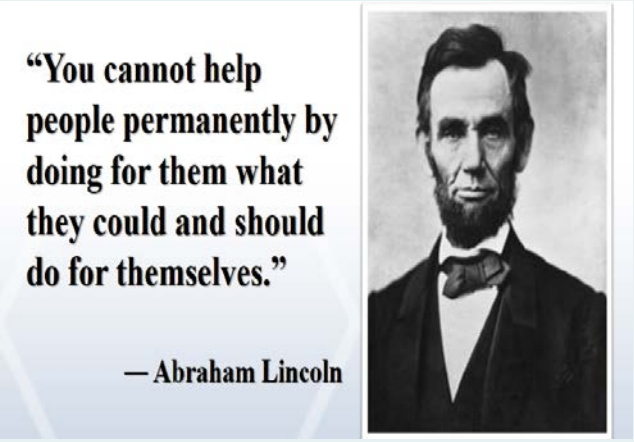
Overview

Consumer Directed Exchange

Consumer directed exchange provides patients with access to their health information, allowing them to manage their healthcare online in a similar fashion to how they might manage their finances through online banking.

When in control of their own health information, patients can actively participate in their care coordination by:

- Bringing their health information to new providers
- Identifying and correcting wrong or missing health information
- Identifying and correcting incorrect billing information
- Tracking and monitoring their own health



Overview

Providers

- CEs must comply with HIPAA
- CEs constrained to permitted purposes of use
- CEs spend 95% of their time working with health data
- …
- Direct functionality

Consumers

- CCAs must comply with FTC regulation
- Consumers can do anything they want with their data
- Consumers spend less than 5% of their time with health data
- …
- Direct functionality

HealthVault · carebox · omedix · MEDYEAR · humetrix · MediPortal (your gateway to better health, BETA) · iShare MEDICAL (innovating the future of healthcare) · NoMoreClipboard.com (easy. accurate. secure) · WOMBA (powered by me) · Get Real Health

The **NATE Blue Button for Consumers** (NBB4C) Trust Bundle is a trust mechanism that provides, to HIPAA covered entities that use Direct, a facile method of exchange with **Consumer Controlled Applications** that must meet or exceed a specific set of evaluation criteria and user experience requirements in order to become a NATE-Qualified Entity.

The NBB4C makes it easier for providers and consumers to trust consumer applications and easier for consumers to use them.

Overview continued

- Exchange metrics

The correct metric is: *"What percentage of Americans have access to their data from all of their providers?"*

- It's not about total exchange volume
- What matters to people is can I fetch my data when I need it in the form and format that I can use?

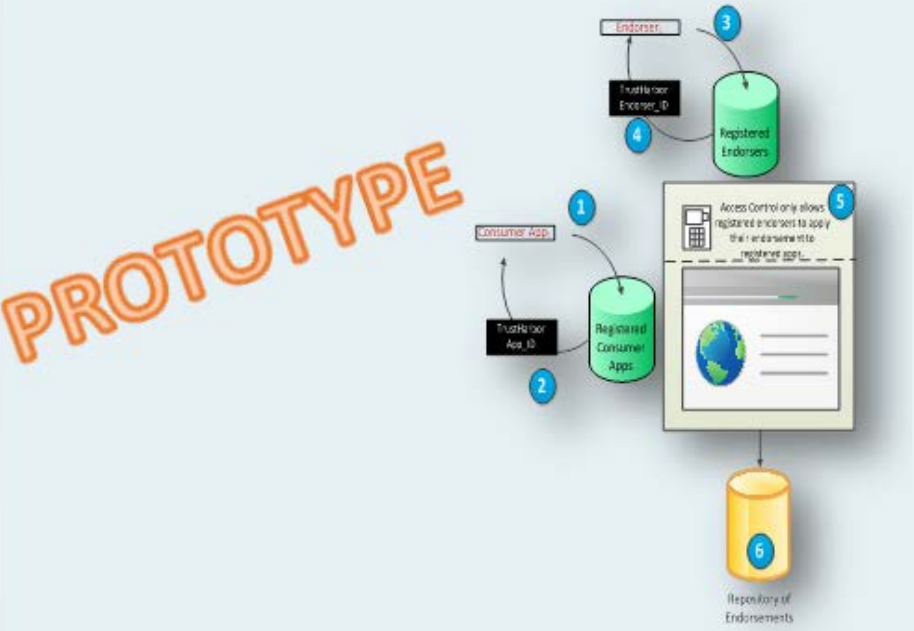
Overview continued

The **National Association for Trusted Exchange** (NATE) is a national non-profit organization focused exclusively on reducing the barriers that inhibit a consumer's access to their health information. NATE has found that sponsoring the development of lightweight trust mechanisms that sit at critical interoperability intersections is one of the most effective ways to realize the intent of applicable law. NATE is an independent, trusted and technology-agnostic convener of interested stakeholders that operates enabling infrastructure for scalable methods of consumer centered data exchange.

NATE has been operating its own trust community since 2012, and since that time, NATE has been enabling HIPAA covered entities (CEs) to compliantly share protected health information with consumers using the app of their choice. NATE will continue to serve as a trusted third party, overseeing trust transactions between CEs and consumers via multiple protocols, including Direct secure messaging and FHIR APIs.

Overview continued

TrustHarbor



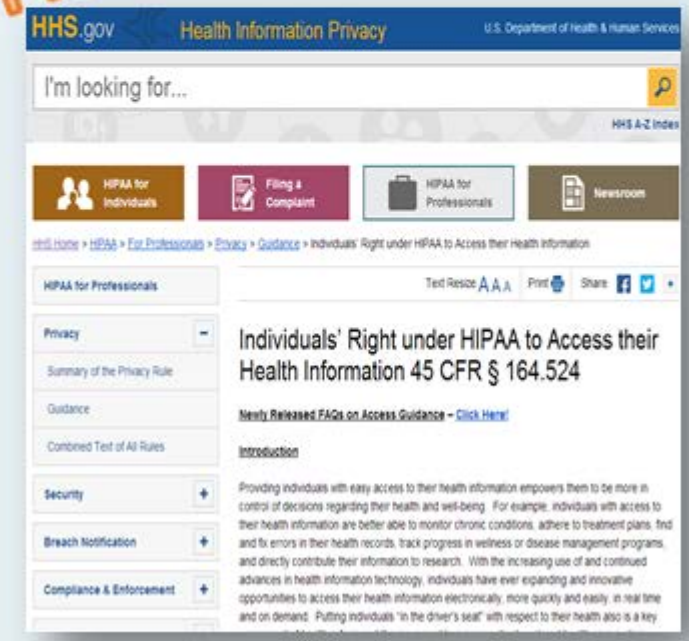
The **NATE TrustHarbor** is a new trust mechanism for API based exchange. The TrustHarbor facilitates trustworthy exchange at the intersection of consumer apps, provider's APIs and validated endorsers.

The TrustHarbor enables:

- Relying parties to discover the endorsements applied by recognized endorsers for a given app
- Consumer apps to seek endorsements from competing endorsers
- A building blocks model of endorsements to fit the different requirements of different transactions in a modular way
- An open resource where bad actors (either apps or endorsers) can be black listed across the ecosystem

Overview continued

PROTOTYPE



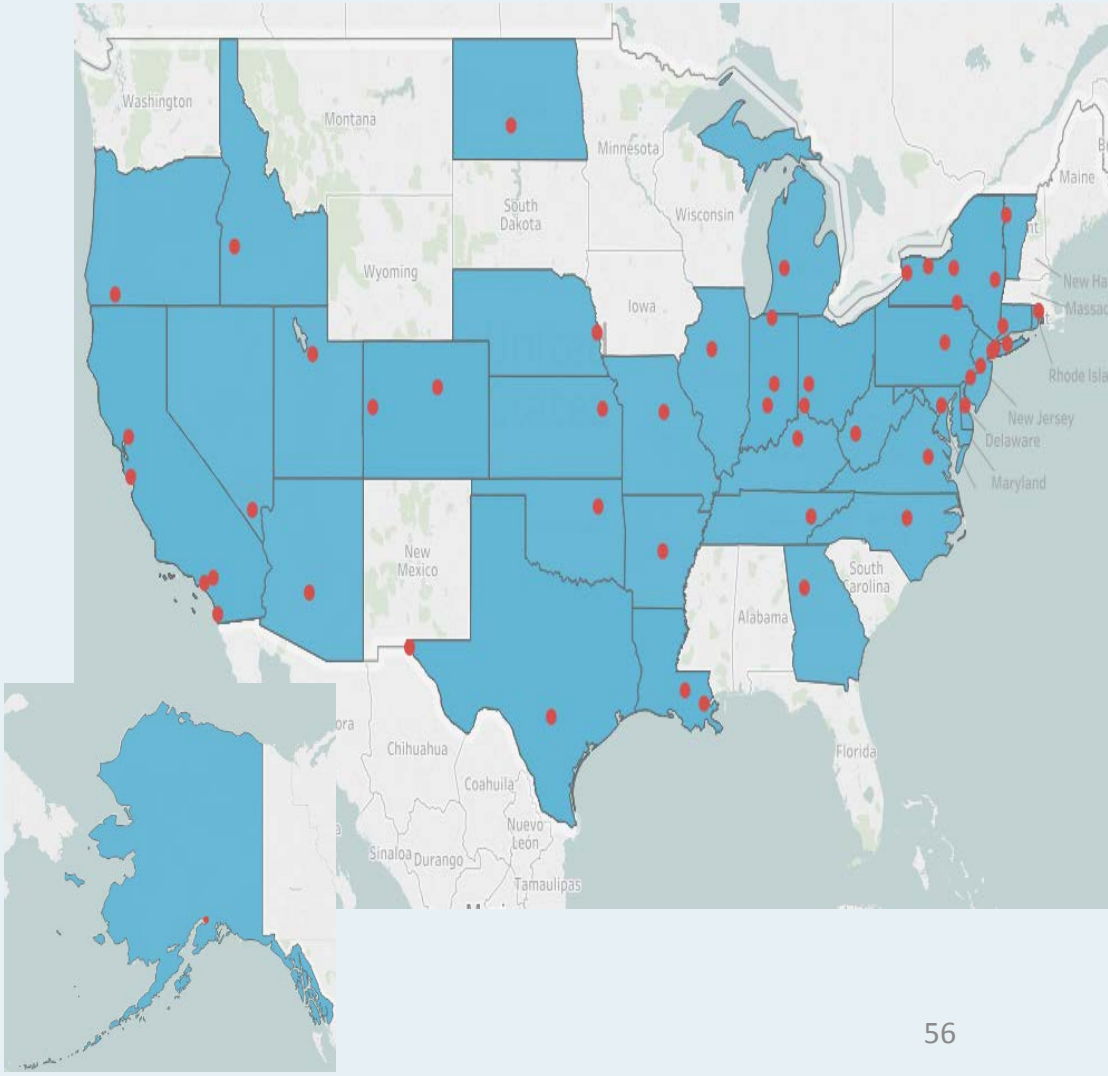
The **NATE Blue Button Directory** (NBBD) allows patients to discover how best to submit their request for health information and establishes a secure end-point that can be used by the HIPAA covered entity's staff responsible for managing these requests.

The NBBD makes it easier for consumers to discover how their providers support the individual right of access.

SHIEC

The Strategic HIE Collaborative (SHIEC)

- 54 member HIE's across 34 states
- Provide person-centric health records
- Unbiased data trustees focused on better health
- Altogether currently serve >195M patients
- Rapid growth from foundation 2 years ago
- 29 strategic business and technology partners



HIE's provide critical infrastructure

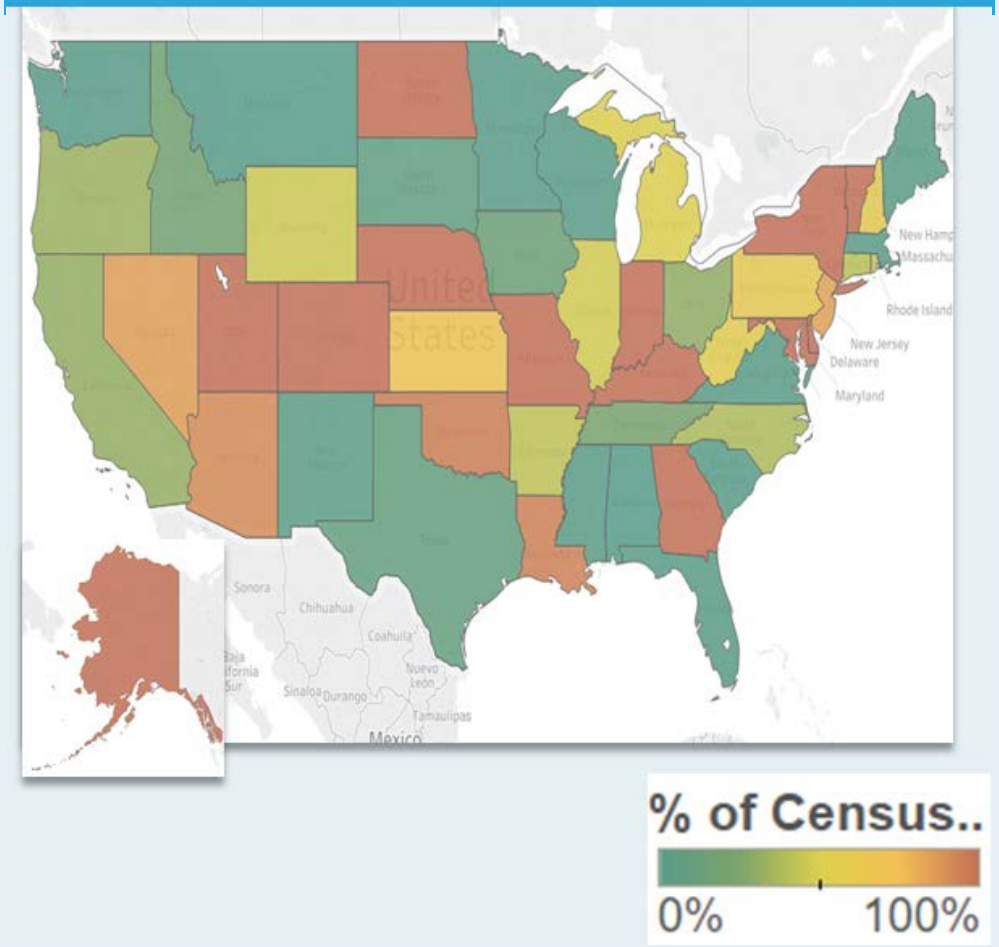
SHIEC members embrace and employ most types of interoperability

- Direct Messaging
- eHealth Exchange
- Carequality
- Imaging exchange
- Public Health interoperability

And now . . .

- **Patient Centered Data Home™**

Percent of Each State's Population in HIE

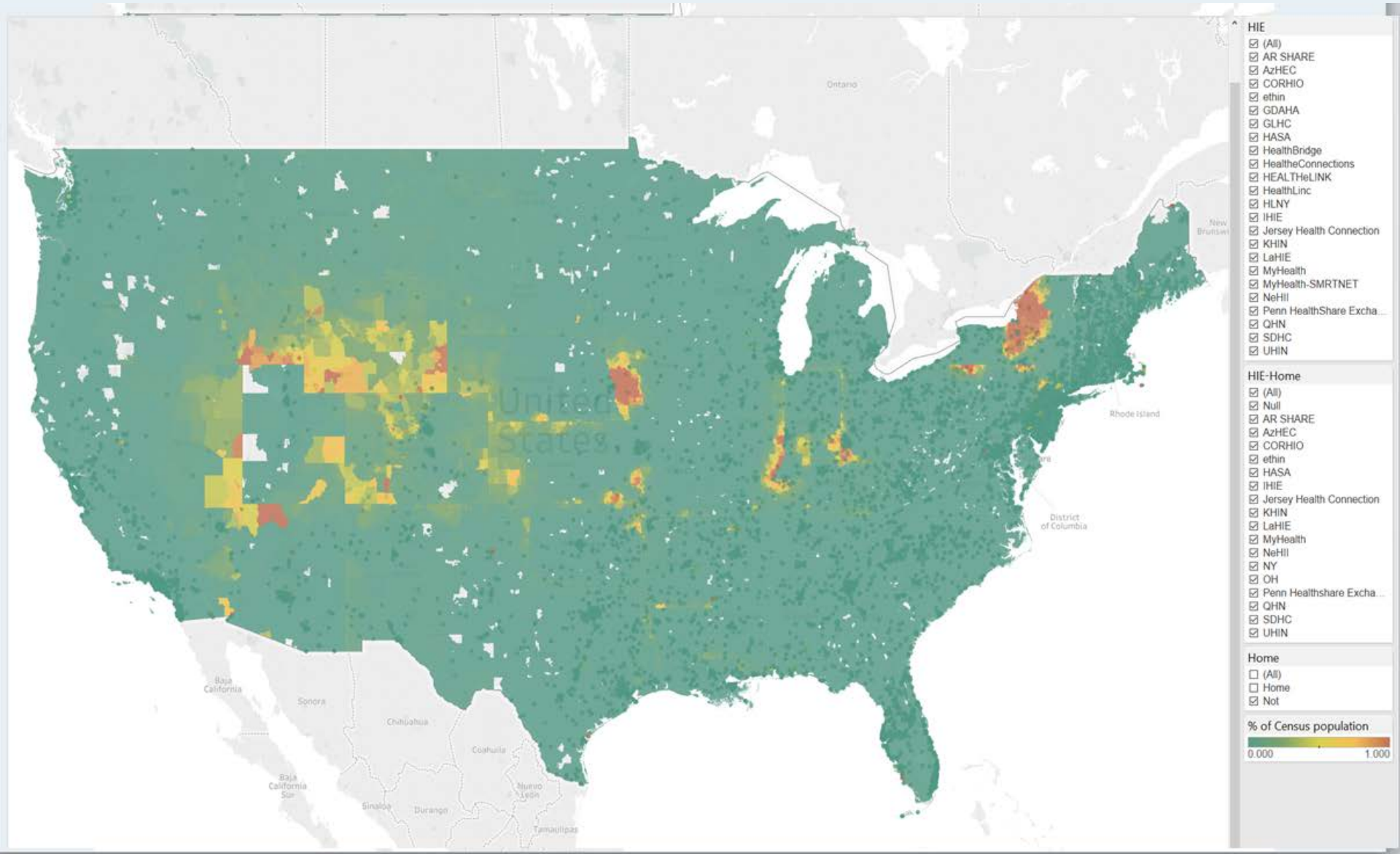


SHIEC HIE's currently cover 60% of Americans

Patient Centered Data Home™: The Vision

- Answers the three key questions
  - Who, When, Where
- Standards based, cost effective, scalable data exchange model
- Links existing HIE systems together
  - Maintain patient-centric data view
- Provides comprehensive real time patient information
  - Requires ability to PUSH
- Resolve identity across HIE's
  - Single "universal" identifier not required
- Preserves local governance and protects local stakeholders– honors local data use policies
- Enhances data aggregations required for quality reporting and shift to Value Based Payment Models

PCDH: How it works



Implications of PCDH model

Centralization of all data on each patient in their PCDH enables:

- Nationwide ADT alerting (with complete histories)
- More accurate care gap analysis (support quality)
- More accurate quality measures (support VBPM's)
- National patient identity assurance
- Possibility of centralized patient consent management
- Patient access to their entire record in one place– (patient empowerment & engagement)

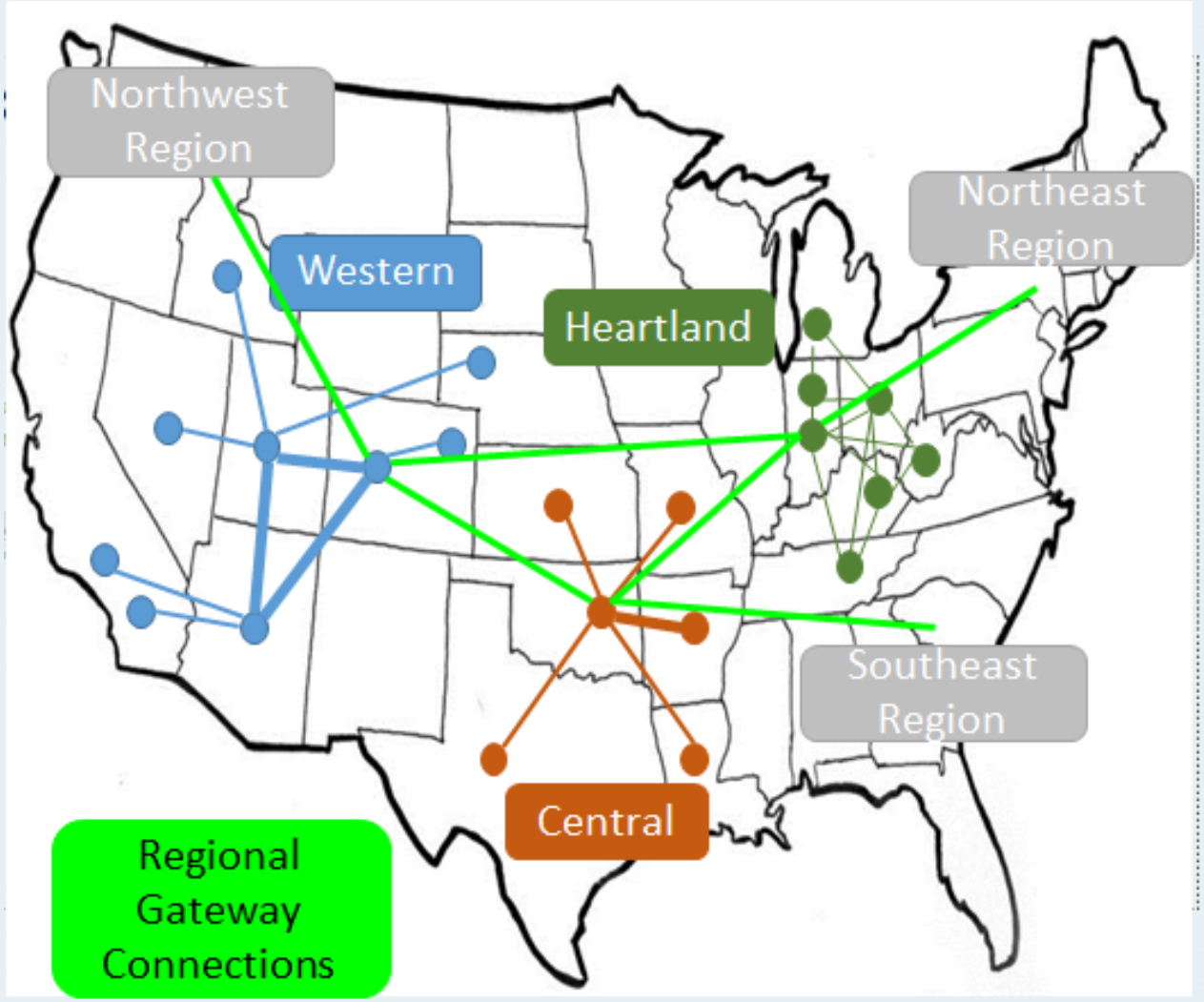
Costs:

- Relatively little– must maintain governance, geographic relationships, and minimal technology

PCDH: Current Metrics and Growth Plan

Since April, 2016:

- 3 regions in Production
- 18 HIE's connected
- Serving 33.9M patients
- >2M notifications PUSHED in response to events
- 1,000's of CCDA's pushed
- 100's of Images exchanged across PCDH network



Other services, infrastructure, initiatives and use cases

PCDH with real time nationwide alerting enables:

- Identity resolution wherever the patient has records
  - PDMP Services and medication data to facilitate management of Opioid abuse
  - Business continuity support during outages or cyberattacks
  - Qualified Clinical Data Registry (QCDR) services to support analytics and MIPS Reporting, Value Based Payment models
  - Connect and support behavioral health improvement
  - Track and address health related social needs (AHC)
  - Enable the generation of new knowledge per 21st Century Cures ACT

The Office of the National Coordinator for Health Information Technology

21st Century Cures Act Trusted Exchange Framework and Common Agreement Kick-Off Meeting

A Personal Perspective on Interoperability

Cynthia Fisher, MBA

The Office of the National Coordinator for Health Information Technology

LUNCH BREAK

Meeting will Resume at 12:45 pm

@ONC_HealthIT HHSONC HealthIT.gov

The Office of the National Coordinator for Health Information Technology

21st Century Cures Act Trusted Exchange Framework and Common Agreement Kick-Off Meeting

Panel Discussion and Audience Question and Answer

Lee Stevens, Office of Policy, Office of State and Interoperability Policy, ONC

The Office of the National Coordinator for Health Information Technology

21st Century Cures Act Trusted Exchange Framework and Common Agreement Kick-Off Meeting

Alignment and Gaps among Current Trust Agreements

Kory Mertz, Audacious Inquiry
Kelly Carulli, Audacious Inquiry

Purpose and Scope of Arrangement

- A number of organizations have established data exchange arrangements to enable cross participant data sharing. These organizations have differing **scopes, goals, and participants**.
- Organizations have taken different approaches to stitching together the fabric of their data exchange arrangement, including but not limited to:
    - Contracts/legal agreements
    - Self-attestation
    - Accreditation
    - Formal technical testing programs (i.e. certification, participant testing, etc.)
- Many operate or facilitate the use of technical infrastructure in some minimum capacity.
- All are exploring adding to the scope of their efforts to respond to evolving participant and market demands.

Permitted Purposes for Data Exchange

- Some organizations limit the permitted purposes for which data can be exchanged to treatment only, while others allow broader uses (e.g. public health, operations etc.).
- Some have established a single set of permitted purposes that apply across all data exchanged, while others align the permitted purposes by use case.
- The data available for exchange among participants in an arrangement varies based on the data captured by the participants.
- These variances in data availability and permitted purposes for the use of data uniquely inform each arrangement and may lead to conflicts across arrangements.

Permitted Participants

- The participant organizations (i.e. health information networks) in data exchange arrangements often have varying permitted participants. Permitted participants include providers, payers, government agencies, health IT developers, etc.

- The variability of permitted participants can create concerns about the exchange of data across networks. This issue is closely tied to the permitted purposes for which data can be used.

Identity Proofing and Authentication

- A long-standing tenet of exchange efforts in healthcare has been focused on providing assurance that participants are exchanging information with another party that they know or that the participant is confident that the other party is who they claim to be and has an active relationship with the patient.

- Data exchange arrangements have identity proofing and authentication requirements and use differing technical and policy frameworks to achieve this.

Technical Approach and Infrastructure

- Varying technical approaches are taken to enable exchange across participants.
- Even in instances where data exchange arrangements are supporting similar use cases, they often use differing technical standards and infrastructure to enable exchange among their participants.
- Some entities have centralized infrastructure that supports various aspects of a transaction and some have infrastructure that is optional but supports improved workflows. Others have no infrastructure that supports exchange among participants.

Cooperation and Non-Discrimination

- Most data exchange arrangements prohibit their participants from creating additional requirements to exchange data with another participant.
- These requirements vary across organizations but include prohibitions on requiring additional legal agreements and sometimes limitations on charging additional fees to exchange data for specific permitted purposes.
- Some include provisions aimed at preventing their participants from establishing policies that unnecessarily discriminate against other participants and attempt to limit the exchange of data.

Accountability

- All data exchange arrangements have established accountability mechanisms to ensure that their participants are following the organization's rules of the road and technical requirements for exchange.
- Each approach has tradeoffs in terms of the level of assurance that all participants are following required policies and standards, compared to the level of effort required for compliance.

The Office of the National Coordinator for Health Information Technology

PUBLIC COMMENT

Comments are Limited to 3 Minutes

Comments Submitted via Webinar will be Archived for the Public Record

@ONC_HealthIT HHSONC HealthIT.gov

The Office of the National Coordinator for Health Information Technology

21st Century Cures Act Trusted Exchange Framework and Common Agreement Kick-Off Meeting

Going Forward

Genevieve Morris, Principal Deputy National Coordinator, ONC
Lauren Richie, Office of Programs and Engagement, ONC

Public Comment Areas (Option for Supplying Comments to ONC)

- **Standardization:** *Adhere to industry and federally recognized standards, policies, best practices, and procedures.*
- **Transparency:** *Conduct all exchange openly and transparently.*
- **Cooperation and Non-Discrimination:** *Collaborate with stakeholders across the continuum of care to exchange electronic health information, even when a stakeholder may be a business competitor.*
- **Security and Patient Safety:** *Exchange electronic health information securely and in a manner that promotes patient safety and ensures data integrity.*
- **Access:** *Ensure that patients and their caregivers have easy access to their electronic health information.*
- **Data-Driven Choice:** *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, and enable consumer choice.*
- **General Comments Category**

Trusted Exchange Framework and Common Agreement Timeline (Preliminary Internal Targets)

Date	Activity
July 24, 2017	**First Stakeholder Engagement Kick-Off Meeting** / 30 Day **Public Comment Period Opens** For Stakeholders to Share Thoughts related to the Trusted Framework and Common Agreement
Mid-September 2017	**Public Webinar** - Overview of Public Comment Received/Status Update for Stakeholders
Late 2017-Early 2018	**Release of Draft Trust Framework/Common Agreement** and Public Comment Period
2018	**Release of Final Version** of the Trust Framework/Common Agreement

Submitting Public Comments

- Comments may be submitted here:

https://oncprojectracking.healthit.gov/wiki/display/INTEROP/Common+Agreement+and+Exchange+Framework

- Letters or attachments also may be submitted via email at exchangeframework@hhs.gov
- This public comment period for the Trusted Exchange Framework and Common Agreement will close at 11:59 pm EDT on August 25, 2017.
- Comment by specific topic area or general comments.
- Use of this form is entirely voluntary.

The Office of the National Coordinator for Health Information Technology

THANK YOU FOR ATTENDING

Public Comments will be open until 11:59 PM August 25, 2017

Future meetings will be announced soon

@ONC_HealthIT HHSONC HealthIT.gov