Interoperability:
It’s a Matter of Trust

60 Mins Live Webinar
SPEAKERS

Lee Barrett,
Executive Director & CEO, EHNAC

Todd Bailey,
Chief Information Officer, CareConvene

Tim Pletcher,
Executive Director, MiHIN
President & CEO, Velatura
Tim Pletcher
Executive Director, MiHIN
President & CEO, Velatura
The Evolution of HIE & trust

Michigan Health Information Network Shared Services (MiHIN)

MiHIN is Michigan’s state-designated entity to continuously improve healthcare quality, efficiency, and patient safety by promoting secure, electronic exchange of health information. MiHIN represents a growing network of public and private organizations working to overcome data sharing barriers, reduce costs, and ultimately advance the health of Michigan’s population.

MiHIN is a network for sharing health information statewide for Michigan
Infrastructure?
Health Information Exchange Creates Efficiency

**BEFORE:**
Duplication of effort, waste and expense

**NOW:**
Connect once to access shared services

Health Plans

Physicians

Specialty Providers

Public Health

Hospitals & Clinics

Lab tests & XRAYs

Medications

Patients & Families

MiHIN
Value of a “hub” = \( \frac{N(N-1)}{2} \)

<table>
<thead>
<tr>
<th># of Organizations</th>
<th>Total Agreements ( \frac{N(N-1)}{2} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>45</td>
</tr>
<tr>
<td>25</td>
<td>300</td>
</tr>
<tr>
<td>100</td>
<td>4,950</td>
</tr>
<tr>
<td>1000</td>
<td>499,500</td>
</tr>
</tbody>
</table>
We Typically Use Virtual Private Networks and Connect to Organizations

- Consumer-Facing Organizations
- Other Data-Sharing Organizations
- Health Information Exchanges
- Pharmacies

MiHIN Statewide Shared Services

- Health Plans
- Public Health & Medicaid
- Medicaid
Traditional ADT Example – Current Workflow

HL7 2.X & Virtual Private Networks

1) Patient goes to hospital which sends message to MiHIN
2) MiHIN checks patient-provider attribution and identifies providers
3) MiHIN retrieves contact and delivery preference for each provider from HPD
4) Notifications routed to providers based on electronic address and preferences
ONC’s 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program

- Improves patient access to data through open APIs
- Allows for choice of apps and drives innovation
- Implements information blocking practices
- Improves patient safety and transparency
Interoperability and Patient Access Final Rule (CMS-9115-F)

**Initial Priorities for Medicaid/MCOs**
- Patient Access API (applicable January 1, 2021) + 6 months
- Provider Directory API (applicable January 1, 2021) + 6 months

**Upcoming Medicaid/MCOs Requirements**
- Payer-to-Payer Data Exchange (applicable January 1, 2022)
- Improving the Dually Eligible Experience by Increasing the Frequency of Federal-State Data Exchanges (applicable April 1, 2022)

**Other Requirement Considerations**
- Public Reporting and Information Blocking
- Digital Contact Information
- ADT Event Notifications
Evolving Model for Intermediaries

1) Patient goes to hospital
2) Hospital checks NPPES for digital contact information
3) Hospital sends alert to MiHIN

How do we know/trust the sender?
### Genuine Need for Scalable Trust

<table>
<thead>
<tr>
<th># of Apps/ Sources</th>
<th>Total Agreements $(N^2-N)/2$</th>
<th>Certificate Exchanges</th>
<th>TRUST Relationships</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>45</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>300</td>
<td></td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>4,950</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1000</td>
<td>499,500</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
InterOp Station Overview

Centralized Developer Portal to Safeguard Data

Flexible Identity Management to Connect Members

Standards-Based, Modular API Platform

Data Transformation to enable FHIR exchange with Apps

Provider Directory API

Patient Access API

Payer-to-Payer Data Exchange

Future APIs

3rd Party App

3rd Party App

3rd Party App

MMIS

MCO Data

Data Warehouse

Other Sources
InterOp Station: Moving Beyond Compliance

Maximize existing investments in HIT to advance policy and technical components in support of broader healthcare reform initiatives.
Developer Portal

Our Developer Portal supports the successful and safe connection of 3rd party applications to your data.

1. **App registers in the Developer Portal.**
2. **App completes security and privacy attestations. Receives authorization.**
3. **Beneficiary selects app and provides log-in information.**
4. **Resource server provides Access Tokens to API.**
5. **Beneficiary is verified and API authorized to send data within scope.**
6. **Beneficiary initiates call for data.**

---

**SMART®**

---

**OpenID®**

---

Our Developer Portal supports the successful and safe connection of 3rd party applications to your data.
Care Convene – Simplifying Healthcare Delivery

Unique Value Proposition

Access
- Increase providers’ visit capacity and improve patient access to care.

Communication
- Simplify patient & provider communication with virtual tools to improve patient engagement and care compliance.

Coordination
- Enable digital coordination of costly inpatient and emergency room visits with real-time hospital notifications.
Consumer Access Workflow
Centralized Patient Record

Health Journal

Wanda Rosa
Gender: Female
Phone: 269-322-1080
Address: 341 James Ave SE Grand Rapids MI 49503
Visit Fees: $0.00
Insurance: Trinity Healthcare of California

Reason for Visit: Anxiety
Patient Comments:

Meet Date: 04/06/2020

Health Journal

Yesterday
CHF Assessment
Trouble breathing

Monday 11/16/2020

New Health Data - SCBSM

Saturday 11/14/2020

Diagnosis - CHF

Type Message and press Enter to send

Care Convene © 2021
FHIR Based Integration within Care Convene

<table>
<thead>
<tr>
<th>USCDI – US Core Data for Interoperability</th>
<th>Care Convene PHR ready</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allergies &amp; Intolerances</td>
<td>Yes</td>
</tr>
<tr>
<td>Medications</td>
<td>Yes</td>
</tr>
<tr>
<td>Procedures</td>
<td>Yes</td>
</tr>
<tr>
<td>Problems</td>
<td>Yes</td>
</tr>
<tr>
<td>Immunizations</td>
<td>Yes</td>
</tr>
<tr>
<td>Provenance</td>
<td>Yes</td>
</tr>
<tr>
<td>Care Team Members</td>
<td>Yes</td>
</tr>
<tr>
<td>Observations</td>
<td>Yes</td>
</tr>
<tr>
<td>Patient Demographics</td>
<td>Yes</td>
</tr>
<tr>
<td>Medications</td>
<td>Yes</td>
</tr>
<tr>
<td>Goals</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Key Points Learned from the July 1st go-live:

- FHIR is a very promising technology.
- FHIR specifications leave room for interpretation.
- Each payer has their own unique technical infrastructure and development standards that influence the outcome of each interoperability project.
- As a vendor, we have to react uniquely to each payer, which in turn is very costly.
Lee Barrett
Executive Director and CEO
EHNAC
“The Interoperability Factor: It’s a Matter of Trust – Solutions for Success”

Lee Barrett, Executive Director, CEO EHNAC
Agenda

- Putting The Rules Together – Lee Barrett
  - EHNAC’s Responses to the Challenges
  - TNAP
  - TDRAAP
- Questions / Wrap Up
Putting It All together

Key Programs Promoting and Aligning with the Interoperability Roadmap
21st Century Cures Today

TEFCA

Interoperability

HIPAA/HITECH Omnibus

FHIR Roadmap

Information Blocking

CMS Patient Access Rule
Assurance, Confidence and Trust for Trusted Exchange Networks

In the 21st Century Cures Act, Congress identified the importance of interoperability and specifically directed OCR to "develop or support a trusted exchange framework, including a common agreement among health information networks nationally." The Trusted Network Accreditation Program (TNAP) was developed to directly align with this goal and the required Trusted Exchange Framework and Common Agreement (TEFCA).

TEFCA will affect a diverse group of industry stakeholders, including Qualified Health Information Networks (QHINs), Health Information Exchanges (HIEs), Accountable Care Organizations (ACOs), data registries, labs, providers, payers, vendors, and suppliers — and TNAP has been designed to address their needs. Maintaining Trusted Network Accreditation in conjunction with HITRUST CSF Validation ensures their security and privacy of trusted networks and the use of enabling technologies in the healthcare ecosystem.

TNAP provides third-party review with accreditation for Trusted Exchange participants, assessing an organization's ability to comply with privacy and security. If HITRUST CIC requirements, HIPAA, HITECH including Omnibus Rule, ARRA and ACA legislative reform provisions as applicable, NIST, Cybersecurity Framework, GDPR and others as well as technical performance, business processes and resource management.

TNAP - QHIN
For those who provide health information network services and wish to demonstrate they can be trusted to carry out services as a Qualified Health Information Network.

Which TNAP Program is Right for You?

TNAP - Participant/Participant Member
For those with the desire to be recognized as a Participant or as a Participant Member in the QHIN Trust Exchange Framework. Participant examples include HINs, health systems, health IT developers, payers and federal agencies.

Trust Is Everything in Healthcare
TNAP-QHINs and TNAP-Participant candidates must hold HITRUST CSF Validated Assessment with Certification.
Trusted Dynamic Registration & Authentication Accreditation Program

The Trusted Dynamic Registration & Authentication Accreditation Program (TDOAAP) is designed to help healthcare organizations and application developers demonstrate their ability to use trusted digital certificates for endpoint identity, registration, authentication, and attribute discovery for electronic healthcare transactions in real-time.

Two TDOAAP programs are available: TDOAAP-Basic and TDOAAP-Comprehensive.

TDOAAP-Basic offers: privacy- and security-related features with minimal overhead, while the included UDAP technical framework certifies on demonstration that an entity’s end-to-end API can be trusted by patients and other industry stakeholders. It is designed specifically for developers of consumer-facing apps, also referred to as a patient’s “App of Their Choice,” as used in workshops such as HCC’s “Build It to Fit It: How to Build SMART T2 app launch with individual sign-on for FHIR data access by one patient at a time with the patient’s own credentials.

TDOAAP-Comprehensive is designed for organizations already holding EHNAC Accreditation or those wanting to demonstrate full HIPAA/FSSC Privacy and Security compliance and support of all relevant UDAP workflows, including privileged client access to sensitive data, for example, FHIR Bulk Data request, broadcast, or targeted queries, Authorization Code Flow in patient-controlled or cross-organizational queries, or any setting in which multiple services deployed by the organization enable UDAP workflows. Program candidates include:

- Providers
- Care organizations
- Mobile app developers
- Health Information Exchanges (HIEs)
- Health Information Networks (HINs)
- Financial institutions
- Regulatory agencies
- Defense contractors
- Clearinghouses
- End users
- Security vendors
- Cloud vendors
- Identity providers

EHNAC

"No single entity can support and act alone in this; it is not a one-component or interoperability throughout the healthcare information highway. Through the creation of a technical and governance infrastructure, TDOAAP interoperability is available with a specific focus on technical standards validating trust and transparency for both organizational and individual access to data."...

Lea Scannell
Executive Director and Chief Executive Officer
EHNAC
Demonstrate Trust with TDRAAP

TDRAAP will serve as a “good housekeeping seal” of proven readiness and trust to enter onto the interoperability digital exchange highway.

The Electronic Healthcare Network Accreditation Commission (EHNAC) is a voluntary, self-governing standards development organization (SDO) established to develop standard criteria and accredit organizations that electronically exchange healthcare data. The EHNAC criteria for each of its accreditation programs sets the foundational requirements for measuring an organization’s ability to meet standards with federal and state healthcare reform mandates such as HIPAA/HITECH, 21st Century Cures Act, TEFCA and other mandates and best practices like NIST, for health care organizations focusing on the areas of privacy, security, cybersecurity, breach handling, confidentiality, best practices, procedures and assets.

Criteria for the TDRAAP Program is available on the EHNAC Criteria Page. Organizations interested in beginning the application process for TDRAAP should complete the application form or contact EHNAC. For organizations that require hands-on support to complete the pre-assessment steps, readiness planning, gap assessments and more, check out EHNAC’s Consulting and Advisory Services.

The open source UDAP profiles have been well-received since they provide dynamic discovery capability and increased confidence in FHIR and other open API transactions through the use of trusted identities and verified attributes.

Julie Naas
UDAP.org

Trust Is Everything in Healthcare

info@ehnac.org | ehnac.org
	
	
	
	
The Office of the National Coordinator for Health IT, (ONC) Cures Act Final Rule supports seamless and secure access, exchange, and use of electronic health information.

The rule give patients (and providers) secure access to health information. It also should increase innovation and competition by fostering an ecosystem of new applications. This will provide patients with more choices in their healthcare.

It calls on the healthcare industry to adopt standardized application programming interfaces (APIs), to allow individuals to securely and easily access structured electronic health information using smartphone applications.

*Source: Office of the National Coordinator - healthit.gov*
The rule includes a provision requiring that patients can electronically access all of their electronic health information (EHI), structured and/or unstructured, at no cost.

- Source: Office of the National Coordinator - healthit.gov
Problem: Lack of seamless data exchange in healthcare has historically detracted from patient care, leading to poor health outcomes, and higher costs.

Resolution: The final rule adds policies to break down national health system barriers to:

1) enable better patient access to their health information,
2) improve interoperability and
3) unleash innovation, while reducing burden on payers and providers.

Patients and providers will be more informed, which can lead to better care and improved patient outcomes and reduce burden.

“In a future where data flows freely and securely between payers, providers, and patients, we can achieve truly coordinated care, improved health outcomes, and reduced costs.”

Source: https://www.cms.gov/newsroom/fact-sheets/interoperability-and-patient-access-fact-sheet
Identifying the right standards can help data flow securely and efficiently. CMS and ONC have identified Health Level 7® (HL7) Fast Healthcare Interoperability Resources® (FHIR) Release 4.0.1 as the foundational standard to support data exchange via secure application programming interfaces (APIs).


“Patients have a right under HIPAA to access their health information and (CMS/ONC believe) a right to know their health information is exchanged in a way that ensures their privacy and security. We are working to balance these important issues in a way that empowers patients to be in charge of their healthcare.”
CMS Patient Access API Requirements

CMS regulated payers like those listed below are required to implement and maintain a secure, standards-based (HL7 FHIR Release 4.0.1) API allowing patients easy access to claims and encounter information, including cost and limited clinical information via third-party applications of their choice.

MA organizations,
Medicaid Fee-for-Service (FFS) programs,
Medicaid managed care plans,
CHIP FFS programs,
CHIP managed care entities, and
QHP issuers on the FFEs

More information about Provider Directory APIs; Payer to Payer Data Exchange and other components can be found on the CMS Website.

Source: https://www.cms.gov/newsroom/fact-sheets/interoperability-and-patient-access-fact-sheet
Client App registration today is usually completed via a manual process, with interoperability and the overall use of Apps in general, an explosion of the use of Client Apps is expected.

Automation is needed to scale the process of enabling trust between the growing number of Client Apps, Servers and Users. A mechanism to replace the generation and management of single-system “silolod” credentials (for each trio of client app, payer/provider, and individual or other system user) must be created. This is a scalability challenge left unsolved by OAuth and OpenID as they stand today. Data access must also be authorized with one or more community standards and Common Agreements.

*Use of UDAP solves the technical challenge! Completion of Privacy & Security Certification/Accreditation offers the necessary trust for data handling!*
The TDRAAP Program Addresses the Challenge!

TDRAAP combines a health care data privacy and security self-governed Standards Development Organization - EHNAC, with the Technical Framework Certification of the Unified Data Access Profiles (UDAP.org).

The program enables TDRAAP Certified/Accredited organizations to show they can be TRUSTED in the ecosystem!
Trusted App

- Sign In Page
  (Consumer’s View)
- Typical user authorization text appears as usual
- Information about the app is also displayed
- Trusted information is highlighted by the “Green Lock”
- Consumer has increased confidence in the interaction
Ecosystem view

Requestor Actor

1. UDAP Dynamic Client Registration request (signed with client’s certificate-backed key)

2. client_id

Responder Actor

UDAP JWT-Based Client Authentication

FHIR Transaction Request

Access Token

FHIR Transaction Response

Art credit: adapted from ONC FAST Security TLC Webinar
Trusted Dynamic Client Registration

- Public Key registration for JWT-Based Authentication of Client Apps
  - extends standard (and common) OAuth 2.0 and OpenID Connect technologies
  - backed by Digital Certificates
  - supports client credentials flow OR authorization code flow
- Server Validation
  - including multi-tenant environments
- Certifications and Endorsements
  - for tailored scopes
- Tiered OAuth for User Authentication
  - with authorization code flow
  - Identity provider as trusted network participant
## TDRAAP Glide Path

### Authentication Levels

<table>
<thead>
<tr>
<th>Star Levels</th>
<th>Description</th>
<th>Benefit of Certified or Accredited Workflow</th>
<th>Industry Effort Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>🌟</td>
<td>OAuth 2.0 – Authorization code flow with Client ID (and Secret)</td>
<td>Access to data one patient at a time with patient’s own credentials</td>
<td>Most difficult to scale (each App must gain Client ID and secret for each different Server)</td>
</tr>
<tr>
<td>⭐️⭐️</td>
<td>UDAP Dynamic Client Registration</td>
<td>No client pre-registration needed</td>
<td>Less difficult to scale; some cost savings for clients &amp; servers</td>
</tr>
<tr>
<td>⭐️⭐️⭐️</td>
<td>UDAP JWT-Based Authentication</td>
<td>No client credential provisioning needed</td>
<td>Even less difficult to scale</td>
</tr>
<tr>
<td>⭐️⭐️⭐️⭐️</td>
<td>UDAP Certifications and Endorsements, Server Metadata &amp; authorization assertions within JWT-Based Authentication</td>
<td>Servers include Server Metadata and indicate validation of Client in UI (if any)</td>
<td>Simpler to scale</td>
</tr>
<tr>
<td>⭐️⭐️⭐️⭐️⭐️</td>
<td>Server Claims and UDAP Tiered DAuth</td>
<td>Clients indicate validation in UI (if any); no user pre-registration needed</td>
<td>Simplest to scale, most cost savings for clients, servers &amp; patients</td>
</tr>
</tbody>
</table>

1. When used with FHIR registration servers capable of UDAP Trusted DCR on the server side.
2. When used with FHIR authorization servers capable of UDAP JWT-Based Authentication on the server side.
3. Claims and assertions made by client applications are validated and/or consumed by servers. This includes additional client application characteristics asserted by Endorsers, such as EHNAC and CARIN, e.g., whether a client application is TDRAAP certified or “affirmatively sharable” their privacy policy with every user; authorization assertions can be used in FHIR patient matching by a privileged client for patient access even when a user is not present.
4. Claims made by “Servers,” such as “Servers’ use of signed metadata and/or Certifications & Endorsements,” are validated by Clients.
Contact Information
Lee Barrett, EHNAC
lbarrett@ehnac.org

UDAP profiles:
http://www.udap.org
Thank you!