Interoperability: It’s a Matter of Trust

60 Mins Live Webinar

MiHIN
MICHIGAN HEALTH INFORMATION NETWORK SHARED SERVICES

velatura

EHNAC™

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)

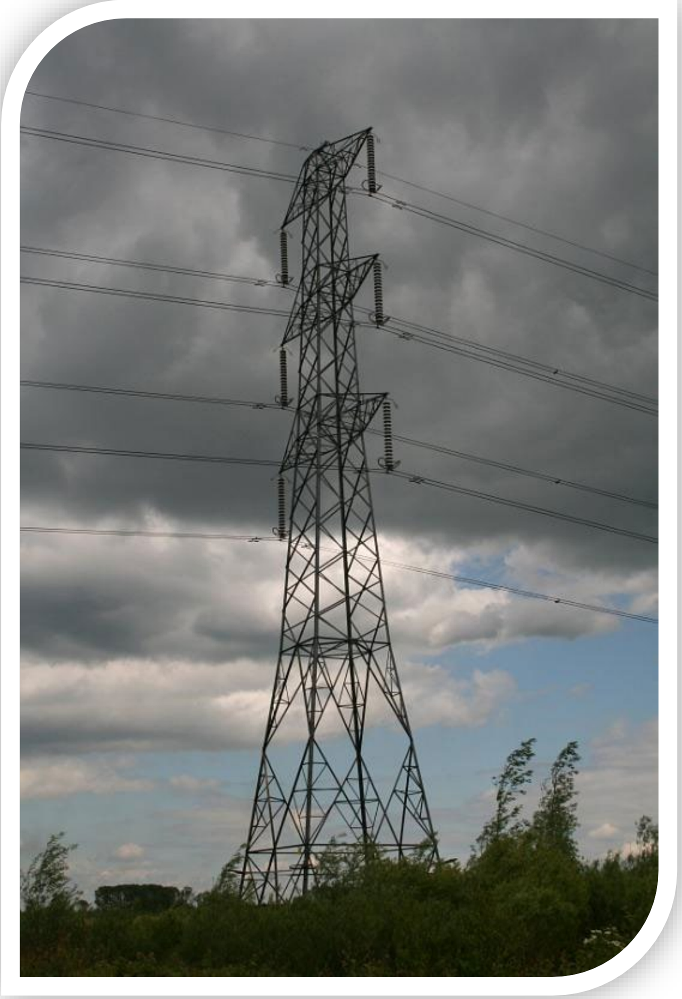
MiHIN is Michigan's **state-designated entity** to continuously improve healthcare quality, efficiency, and patient safety by promoting secure, electronic exchange of health information. MiHIN represents a growing network of public and private organizations working to overcome data sharing barriers,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

MiHIN is a

network for sharing health information statewide for Michigan

MiHIN MICHIGAN HEALTH INFORMATION NETWORK SHARED SERVICES

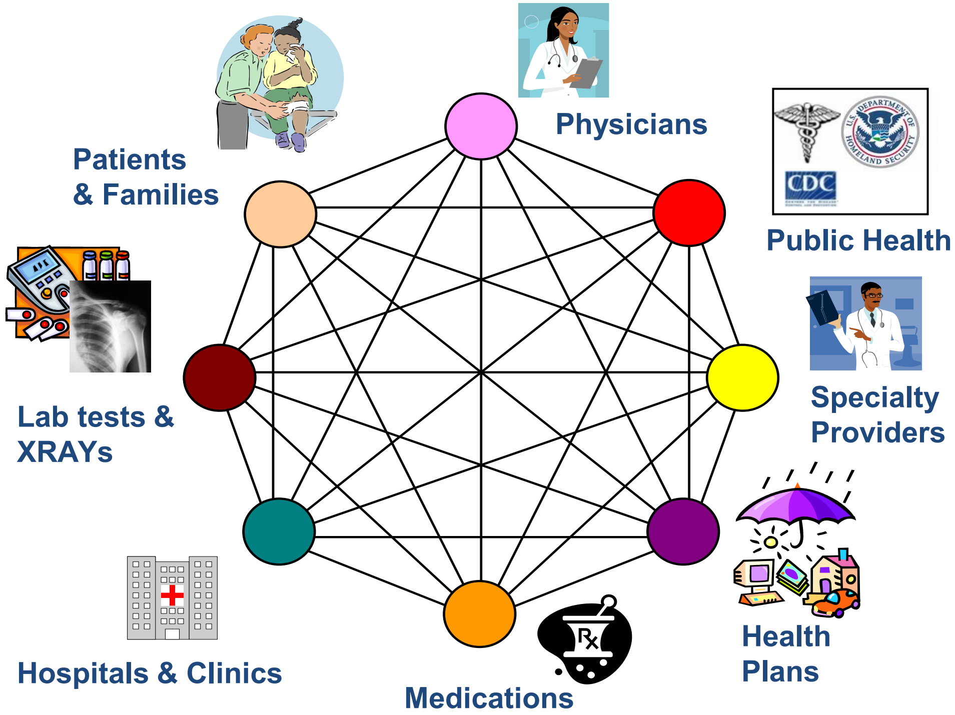
Infrastructure?



Health Information Exchange Creates Efficiency

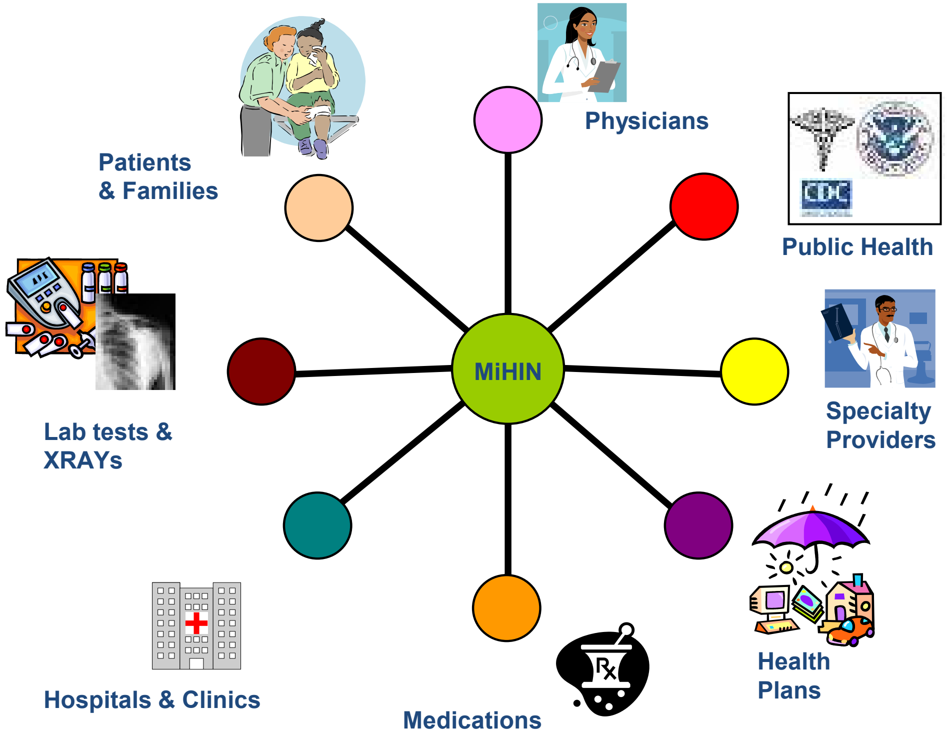
BEFORE:

Duplication of effort,
waste and expense



NOW:

Connect once to access
shared services

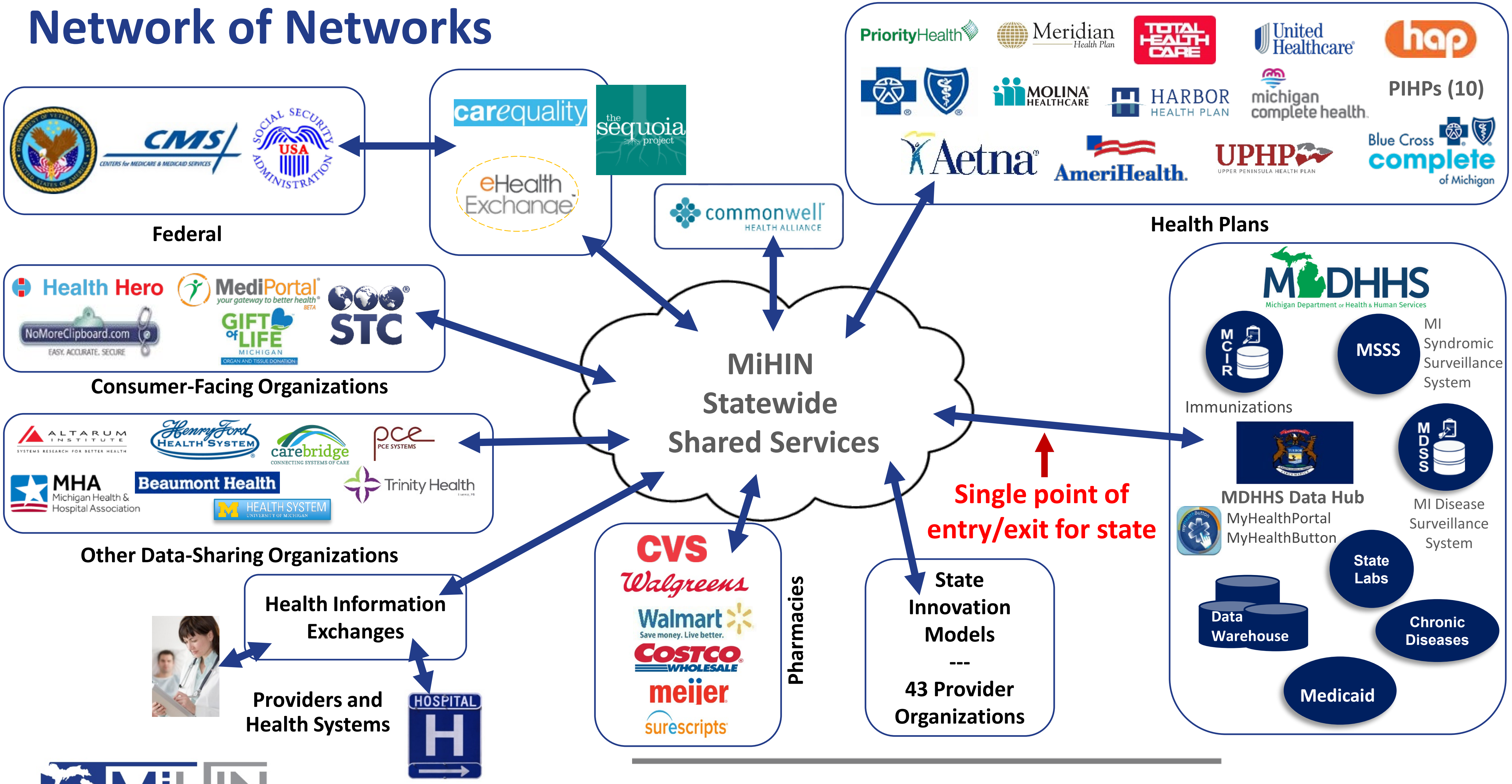


MiHIN
MICHIGAN HEALTH INFORMATION NETWORK
SHARED SERVICES

Value of a “hub” = (N*(N-1))/2

# of Organizations	Total Agreements (N*(N-1))/2
2	1
10	45
25	300
100	4,950
1000	499,500

Network of Networks



Federal

Consumer-Facing Organizations

Other Data-Sharing Organizations

Health Information Exchanges

Providers and Health Systems

Pharmacies

Health Plans

PIHPs (10)

MiHIN Statewide Shared Services

Single point of entry/exit for state

State Innovation Models
---
43 Provider Organizations

Immunizations

MI Syndromic Surveillance System

MDHHS Data Hub

MyHealthPortal
MyHealthButton

MI Disease Surveillance System

State Labs

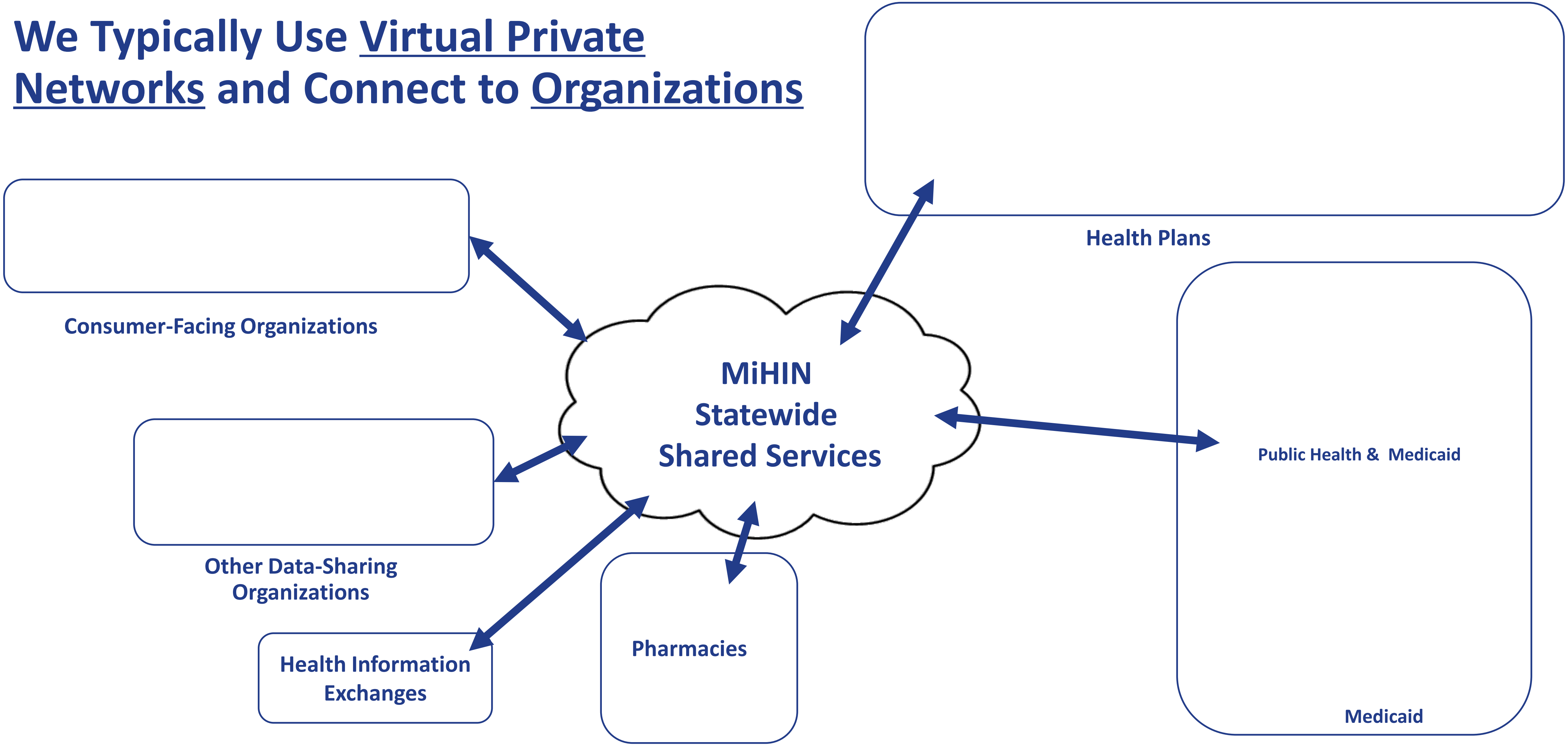
Data Warehouse

Chronic Diseases

Medicaid

CMS
CENTERS for MEDICARE & MEDICAID SERVICES
SOCIAL SECURITY ADMINISTRATION
USA
carequality
the sequoia project
eHealth Exchange
commonwell HEALTH ALLIANCE
PriorityHealth
Meridian Health Plan
TOTAL HEALTH CARE
United Healthcare
hap
MOLINA HEALTHCARE
HARBOR HEALTH PLAN
michigan complete health
Aetna
AmeriHealth
UPHP UPPER PENINSULA HEALTH PLAN
Blue Cross complete of Michigan
Health Hero
MediPortal your gateway to better health BETA
NoMoreClipboard.com EASY. ACCURATE. SECURE
GIFT of LIFE MICHIGAN ORGAN AND TISSUE DONATION
STC
ALTARUM INSTITUTE SYSTEMS RESEARCH FOR BETTER HEALTH
Henry Ford HEALTH SYSTEM
carebridge CONNECTING SYSTEMS OF CARE
pce PCE SYSTEMS
MHA Michigan Health & Hospital Association
Beaumont Health
M HEALTH SYSTEM UNIVERSITY OF MICHIGAN
Trinity Health
CVS
Walgreens
Walmart Save money. Live better.
COSTCO WHOLESALE
meijer
surescripts
MDHHS Michigan Department of Health & Human Services
MCIR
MSSS
MDSS
HOSPITAL
H

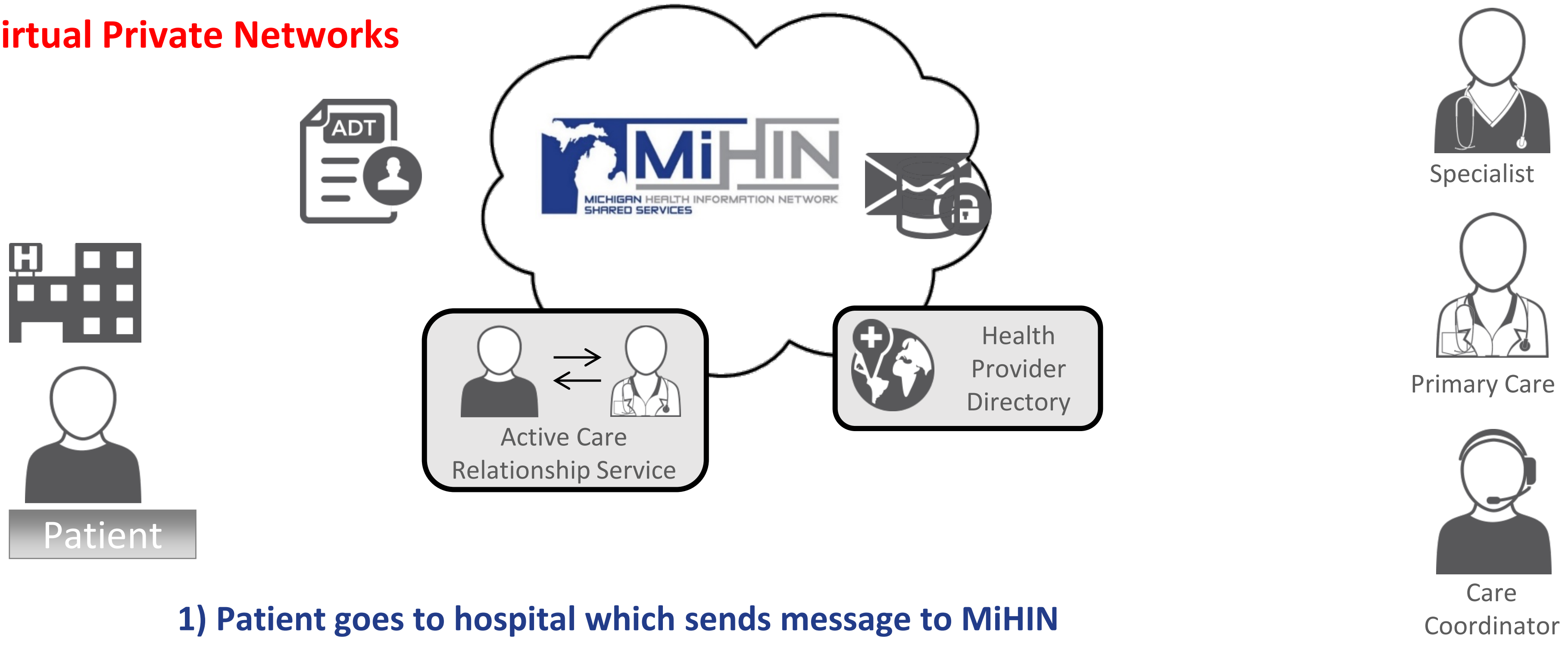
We Typically Use Virtual Private Networks and Connect to Organizations



Health Plans
Consumer-Facing Organizations
MiHIN
Statewide
Shared Services
Public Health & Medicaid
Other Data-Sharing Organizations
Health Information Exchanges
Pharmacies
Medicaid

Traditional ADT Example – Current Workflow

HL7 2.X & Virtual Private Networks


ADT
MiHIN
MICHIGAN HEALTH INFORMATION NETWORK
SHARED SERVICES
H
Patient
Active Care Relationship Service
Health Provider Directory
Specialist
Primary Care
Care Coordinator

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

MiHIN
MICHIGAN HEALTH INFORMATION NETWORK
SHARED SERVICES

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

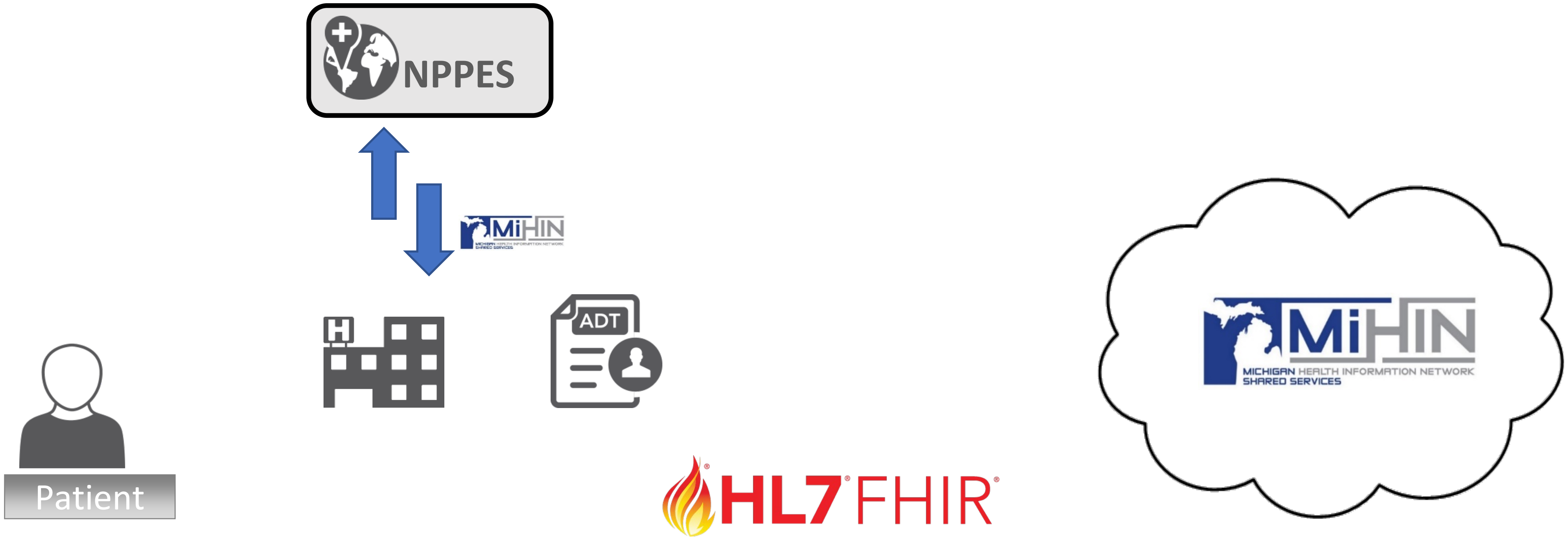
Upcoming Medicaid/ MCOs Requirements

- 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



How do we know/trust the sender?

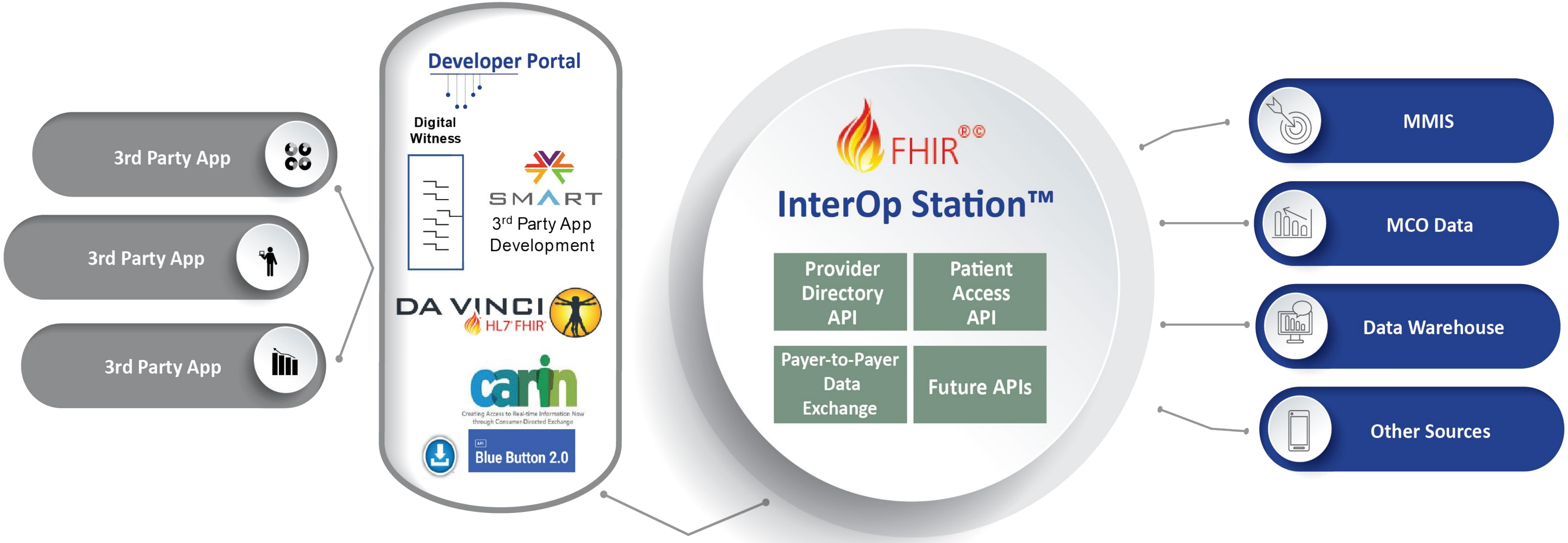
1) Patient goes to hospital
2) Hospital checks NPPES for digital contact information
3) Hospital sends alert to MiHIN

Genuine Need for Scalable Trust

	Total Agreements
# of Apps/Sources	(N*(N-1))/2
2	1
10	45
25	300
100	4,950
1000	499,500

Certificate Exchanges
TRUST Relationships

InterOp Station Overview



3rd Party App

3rd Party App

3rd Party App

Developer Portal

Digital Witness

SMART 3rd Party App Development

DA VINCI HL7 FHIR

carin

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

Blue Button 2.0

FHIR®©

InterOp Station™

Provider Directory API	Patient Access API
Payer-to-Payer Data Exchange	Future APIs

MMIS

MCO Data

Data Warehouse

Other Sources

Centralized Developer Portal to Safeguard Data

Flexible Identity Management to Connect Members

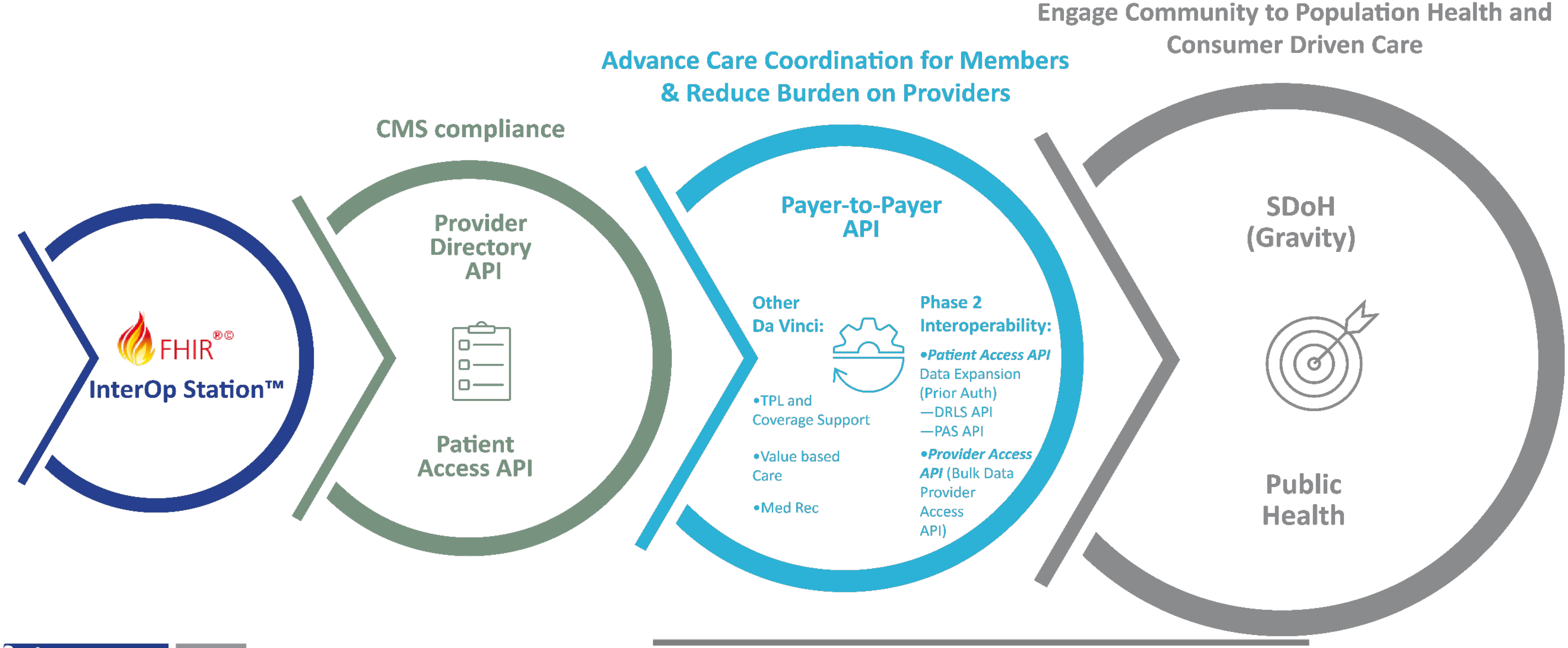
Standards- Based, Modular API Platform

Data Transformation to enable FHIR exchange with Apps

MiHIN
MICHIGAN HEALTH INFORMATION NETWORK
SHARED SERVICES

InterOp Station: Moving Beyond Compliance

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



FHIR®©
InterOp Station™

CMS compliance

Provider Directory API

Patient Access API

Advance Care Coordination for Members & Reduce Burden on Providers

Payer-to-Payer API

Other Da Vinci:

- TPL and Coverage Support
- Value based Care
- Med Rec

Phase 2 Interoperability:

- ***Patient Access API*** Data Expansion (Prior Auth)
  —DRLS API
  —PAS API
- ***Provider Access API*** (Bulk Data Provider Access API)

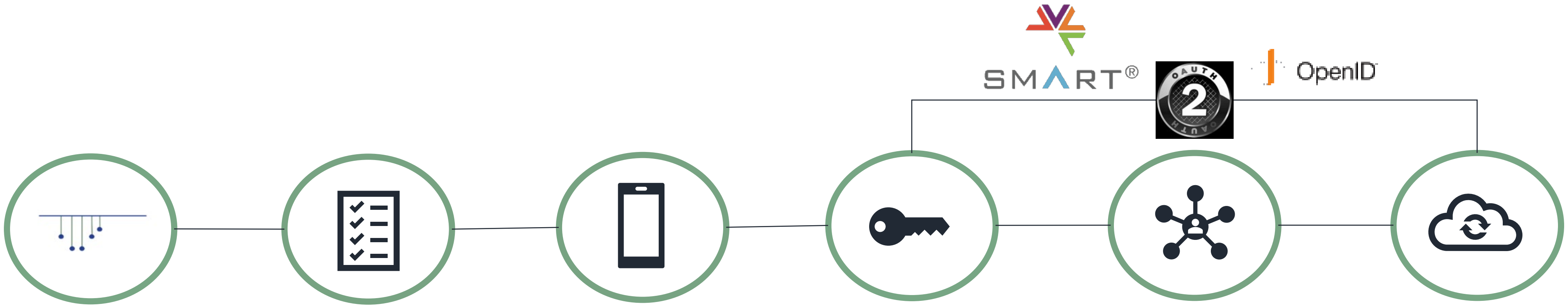
Engage Community to Population Health and Consumer Driven Care

SDoH (Gravity)

Public Health

Developer Portal

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



App registers in the Developer Portal.

App completes security and privacy attestations. Receives authorization.

Beneficiary selects app and provides log-in information.

Resource server provides Access Tokens to API.

Beneficiary is verified and API authorized to send data within scope.

Beneficiary initiates call for data.

Todd Bailey
Chief Information Officer
Care Convene

Care Convene – Simplifying Healthcare Delivery

Unique Value Proposition

Access

Communication

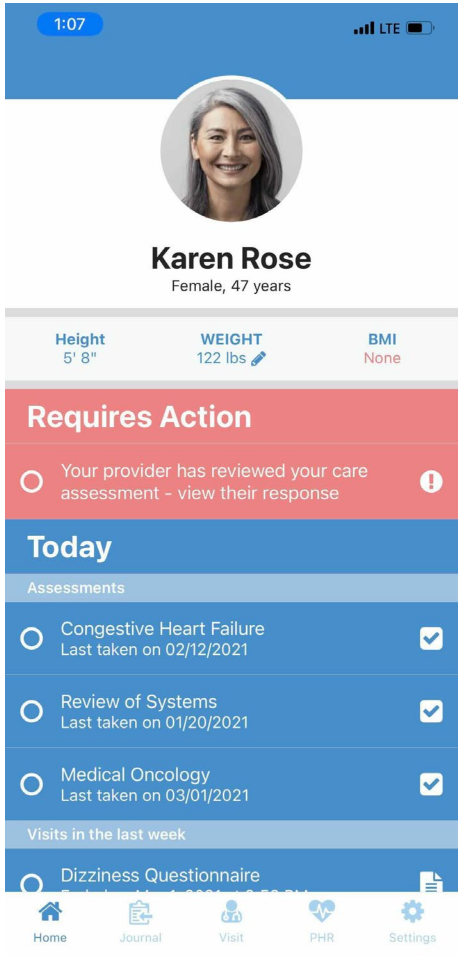
Coordination

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

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

- Enable digital coordination of costly inpatient and emergency room visits with real-time hospital notifications.

Consumer Access Workflow



Karen Rose

Female, 47 years

Height	WEIGHT	BMI
5' 8"	122 lbs	None

Requires Action

○ Your provider has reviewed your care assessment - view their response

Today

Assessments

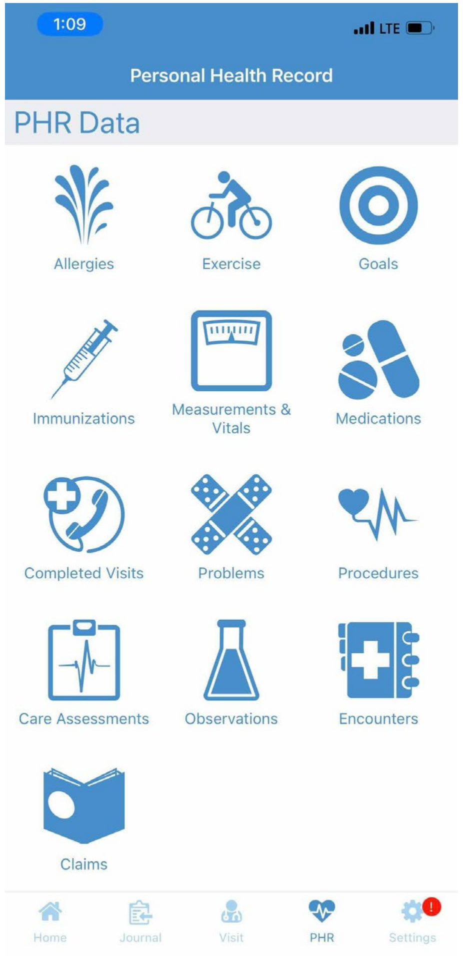
○ Congestive Heart Failure
Last taken on 02/12/2021 ☑

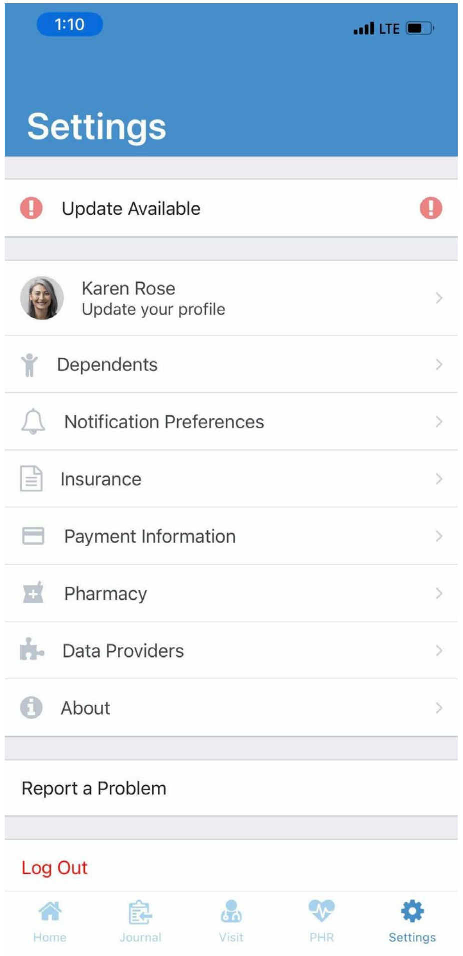
○ Review of Systems
Last taken on 01/20/2021 ☑

○ Medical Oncology
Last taken on 03/01/2021 ☑

Visits in the last week

○ Dizziness Questionnaire



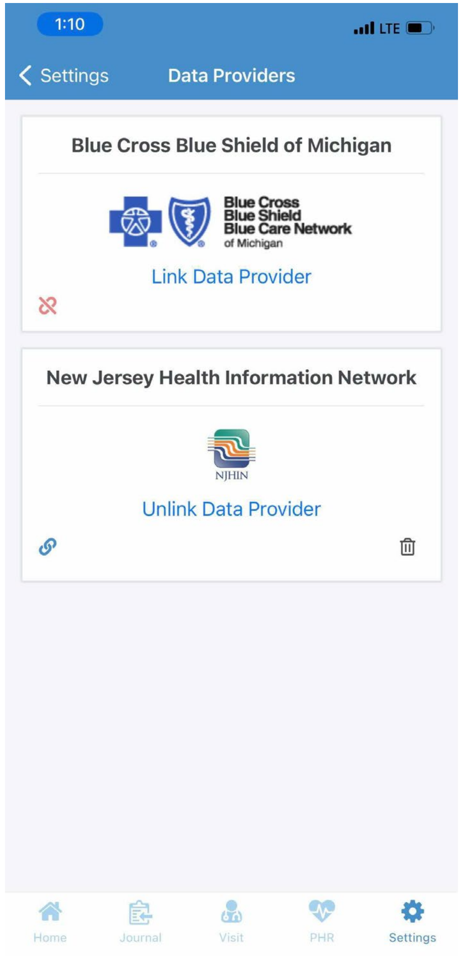


Settings

- Update Available
- Karen Rose
Update your profile
- Dependents
- Notification Preferences
- Insurance
- Payment Information
- Pharmacy
- Data Providers
- About

Report a Problem

Log Out



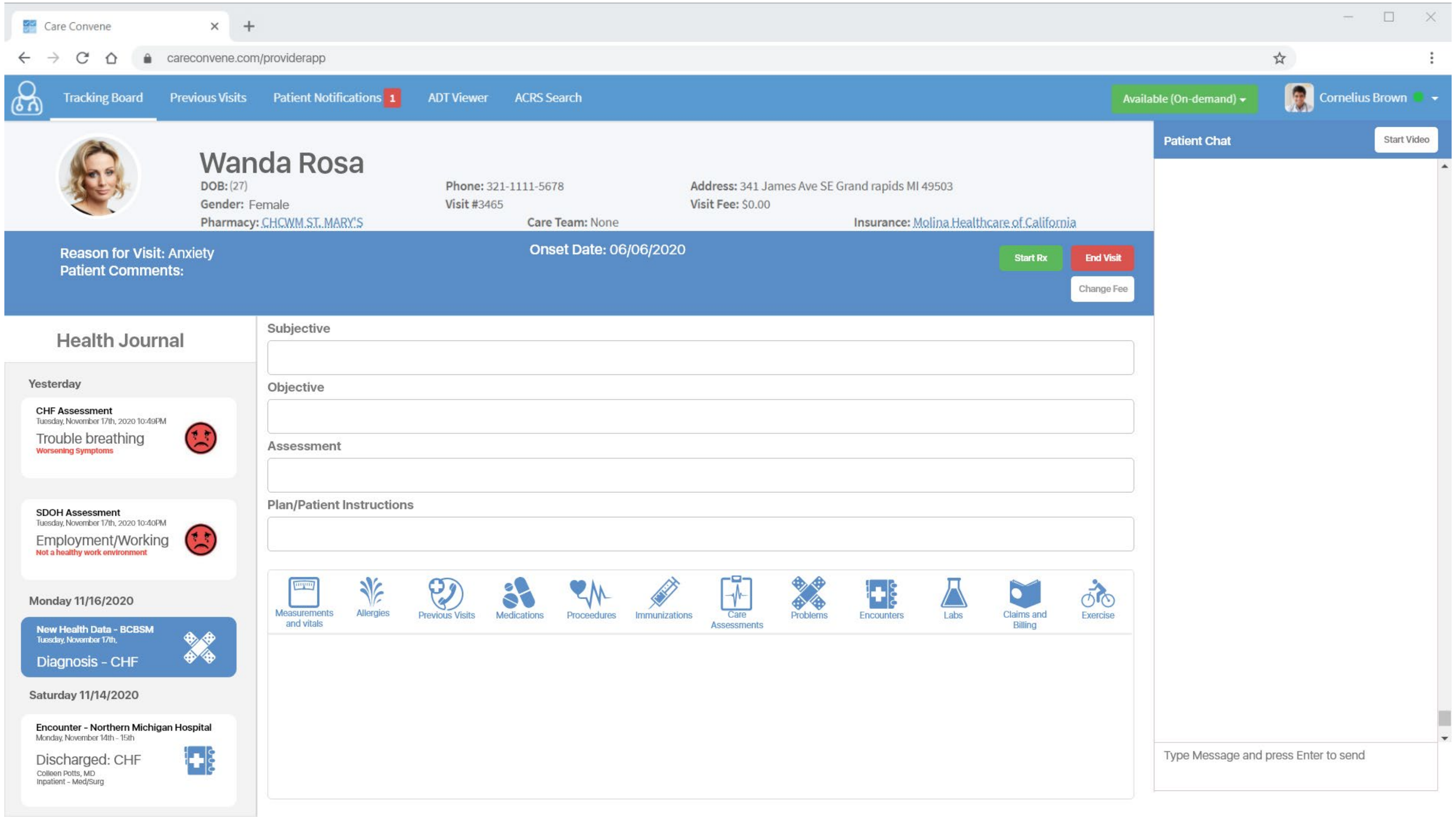
Blue Cross Blue Shield of Michigan

Link Data Provider

New Jersey Health Information Network

Unlink Data Provider

Centralized Patient Record



Wanda Rosa

DOB: (27)
Gender: Female
Pharmacy: CHCWM ST. MARY'S
Phone: 321-1111-5678
Visit #3465
Care Team: None
Address: 341 James Ave SE Grand rapids MI 49503
Visit Fee: $0.00
Insurance: Molina Healthcare of California

Reason for Visit: Anxiety
Patient Comments:
Onset Date: 06/06/2020

Subjective

Objective

Assessment

Plan/Patient Instructions

Health Journal

Yesterday

CHF Assessment
Tuesday, November 17th, 2020 10:49PM
Trouble breathing
Worsening Symptoms

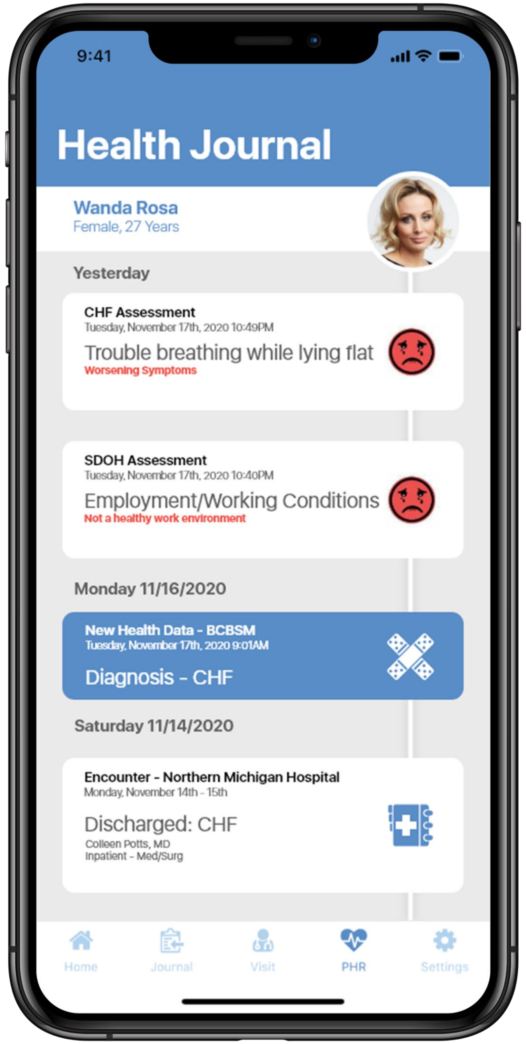
SDOH Assessment
Tuesday, November 17th, 2020 10:40PM
Employment/Working
Not a healthy work environment

Monday 11/16/2020

New Health Data - BCBSM
Tuesday, November 17th,
Diagnosis - CHF

Saturday 11/14/2020

Encounter - Northern Michigan Hospital
Monday, November 14th - 15th
Discharged: CHF
Colleen Potts, MD
Inpatient - Med/Surg



Health Journal

Wanda Rosa
Female, 27 Years

Yesterday

CHF Assessment
Tuesday, November 17th, 2020 10:49PM
Trouble breathing while lying flat
Worsening Symptoms

SDOH Assessment
Tuesday, November 17th, 2020 10:40PM
Employment/Working Conditions
Not a healthy work environment

Monday 11/16/2020

New Health Data - BCBSM
Tuesday, November 17th, 2020 9:01AM
Diagnosis - CHF

Saturday 11/14/2020

Encounter - Northern Michigan Hospital
Monday, November 14th - 15th
Discharged: CHF
Colleen Potts, MD
Inpatient - Med/Surg

FHIR Based Integration within Care Convene

USCDI – US Core Data for Interoperability	Care Convene PHR ready
Allergies & Intolerances	Yes
Medications	Yes
Procedures	Yes
Problems	Yes
Immunizations	Yes
Provenance	Yes
Care Team Members	Yes
Observations	Yes
Patient Demographics	Yes
Medications	Yes
Goals	Yes

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

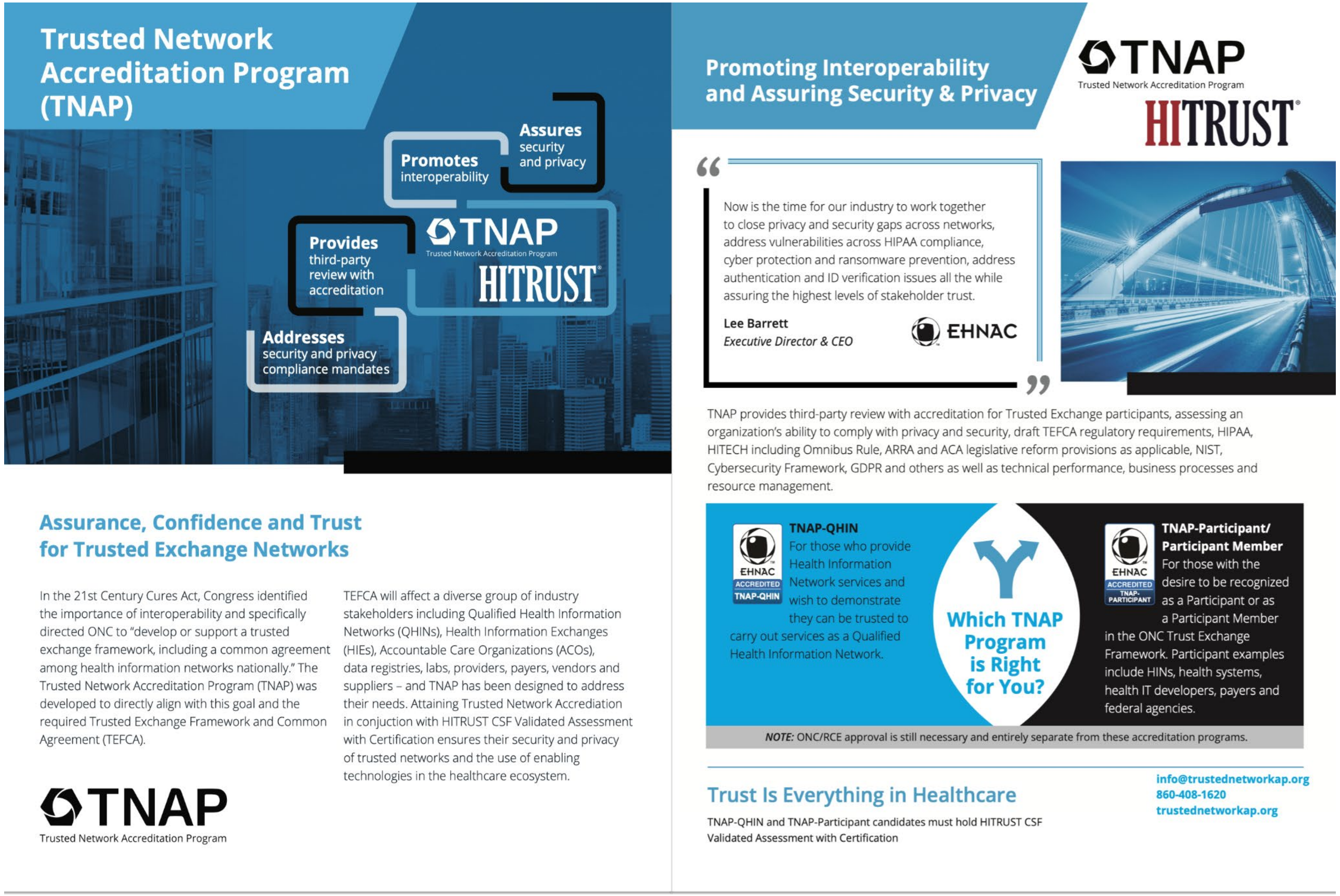
Interoperability

HIPAA/HITECH Omnibus

FHIR Roadmap

Information Blocking

CMS Patient Access Rule



Trusted Network Accreditation Program (TNAP)

Promotes interoperability

Assures security and privacy

Provides third-party review with accreditation

Addresses security and privacy compliance mandates

TNAP
Trusted Network Accreditation Program
HITRUST

Assurance, Confidence and Trust for Trusted Exchange Networks

In the 21st Century Cures Act, Congress identified the importance of interoperability and specifically directed ONC 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. Attaining Trusted Network Accrediation in conjuction with HITRUST CSF Validated Assessment with Certification ensures their security and privacy of trusted networks and the use of enabling technologies in the healthcare ecosystem.

TNAP
Trusted Network Accreditation Program

Promoting Interoperability and Assuring Security & Privacy

TNAP
Trusted Network Accreditation Program
HITRUST

> "Now is the time for our industry to work together to close privacy and security gaps across networks, address vulnerabilities across HIPAA compliance, cyber protection and ransomware prevention, address authentication and ID verification issues all the while assuring the highest levels of stakeholder trust.
>
> **Lee Barrett**
> *Executive Director & CEO*
> EHNAC"

TNAP provides third-party review with accreditation for Trusted Exchange participants, assessing an organization's ability to comply with privacy and security, draft TEFCA regulatory 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.

Which TNAP Program is Right for You?

EHNAC ACCREDITED TNAP-QHIN

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.

EHNAC ACCREDITED TNAP-PARTICIPANT

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

NOTE: ONC/RCE approval is still necessary and entirely separate from these accreditation programs.

Trust Is Everything in Healthcare

TNAP-QHIN and TNAP-Participant candidates must hold HITRUST CSF Validated Assessment with Certification

info@trustednetworkap.org
860-408-1620
trustednetworkap.org

EHNAC

Trusted Dynamic Registration & Authentication Accreditation Program

Trusted Dynamic Registration & Authentication Accreditation Program

The **Trusted Dynamic Registration & Authentication Accreditation Program (TDRAAP)** 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.

EHNAC

UDAP

Developed to support an organization's continued focus on interoperability – a foundational component of the Office of the National Coordinator's (ONC's) Cures Act Final Rule and related CMS Interoperability and Patient Access Final Rule – the program combines technical certification with third-party review of privacy and security, while enabling trust and transparency for organizational and individual access to data.

Two TDRAAP programs options are available: **TDRAAP-Basic** and **TDRAAP-Comprehensive**

EHNAC ACCREDITED TDRAAP-BASIC

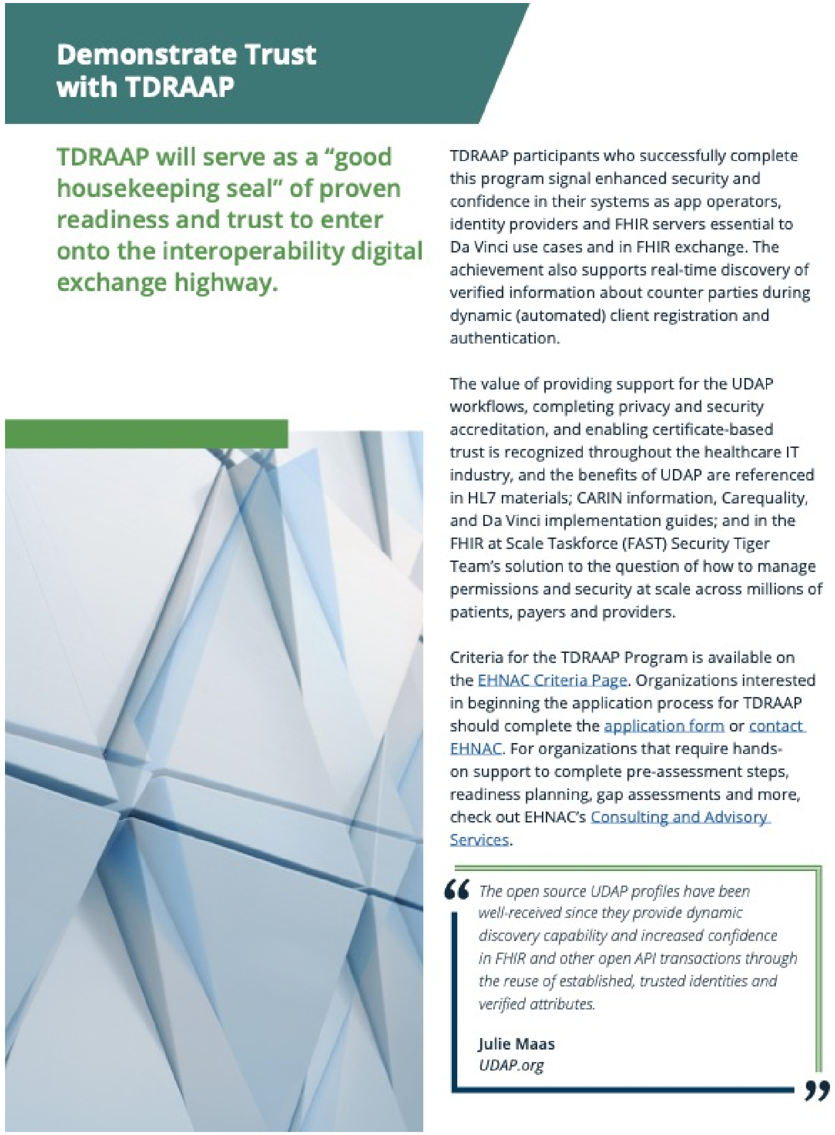
TDRAAP-Basic offers privacy and security self-attestation with minimal validation while the included UDAP technical framework certification demonstrates that an entity's end-to-end API can be trusted by patients and other industry stakeholders. It is designed specifically for developers of consumer-facing apps, also referred to as a patient's "App of their Choice," as used in workflows such as ONC-certified Health IT that include SMART app launch with individual sign-on for FHIR data access by one patient at a time with the patient's own credentials.

EHNAC ACCREDITED TDRAAP-COMPREHENSIVE

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

- Payers
- Providers
- Mobile app developers
- Health Information Exchanges (HIEs)
- Health Information Networks (HINs)
- Financial institutions
- Regulatory agencies
- Defense contractors
- Clearinghouses
- EHR vendors
- Security vendors
- Cloud vendors
- Identity Providers

> *The ability to efficiently register and authenticate endpoints is a core component of interoperability throughout the healthcare information highway. Through the creation of a technical and governance infrastructure, TDRAAP supports interoperability with a specific focus on technical standards enabling trust and transparency for both organizational and individual access to data.*
>
> Lee Barrett
> *Executive Director and Chief Executive Officr*
> EHNAC



Demonstrate Trust with TDRAAP

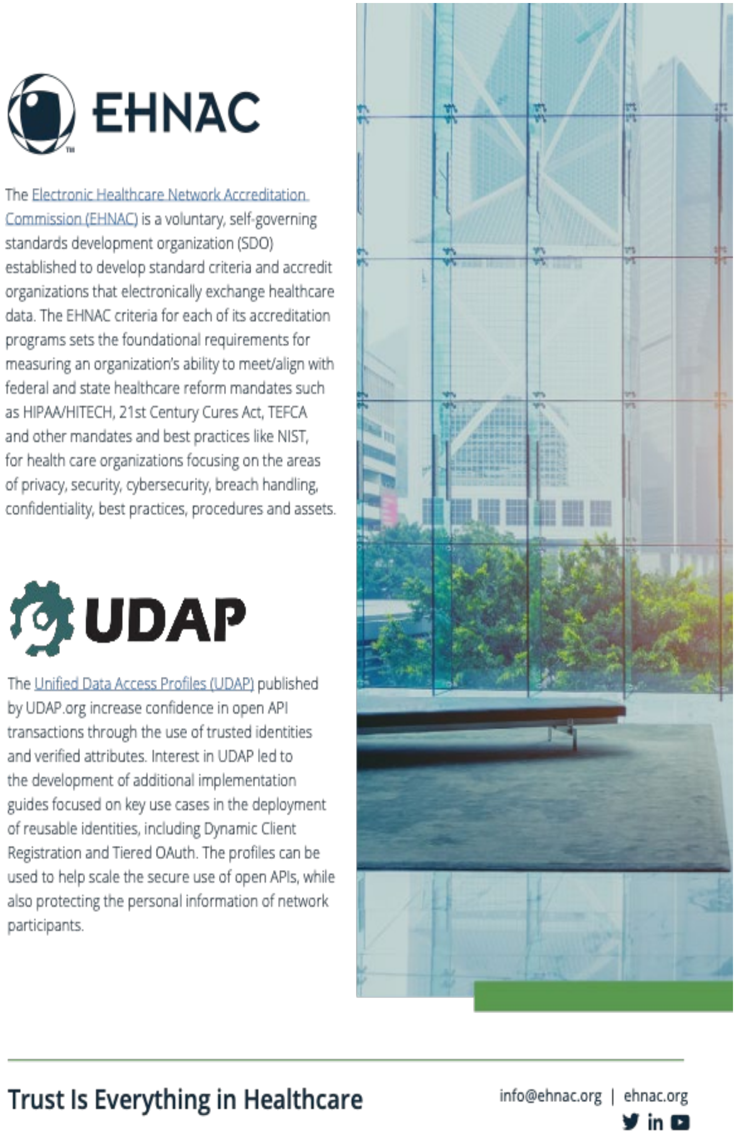
TDRAAP will serve as a "good housekeeping seal" of proven readiness and trust to enter onto the interoperability digital exchange highway.

TDRAAP participants who successfully complete this program signal enhanced security and confidence in their systems as app operators, identity providers and FHIR servers essential to Da Vinci use cases and in FHIR exchange. The achievement also supports real-time discovery of verified information about counter parties during dynamic (automated) client registration and authentication.

The value of providing support for the UDAP workflows, completing privacy and security accreditation, and enabling certificate-based trust is recognized throughout the healthcare IT industry, and the benefits of UDAP are referenced in HL7 materials; CARIN information, Carequality, and Da Vinci implementation guides; and in the FHIR at Scale Taskforce (FAST) Security Tiger Team's solution to the question of how to manage permissions and security at scale across millions of patients, payers and providers.

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 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 reuse of established, trusted identities and verified attributes.*
>
> **Julie Maas**
> *UDAP.org*



EHNAC

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/align 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.

UDAP

The Unified Data Access Profiles (UDAP) published by UDAP.org increase confidence in open API transactions through the use of trusted identities and verified attributes. Interest in UDAP led to the development of additional implementation guides focused on key use cases in the deployment of reusable identities, including Dynamic Client Registration and Tiered OAuth. The profiles can be used to help scale the secure use of open APIs, while also protecting the personal information of network participants.

Trust Is Everything in Healthcare

info@ehnac.org | ehnac.org

Why Is This Program Needed?

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.

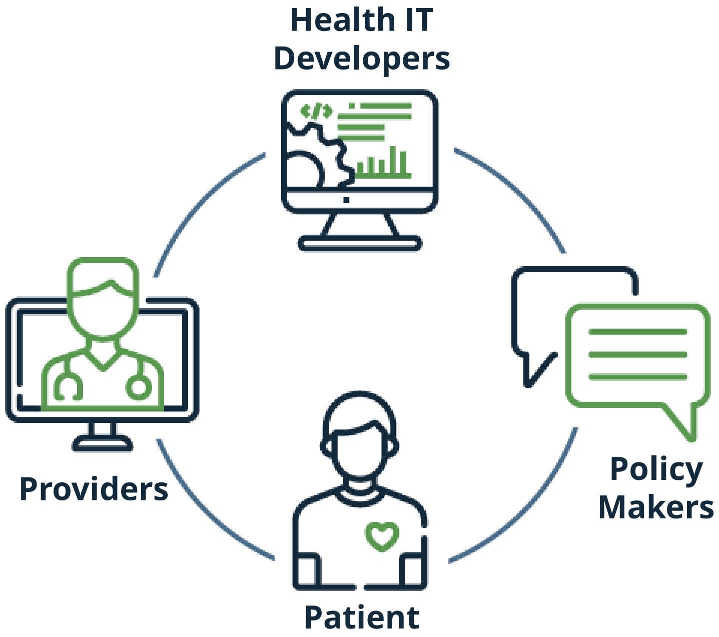
It calls on the healthcare industry to adopt standardized application programming interfaces (APIs), to allow individuals to securely and easily access structured electronic health information using smartphone applications.

- Source: Office of the National Coordinator - healthit.gov

Regulatory Requirements and Industry Need

The rule includes a provision requiring that patients can electronically access all of their electronic health information (EHI), structured and/or unstructured, <u>at no cost.</u>

- Source: Office of the National Coordinator - healthit.gov



CMS Interoperability & Patient Access Rule Goals

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

Privacy, Security & Standards are Core

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).

CMS has adopted the FHIR-based API standards set forth in the 21st Century Cures Act rule at 45 CFR 170.215.

“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

Industry Challenge? An issue of scalability

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.

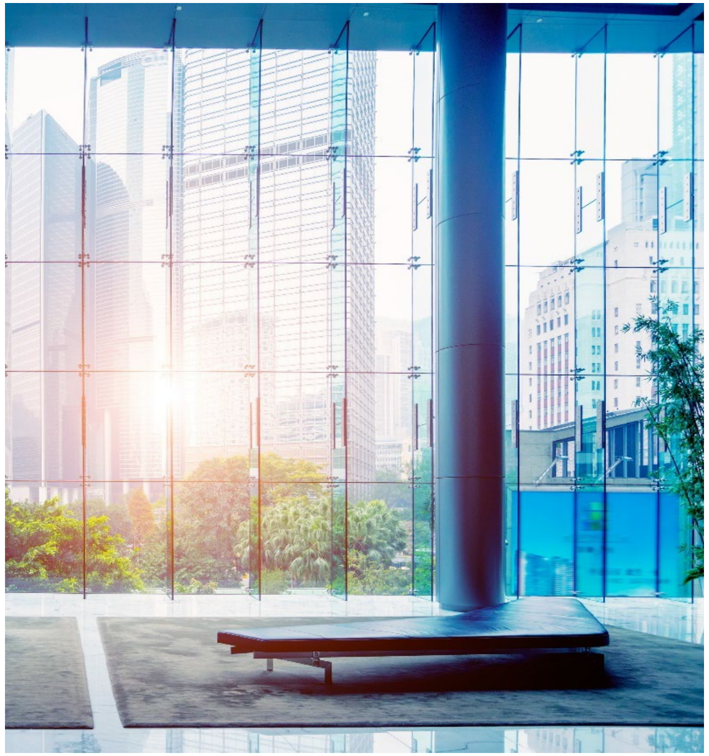
Automation is needed to scale the process of enabling trust between the growing number of Client Apps, Servers and Users. A mechanism to replace the generation and management of single-system “siloed” credentials (for each trio of client app, payer/provider, and individual or other system user) must 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).

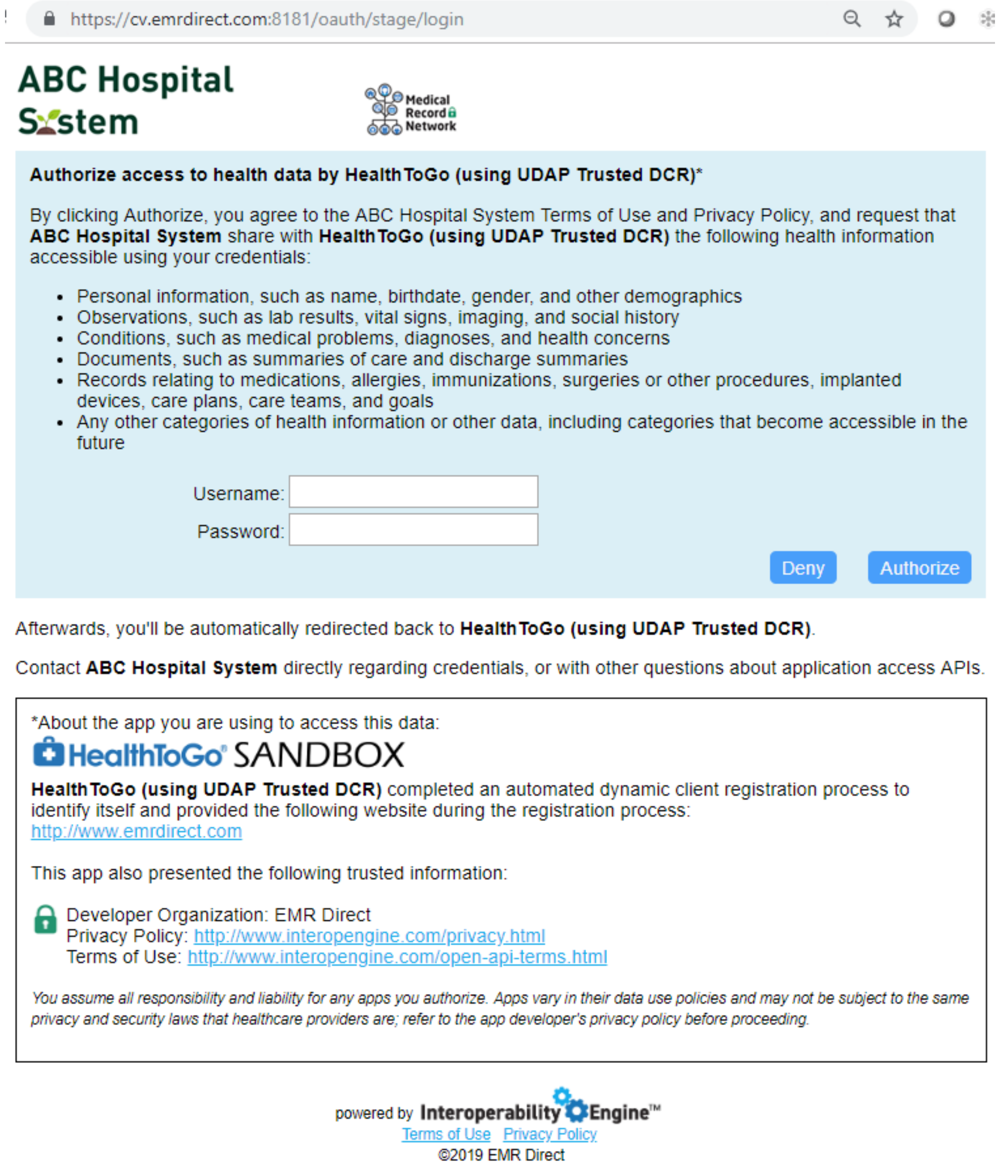
The program enables TDRAAP Certified/Accredited organizations to show they can be TRUSTED in the ecosystem!



EHNAC™

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


https://cv.emrdirect.com:8181/oauth/stage/login
ABC Hospital System
Medical Record Network
Deny
Authorize
HealthToGo SANDBOX
powered by Interoperability Engine™

Authorize access to health data by HealthToGo (using UDAP Trusted DCR)*

By clicking Authorize, you agree to the ABC Hospital System Terms of Use and Privacy Policy, and request that **ABC Hospital System** share with **HealthToGo (using UDAP Trusted DCR)** the following health information accessible using your credentials:

- Personal information, such as name, birthdate, gender, and other demographics
- Observations, such as lab results, vital signs, imaging, and social history
- Conditions, such as medical problems, diagnoses, and health concerns
- Documents, such as summaries of care and discharge summaries
- Records relating to medications, allergies, immunizations, surgeries or other procedures, implanted devices, care plans, care teams, and goals
- Any other categories of health information or other data, including categories that become accessible in the future

Username:

Password:

Afterwards, you'll be automatically redirected back to **HealthToGo (using UDAP Trusted DCR)**.

Contact **ABC Hospital System** directly regarding credentials, or with other questions about application access APIs.

*About the app you are using to access this data:

HealthToGo (using UDAP Trusted DCR) completed an automated dynamic client registration process to identify itself and provided the following website during the registration process:
http://www.emrdirect.com

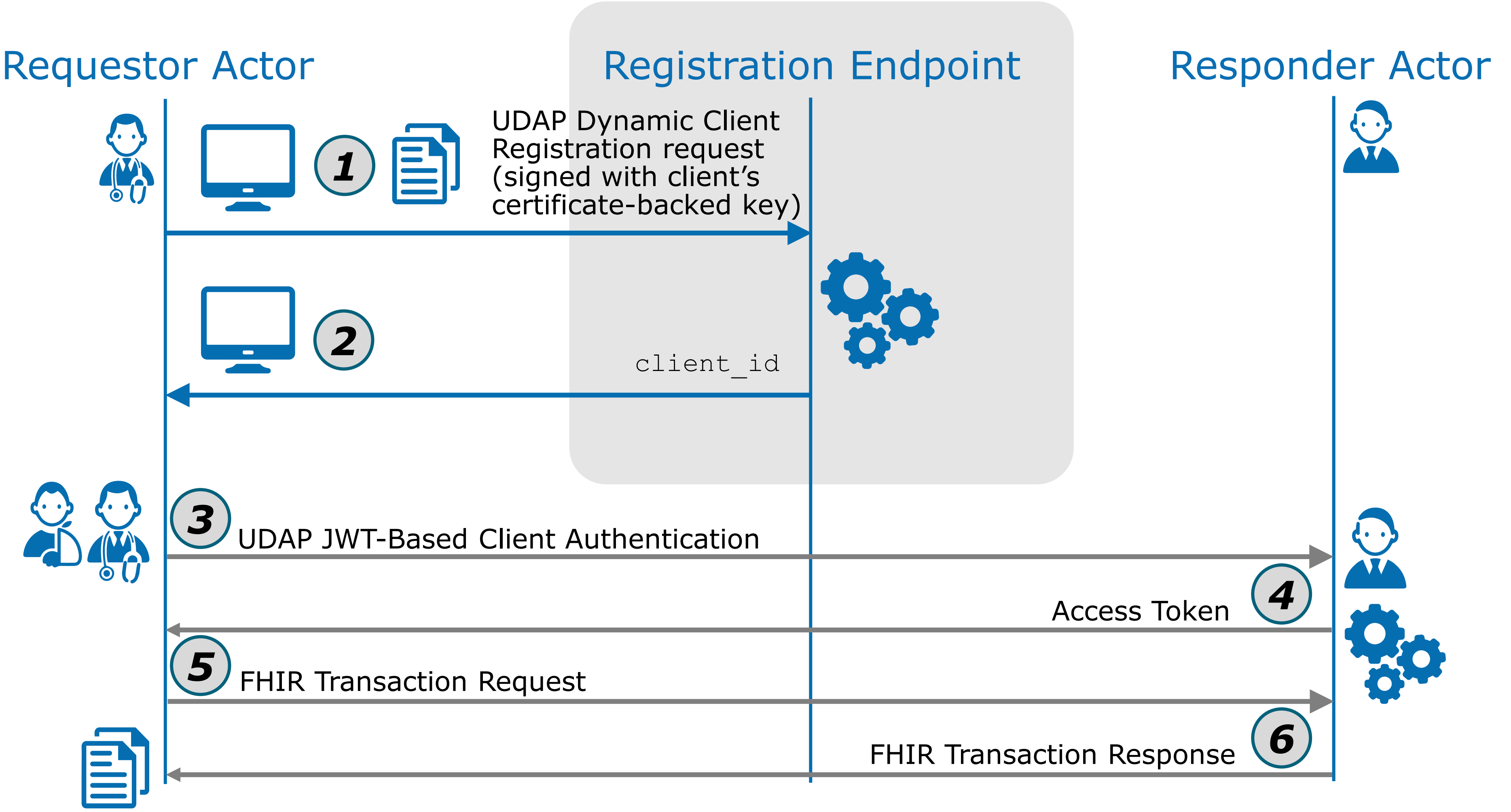
This app also presented the following trusted information:

🔒 Developer Organization: EMR Direct
Privacy Policy: http://www.interopengine.com/privacy.html
Terms of Use: http://www.interopengine.com/open-api-terms.html

You assume all responsibility and liability for any apps you authorize. Apps vary in their data use policies and may not be subject to the same privacy and security laws that healthcare providers are; refer to the app developer's privacy policy before proceeding.

Terms of Use Privacy Policy
©2019 EMR Direct

Ecosystem view


Requestor Actor
Registration Endpoint
Responder Actor
1
UDAP Dynamic Client Registration request (signed with client's certificate-backed key)
2
client_id
3
UDAP JWT-Based Client Authentication
4
Access Token
5
FHIR Transaction Request
6
FHIR Transaction Response

Art credit: adapted from ONC FAST Security TLC Webinar

EMR Direct
SIMPLIFYING INTEROPERABILITY

EHNAC

Trusted Dynamic Client Registration

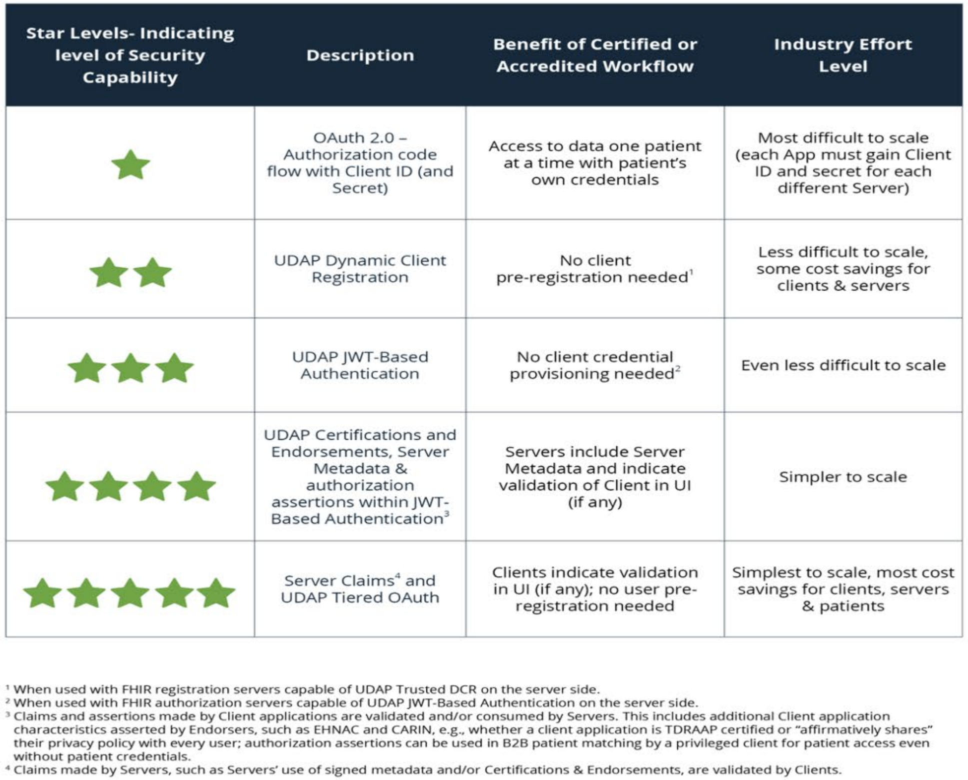
- Public Key registration for JWT-Based Authentication of Client Apps
  - extends standard (and common) OAuth 2.0 and OpenID Connect technologies
  - backed by Digital Certificates
  - supports client credentials flow OR authorization code flow
- Server Validation
  - including multi-tenant environments
- 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

EHNAC™
CERTIFIED
TDRAAP-BASIC

EHNAC™
ACCREDITED
TDRAAP-COMPREHENSIVE



Star Levels- Indicating level of Security Capability	Description	Benefit of Certified or Accredited Workflow	Industry Effort Level
★	OAuth 2.0 – Authorization code flow with Client ID (and Secret)	Access to data one patient at a time with patient's own credentials	Most difficult to scale (each App must gain Client ID and secret for each different Server)
★★	UDAP Dynamic Client Registration	No client pre-registration needed[1]	Less difficult to scale, some cost savings for clients & servers
★★★	UDAP JWT-Based Authentication	No client credential provisioning needed[2]	Even less difficult to scale
★★★★	UDAP Certifications and Endorsements, Server Metadata & authorization assertions within JWT-Based Authentication[3]	Servers include Server Metadata and indicate validation of Client in UI (if any)	Simpler to scale
★★★★★	Server Claims[4] and UDAP Tiered OAuth	Clients indicate validation in UI (if any); no user pre-registration needed	Simplest to scale, most cost savings for clients, servers & patients

[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 shares" their privacy policy with every user; authorization assertions can be used in B2B patient matching by a privileged client for patient access even without patient credentials.
[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!