Open@Epic
CONFERENCE 2025

Access Granted: OAuth 2.0 Unlocked

Presenters

Ben Young

MyChart

Rob Klootwyk

Care Everywhere

Rashid Kolaghassi

Interconnect

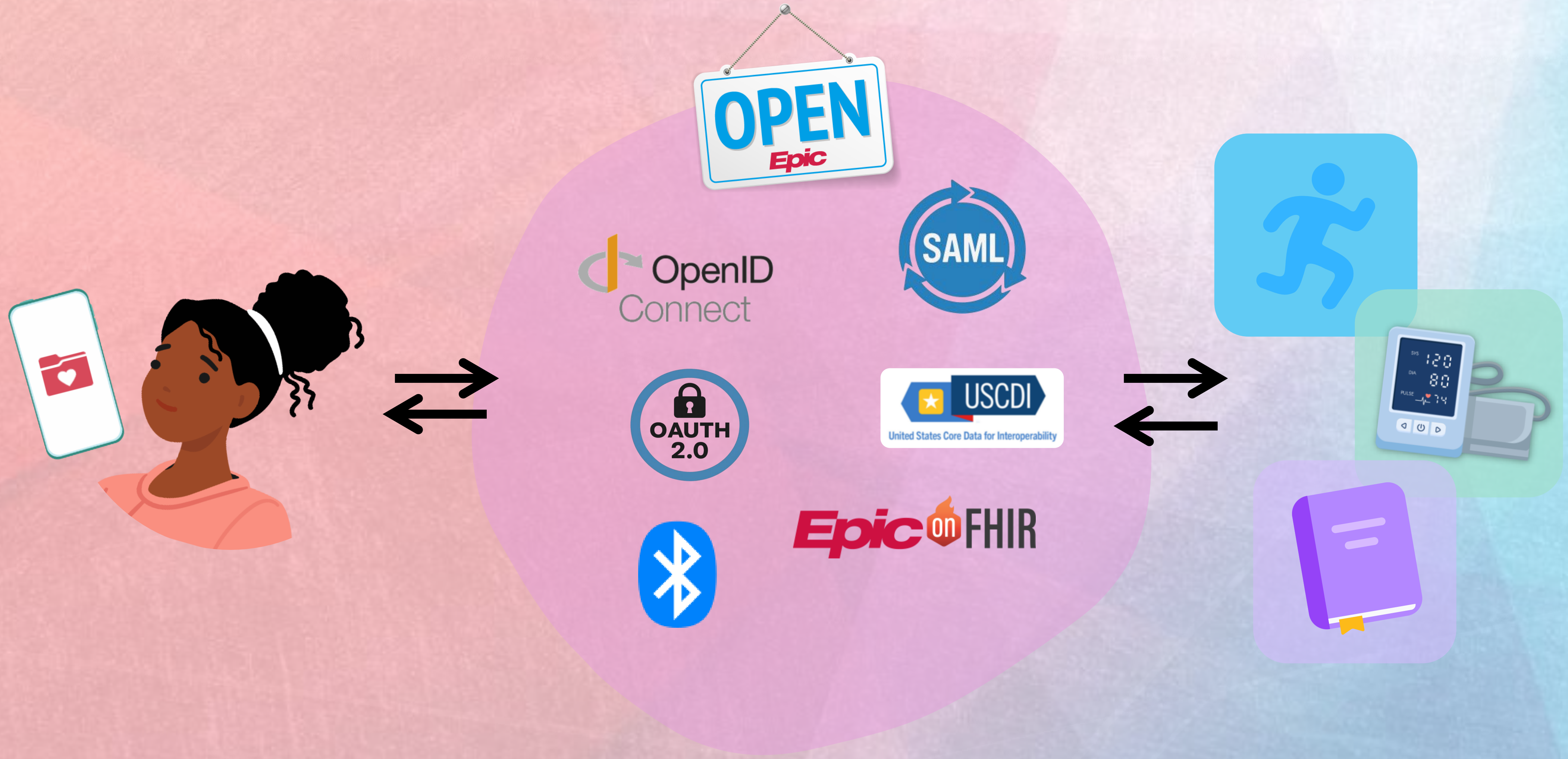
Learning Objectives

1. Understand why health systems leverage **OAuth 2.0 for Interoperability**

2. Explore how applications use **OAuth 2.0 to access data in healthcare**

3. Learn Epic's **roadmap** for patient-facing app authorization

Patient-Mediated Interoperability



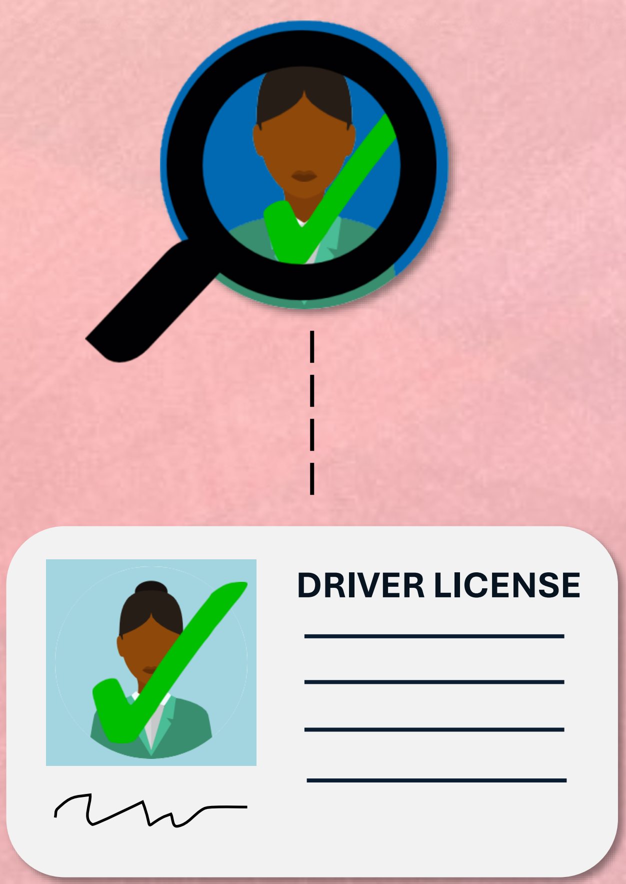
Pillars of Patient-Driven Sharing

Identity Verification

Patient Matching

Patient Choice

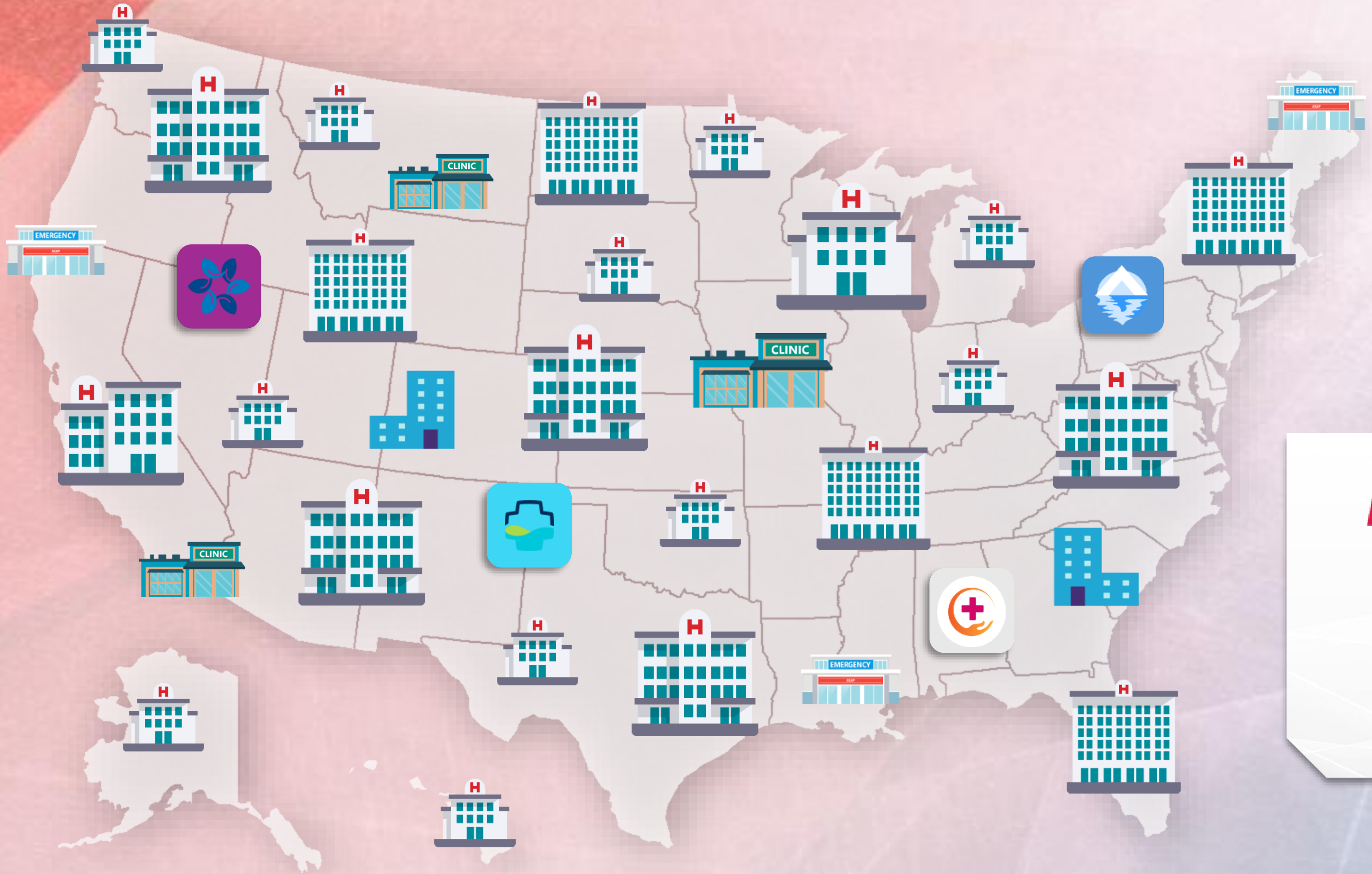
ID Verification



Patient Matching

Patient Choice

OAuth 2.0 and TEFCA™



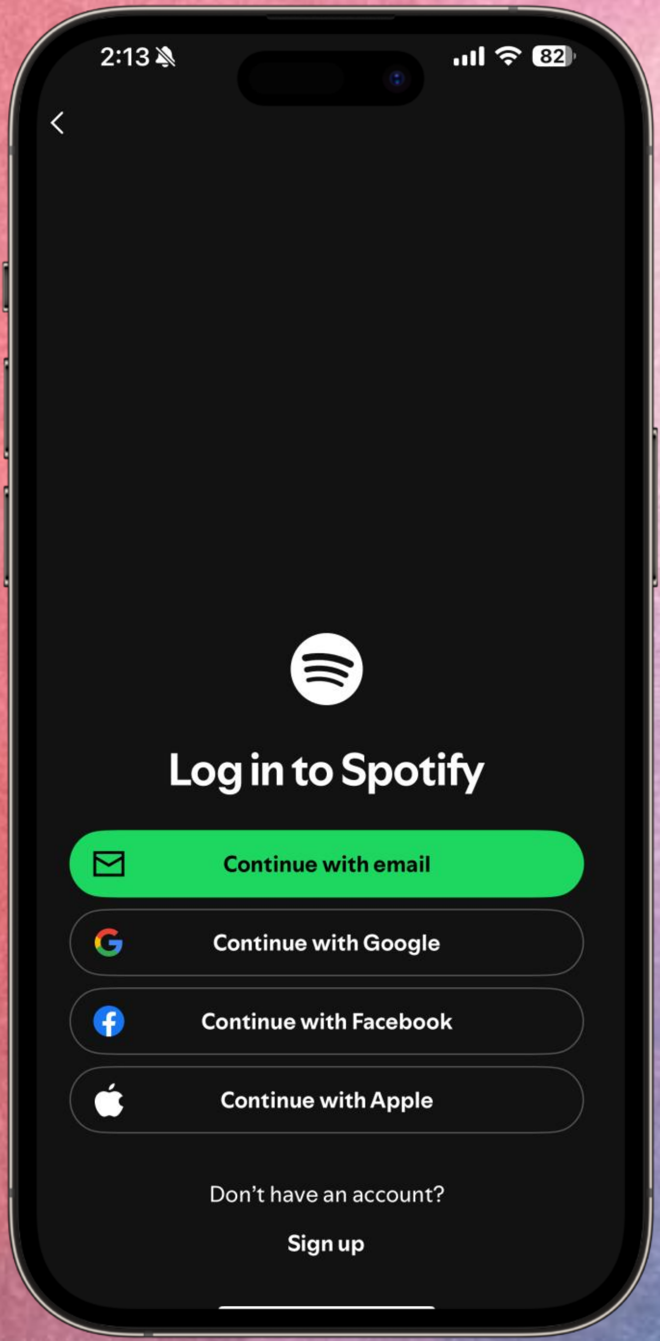
Epic Community Adoption:

2,300 Hospitals

55,000 Clinics

OAuth 2.0 in ***Everyday Life***

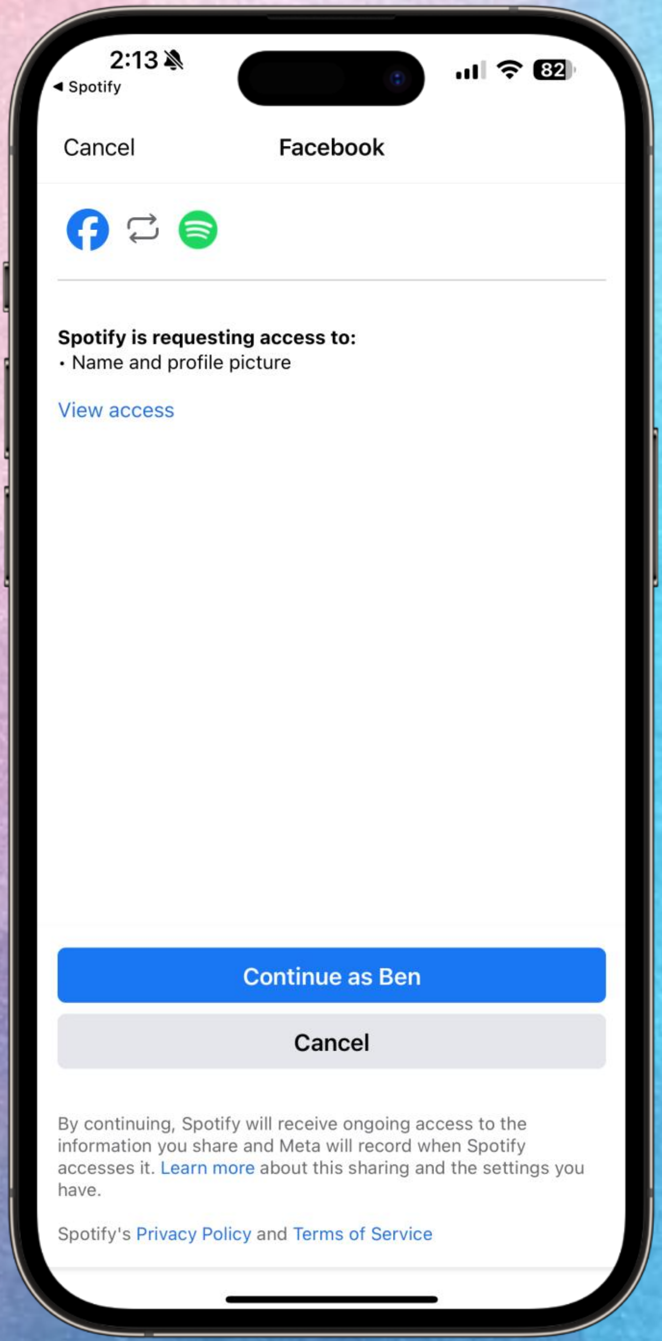
Powering Consumer Logins



Log in to Spotify

Don't have an account?

Sign up

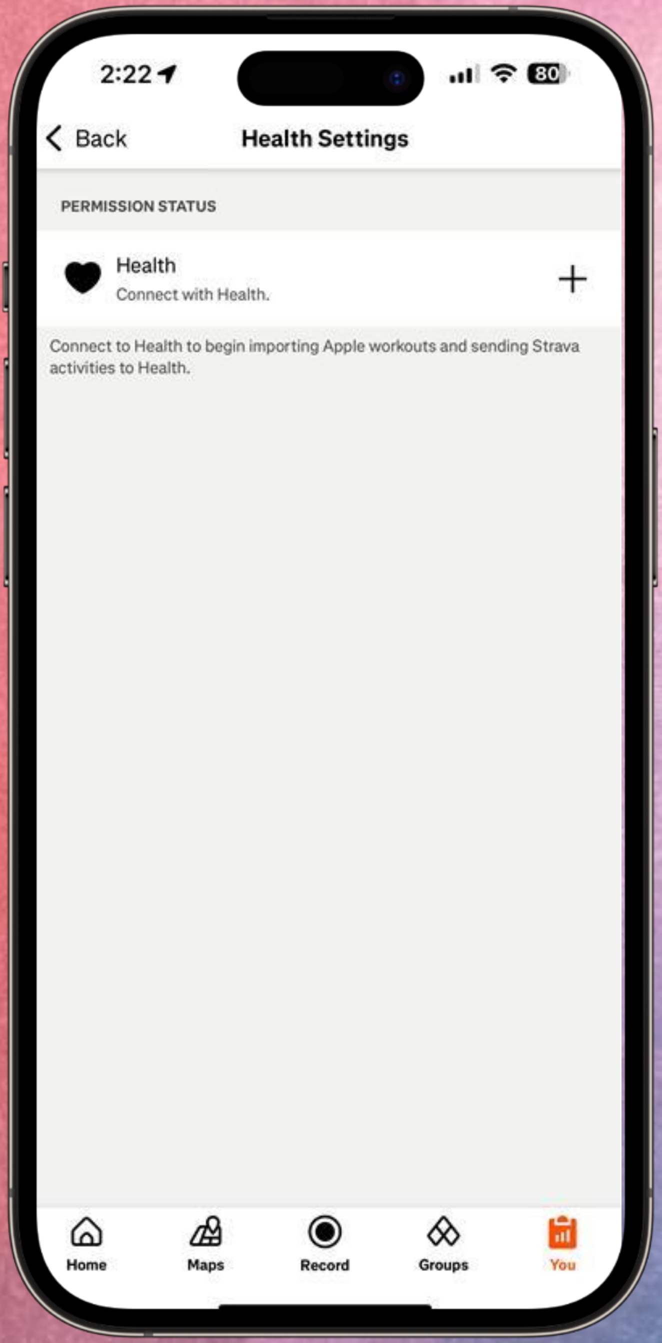


Spotify is requesting access to:
- Name and profile picture

By continuing, Spotify will receive ongoing access to the information you share and Meta will record when Spotify accesses it. Learn more about this sharing and the settings you have.

Spotify's Privacy Policy and Terms of Service

Fitness

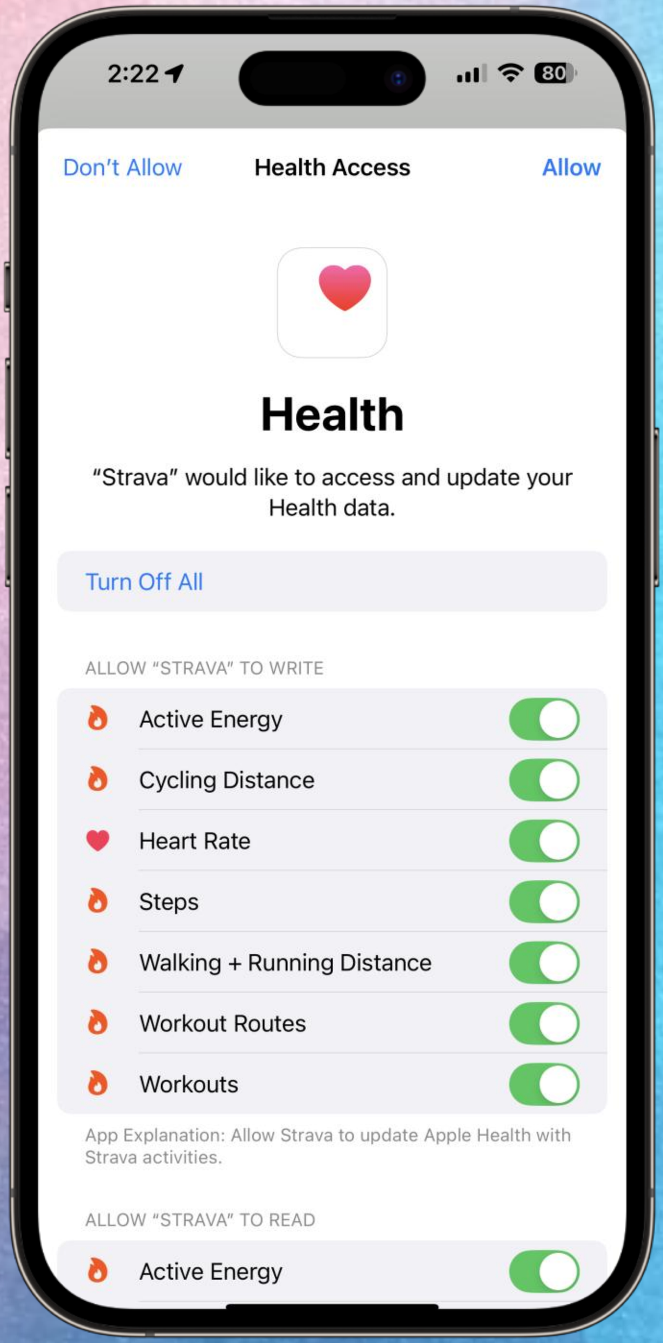


< Back **Health Settings**

PERMISSION STATUS

Health
Connect with Health. +

Connect to Health to begin importing Apple workouts and sending Strava activities to Health.



Don't Allow **Health Access** Allow

Health

"Strava" would like to access and update your Health data.

Turn Off All

ALLOW "STRAVA" TO WRITE

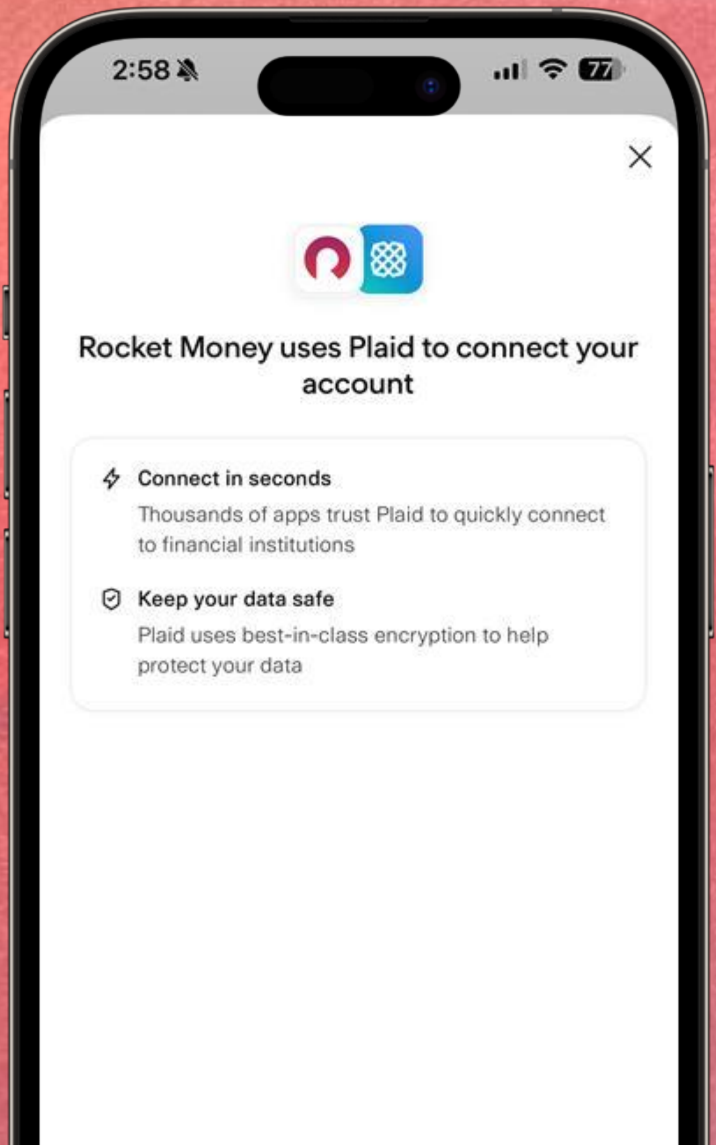
- Active Energy ☑
- Cycling Distance ☑
- Heart Rate ☑
- Steps ☑
- Walking + Running Distance ☑
- Workout Routes ☑
- Workouts ☑

App Explanation: Allow Strava to update Apple Health with Strava activities.

ALLOW "STRAVA" TO READ

- Active Energy ☑

Finance



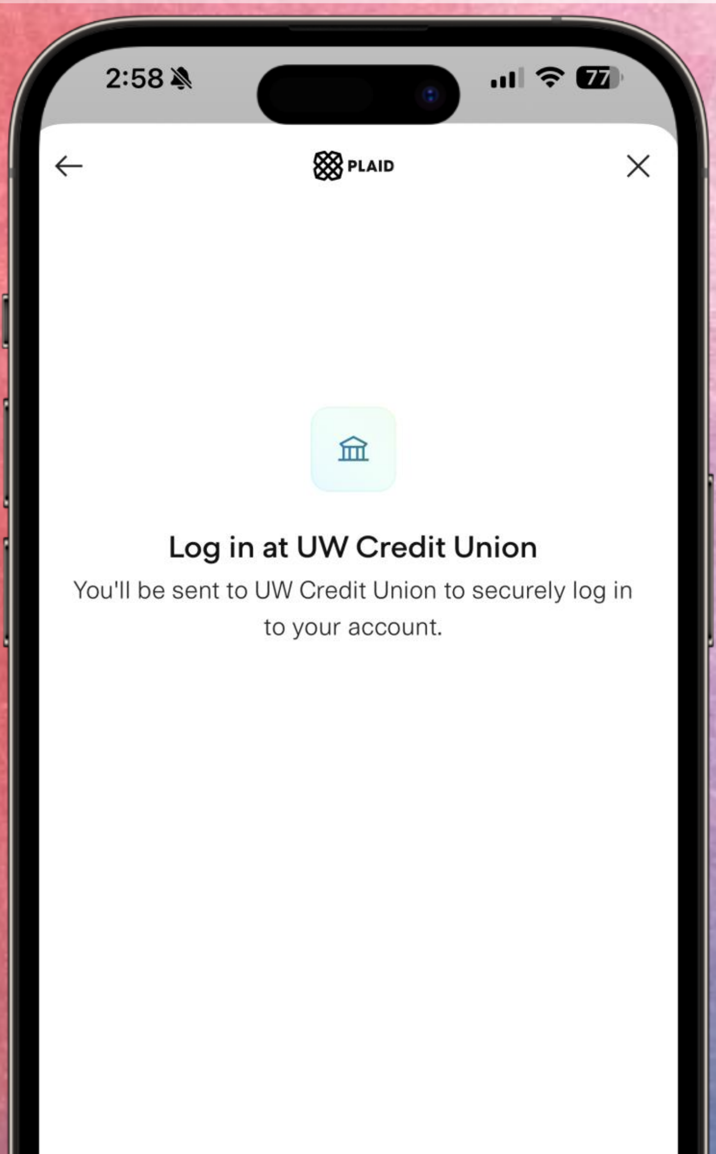
Rocket Money uses Plaid to connect your account

Connect in seconds

Thousands of apps trust Plaid to quickly connect to financial institutions

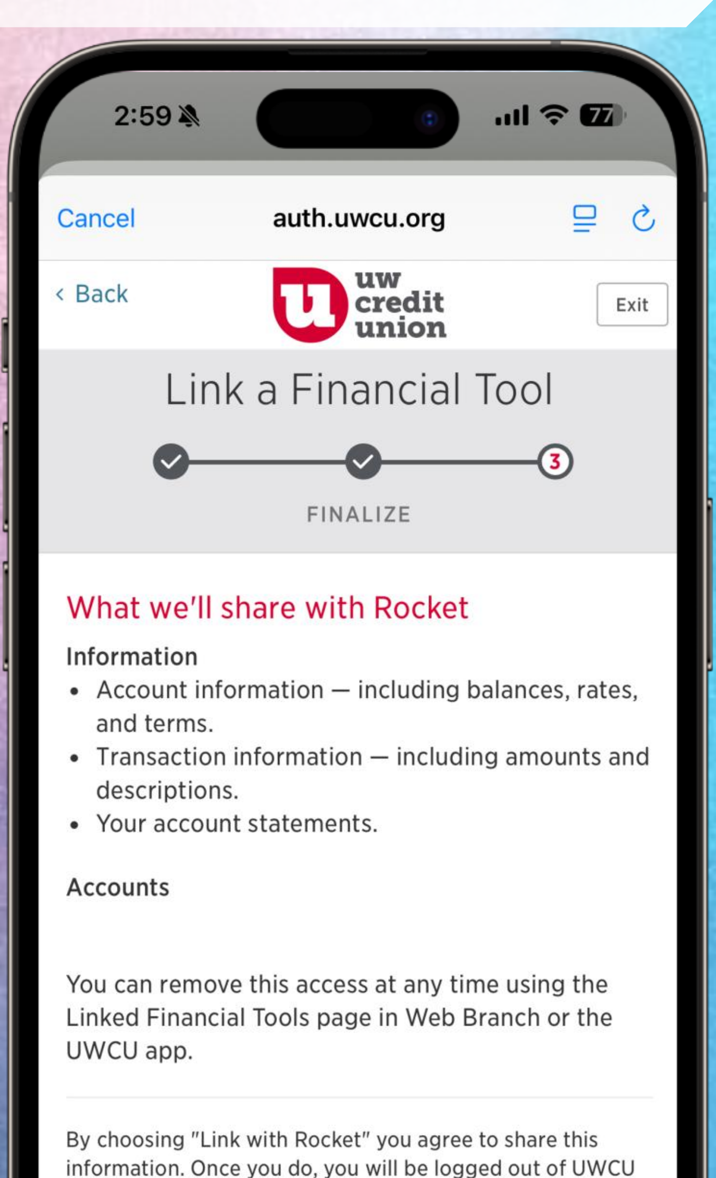
Keep your data safe

Plaid uses best-in-class encryption to help protect your data



Log in at UW Credit Union

You'll be sent to UW Credit Union to securely log in to your account.



Link a Financial Tool

FINALIZE

What we'll share with Rocket

Information

- Account information — including balances, rates, and terms.
- Transaction information — including amounts and descriptions.
- Your account statements.

Accounts

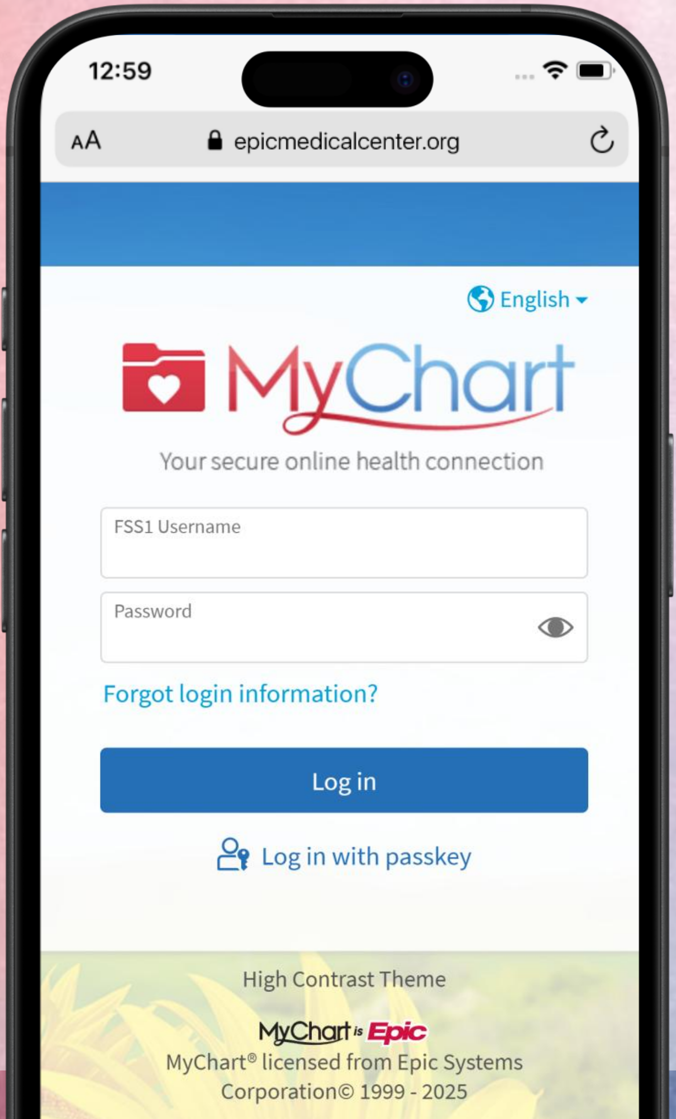
You can remove this access at any time using the Linked Financial Tools page in Web Branch or the UWCU app.

By choosing "Link with Rocket" you agree to share this information. Once you do, you will be logged out of UWCU

OAuth 2.0 for ***Patients***

Step 1: Authentication

1. **Authenticate with Credential of Choice**
   - Biometrics
   - Password
   - Email/SMS
2. **Select a patient**



12:59

epicmedicalcenter.org

English

MyChart

Your secure online health connection

FSS1 Username

Password

Forgot login information?

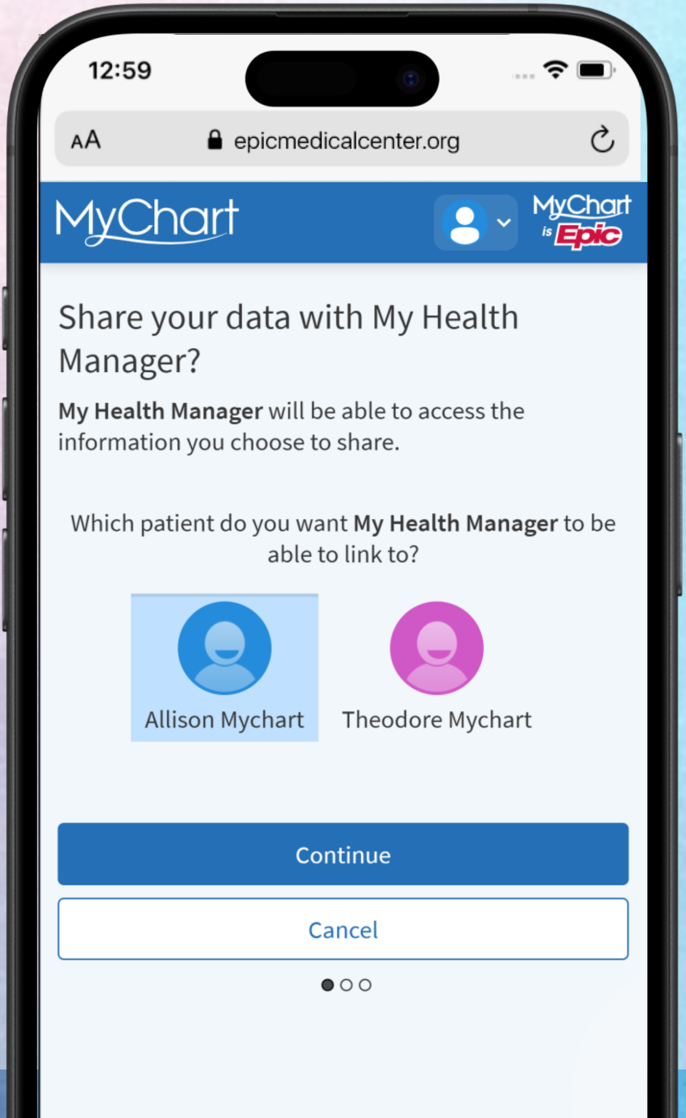
Log in

Log in with passkey

High Contrast Theme

MyChart is Epic

MyChart® licensed from Epic Systems Corporation© 1999 - 2025



12:59

epicmedicalcenter.org

MyChart

MyChart is Epic

Share your data with My Health Manager?

My Health Manager will be able to access the information you choose to share.

Which patient do you want **My Health Manager** to be able to link to?

Allison Mychart

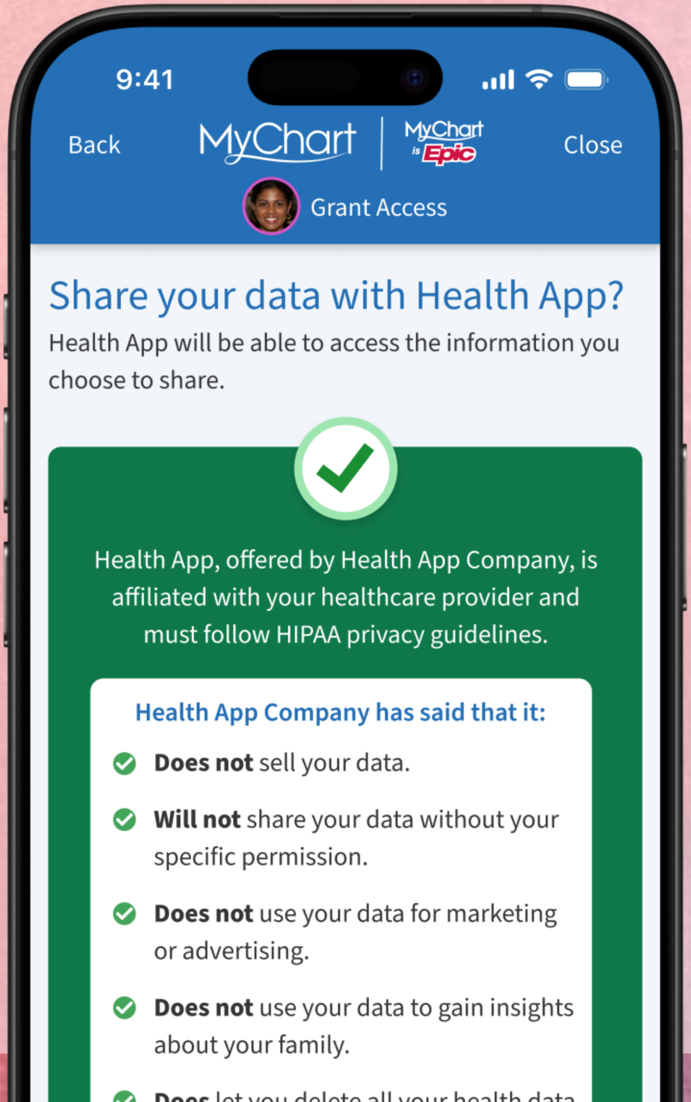
Theodore Mychart

Continue

Cancel

● ○ ○

Step 2: Data Usage Questionnaire



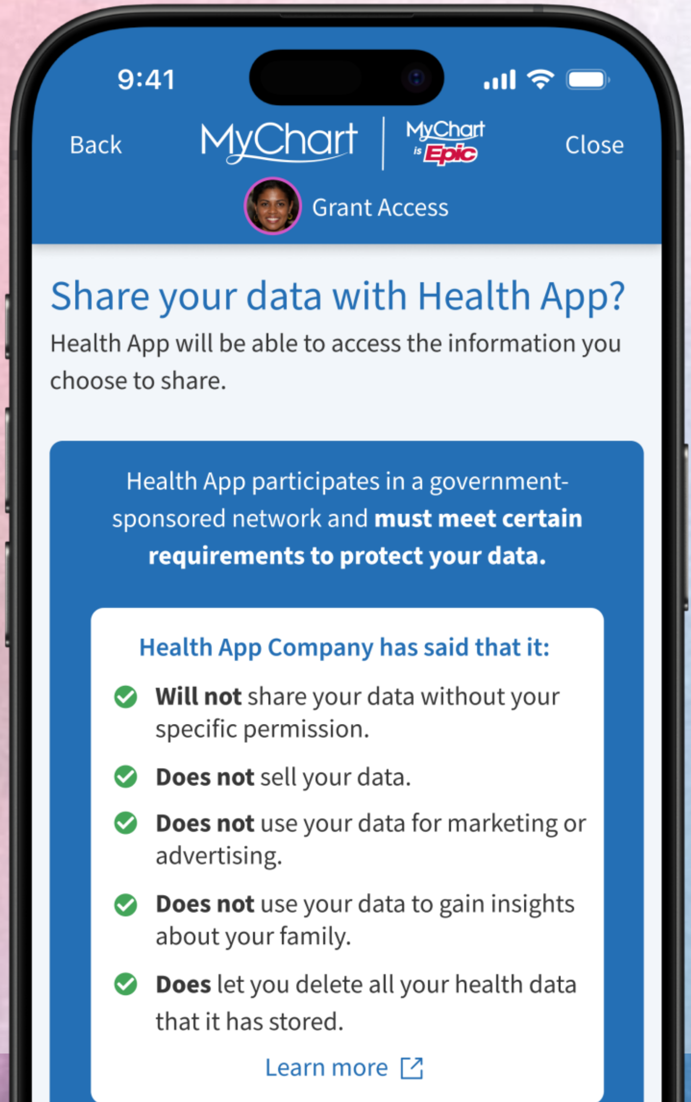
Share your data with Health App?

Health App will be able to access the information you choose to share.

Health App, offered by Health App Company, is affiliated with your healthcare provider and must follow HIPAA privacy guidelines.

Health App Company has said that it:

- ✓ **Does not** sell your data.
- ✓ **Will not** share your data without your specific permission.
- ✓ **Does not** use your data for marketing or advertising.
- ✓ **Does not** use your data to gain insights about your family.
- ✓ **Does** let you delete all your health data



Share your data with Health App?

Health App will be able to access the information you choose to share.

Health App participates in a government-sponsored network and **must meet certain requirements to protect your data.**

Health App Company has said that it:

- ✓ **Will not** share your data without your specific permission.
- ✓ **Does not** sell your data.
- ✓ **Does not** use your data for marketing or advertising.
- ✓ **Does not** use your data to gain insights about your family.
- ✓ **Does** let you delete all your health data that it has stored.

Learn more

Patient Attitudes Toward Data Sharing

Pew

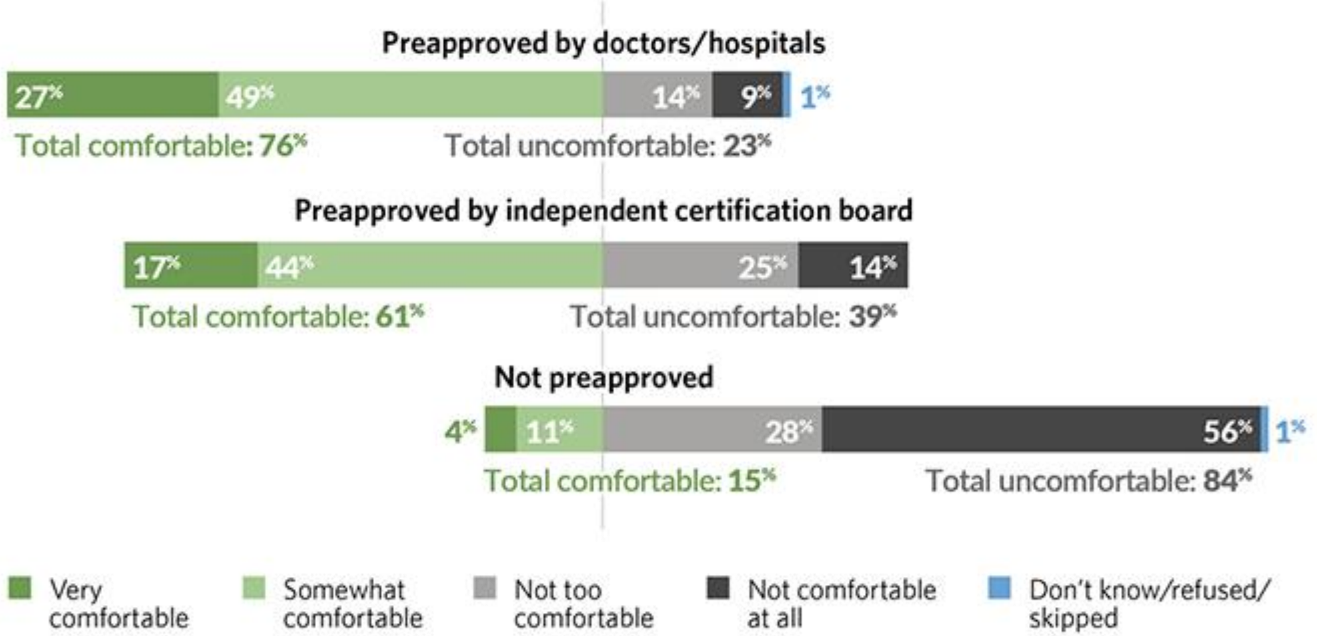
July 2021

Surveyed patients were 44% less likely to be concerned about sharing their health data with an app if its covered by HIPAA

Figure 1

Apps Without Provider or Independent Approval Viewed Skeptically

Respondents' level of comfort downloading health data to apps

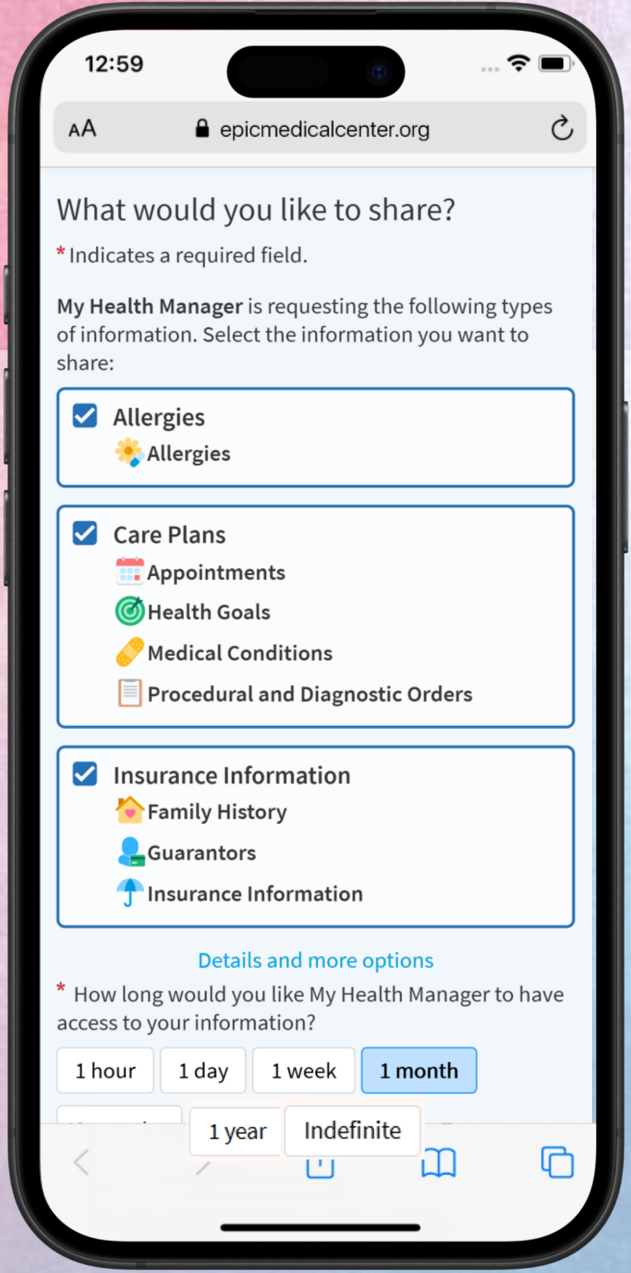


Note: The question stated: "Please indicate how comfortable you would feel downloading and storing your medical information and data on the different types of health apps that you select to use on your smart phone, computer or tablet with the specifications below."

© 2021 The Pew Charitable Trusts

Step 3: Scope and Duration Selection

- Added in response to 21st Century Cures
- Gives proxies and patients granular control over what data is shared



12:59

AA epicmedicalcenter.org

What would you like to share?

* Indicates a required field.

My Health Manager is requesting the following types of information. Select the information you want to share:

☑ Allergies
- Allergies

☑ Care Plans
- Appointments
- Health Goals
- Medical Conditions
- Procedural and Diagnostic Orders

☑ Insurance Information
- Family History
- Guarantors
- Insurance Information

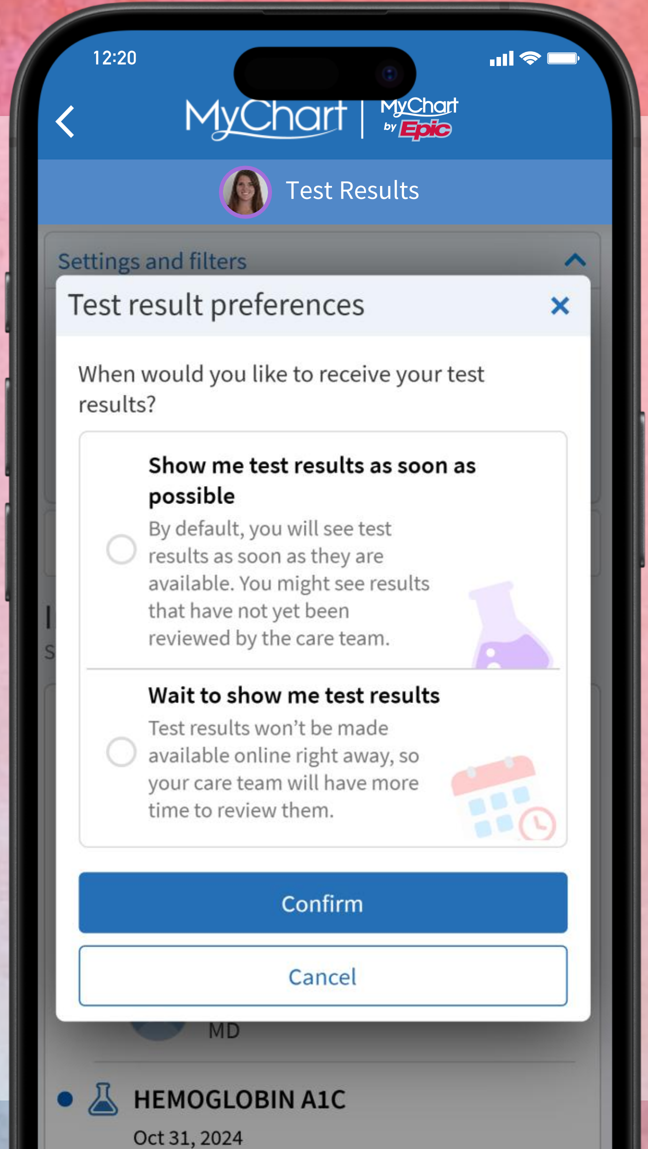
Details and more options

* How long would you like My Health Manager to have access to your information?

1 hour | 1 day | 1 week | [✓ 1 month] | 1 year | Indefinite

Respecting Patient Preferences

- Granular Access for Parents and Proxies
- Exclude irrelevant information
- Navigate state specific laws



Test result preferences

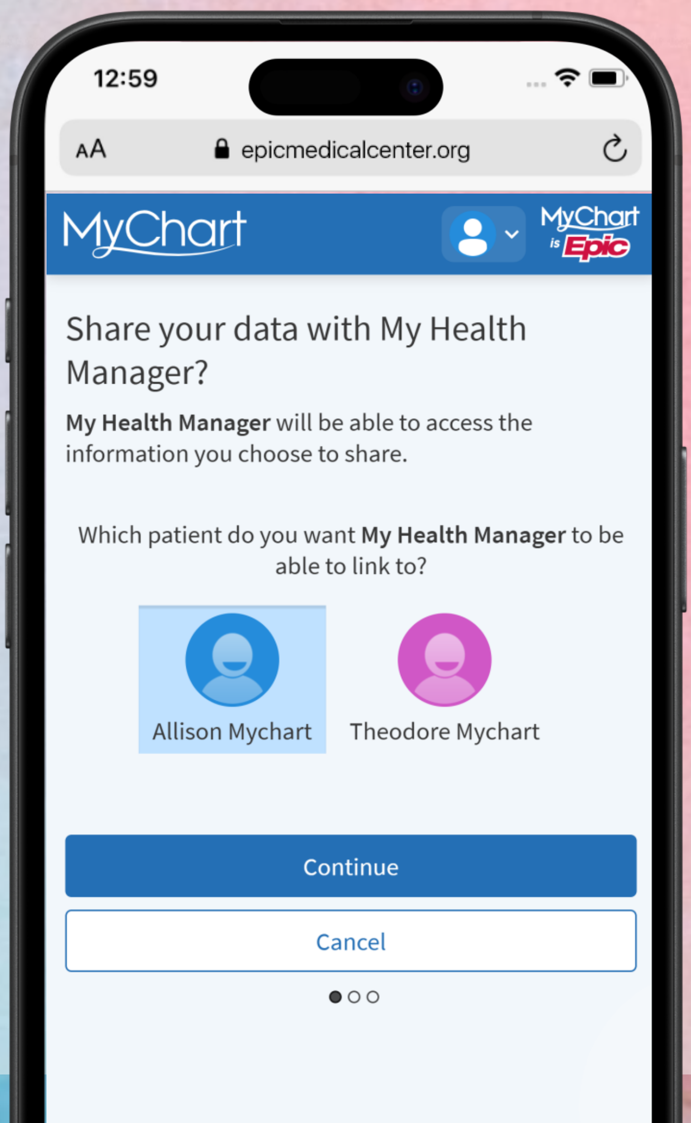
When would you like to receive your test results?

○ **Show me test results as soon as possible**
By default, you will see test results as soon as they are available. You might see results that have not yet been reviewed by the care team.

○ **Wait to show me test results**
Test results won't be made available online right away, so your care team will have more time to review them.

OAuth 2.0 in a Nutshell

Health app, what meds do I need to take today?



Share your data with My Health Manager?

My Health Manager will be able to access the information you choose to share.

Which patient do you want **My Health Manager** to be able to link to?

Allison Mychart

Theodore Mychart

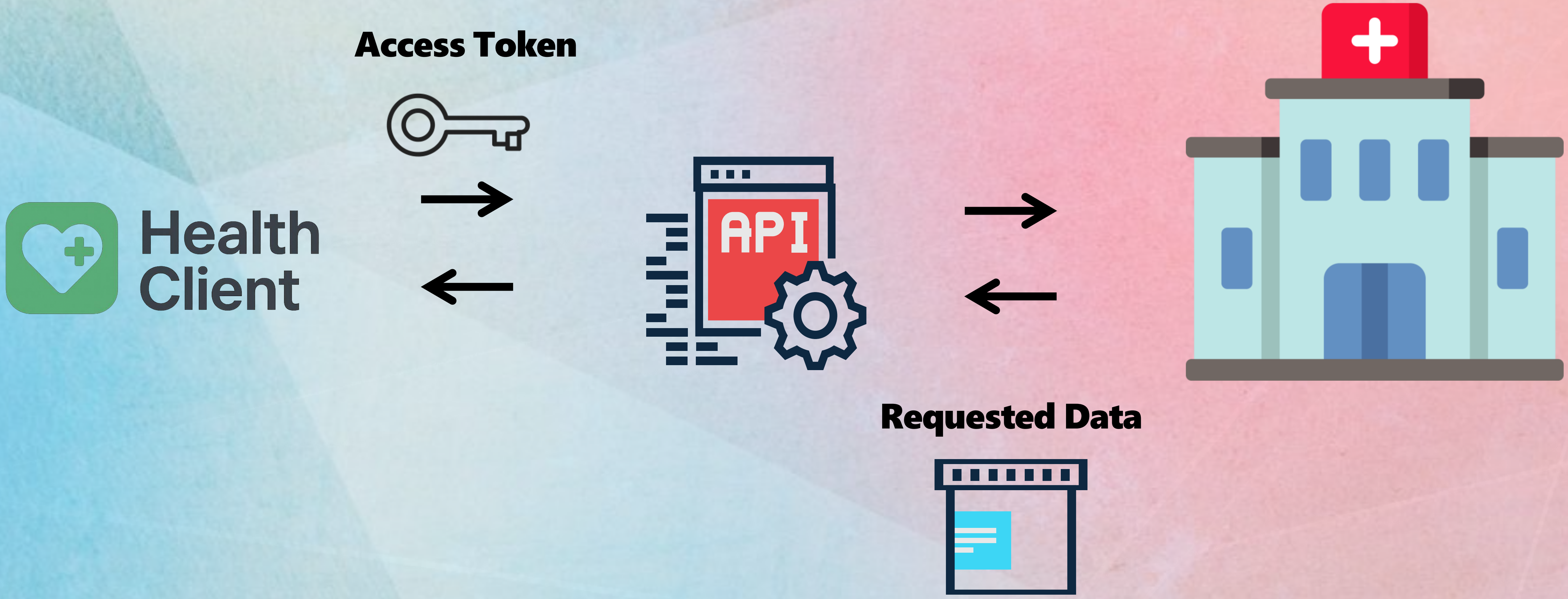
Continue

Cancel

● ○ ○

Can I get an access token to check?

OAuth 2.0 in a Nutshell



Access Token

Health Client

Requested Data

OAuth 2.0 in a Nutshell

Actors

Define who does what

Workflow

How access tokens are obtained

Security

How messages are exchanged securely

Authentication Layer

How identity is communicated

Building on OAuth 2.0

Scopes

Define what data the client can access

Standardized APIs

Common data format

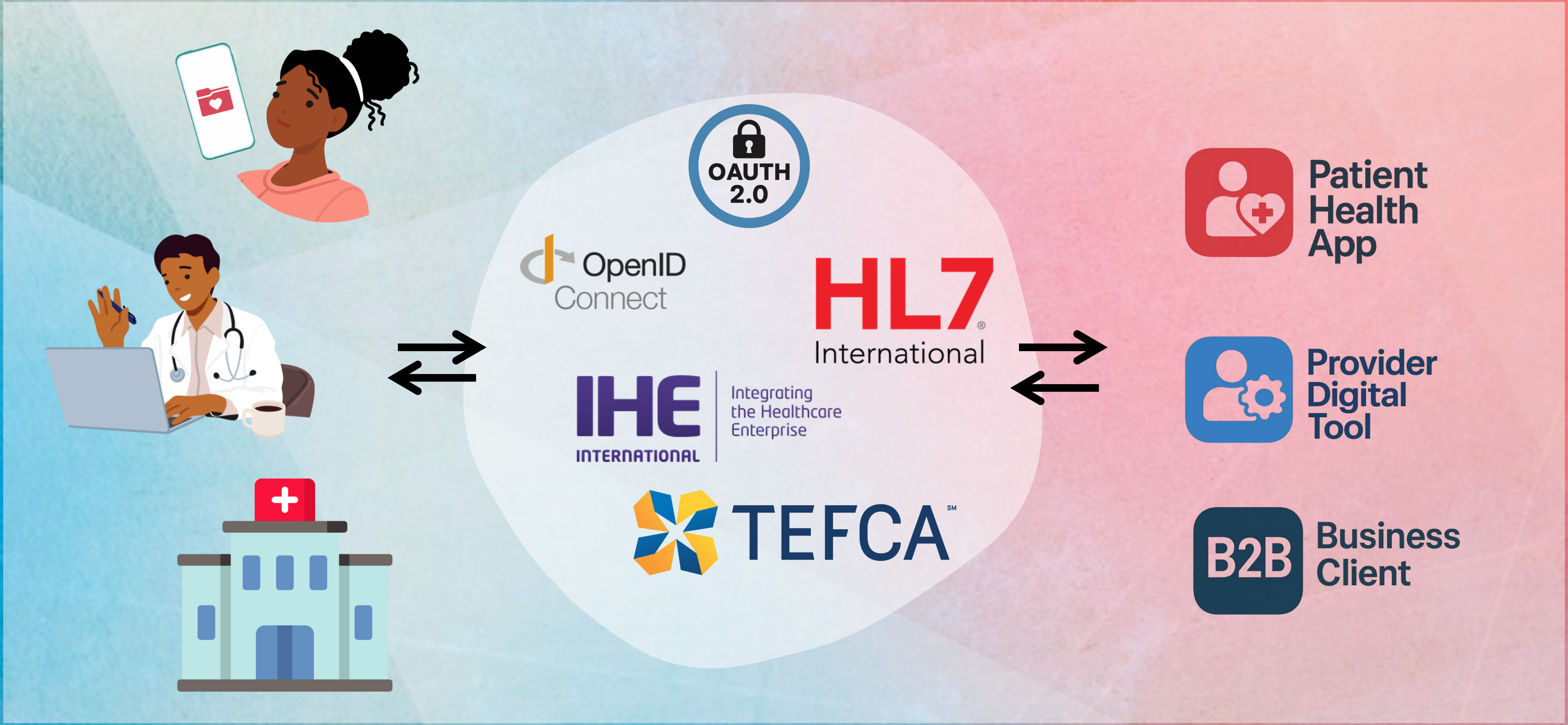
Context

Support users within their workflow

Scale

Expand across systems

Building on OAuth 2.0



Patient Health App

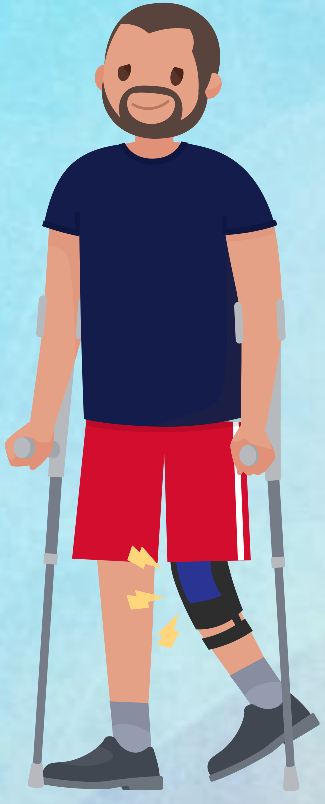
Provider Digital Tool

Business Client

138 Billion

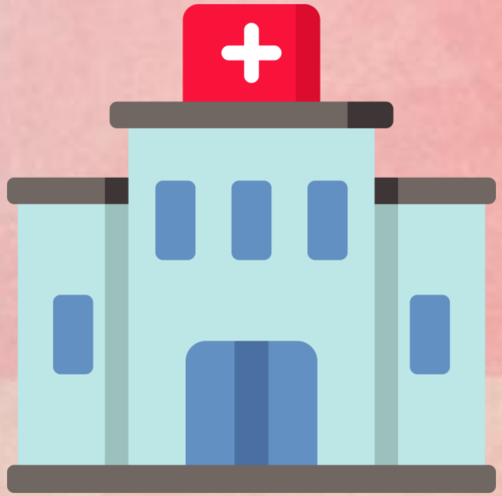
FHIR API Calls Last Year

Healthcare's Use of OAuth 2.0



Patients

Providers



B2B

Your Role in OAuth 2.0

Health
Client

Your Role in OAuth 2.0

Patient Health App

Patients

Provider Digital Tool

Providers

B2B Business Client

B2B

Steps for Trusted Data Exchange

with OAuth 2.0

1. User Registration
2. Client Registration
3. Data Request
4. Authentication
5. Patient Matching
6. Consent & Authorization
7. Data Exchange

User Registration

Step:

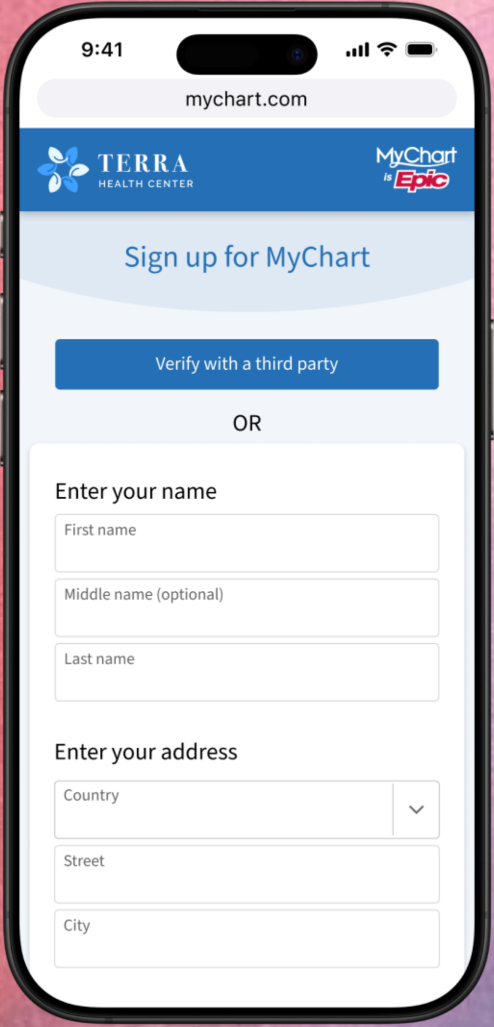
1. **User Registration**
2. Client Registration
3. Data Request
4. Authentication
5. Patient Matching
6. Consent & Authorization
7. Data Exchange

User Registration

with ID Verification

Step:

1. **User Registration**
2. Client Registration
3. Data Request
4. Authentication
5. Patient Matching
6. Consent & Authorization
7. Data Exchange



9:41

mychart.com

TERRA HEALTH CENTER

MyChart is Epic

Sign up for MyChart

Verify with a third party

OR

Enter your name

First name

Middle name (optional)

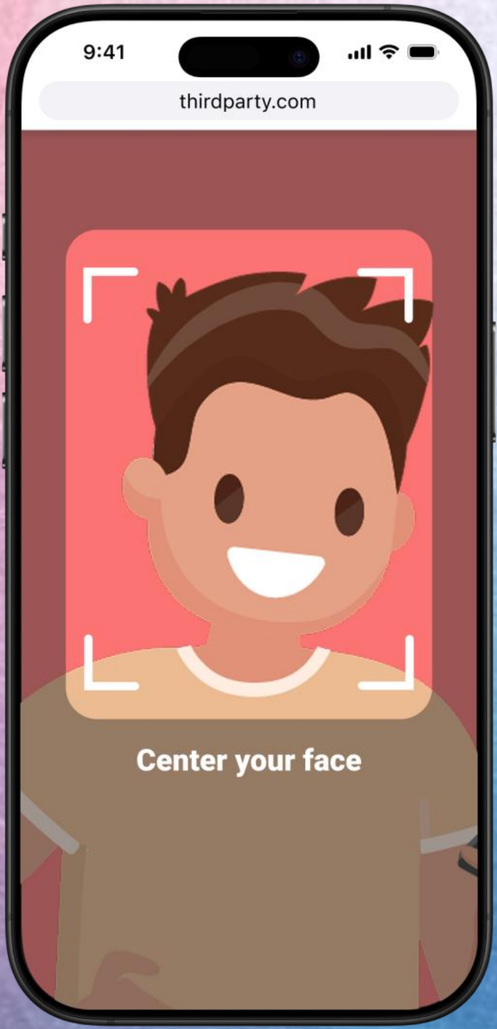
Last name

Enter your address

Country

Street

City



9:41

thirdparty.com

Center your face

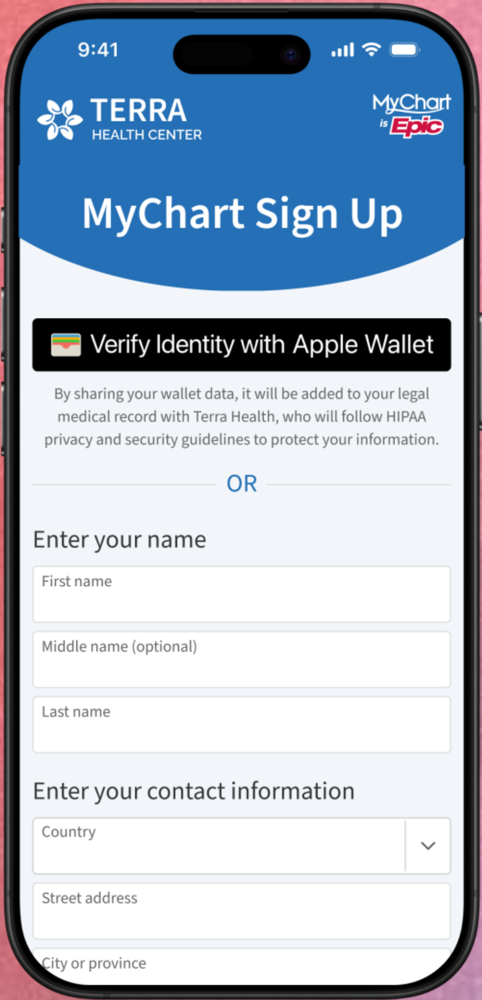
CURRENT

User Registration

with Mobile Driver's Licenses

Step:

1. **User Registration**
2. Client Registration
3. Data Request
4. Authentication
5. Patient Matching
6. Consent & Authorization
7. Data Exchange


9:41

TERRA HEALTH CENTER

MyChart is Epic

MyChart Sign Up

Verify Identity with Apple Wallet

By sharing your wallet data, it will be added to your legal medical record with Terra Health, who will follow HIPAA privacy and security guidelines to protect your information.

OR

Enter your name

First name

Middle name (optional)

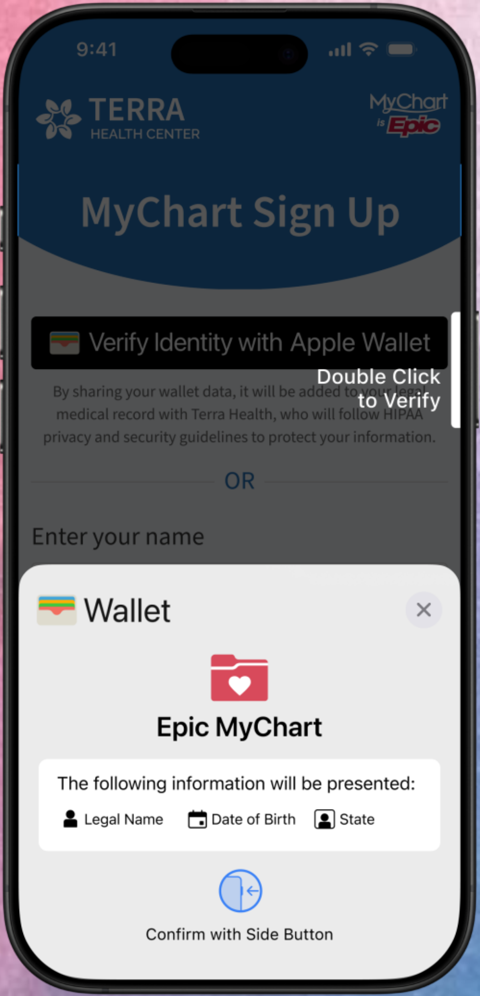
Last name

Enter your contact information

Country

Street address

City or province


9:41

TERRA HEALTH CENTER

MyChart is Epic

MyChart Sign Up

Verify Identity with Apple Wallet

Double Click to Verify

By sharing your wallet data, it will be added to your legal medical record with Terra Health, who will follow HIPAA privacy and security guidelines to protect your information.

OR

Enter your name

Wallet ✕

Epic MyChart

The following information will be presented:

Legal Name · Date of Birth · State

Confirm with Side Button

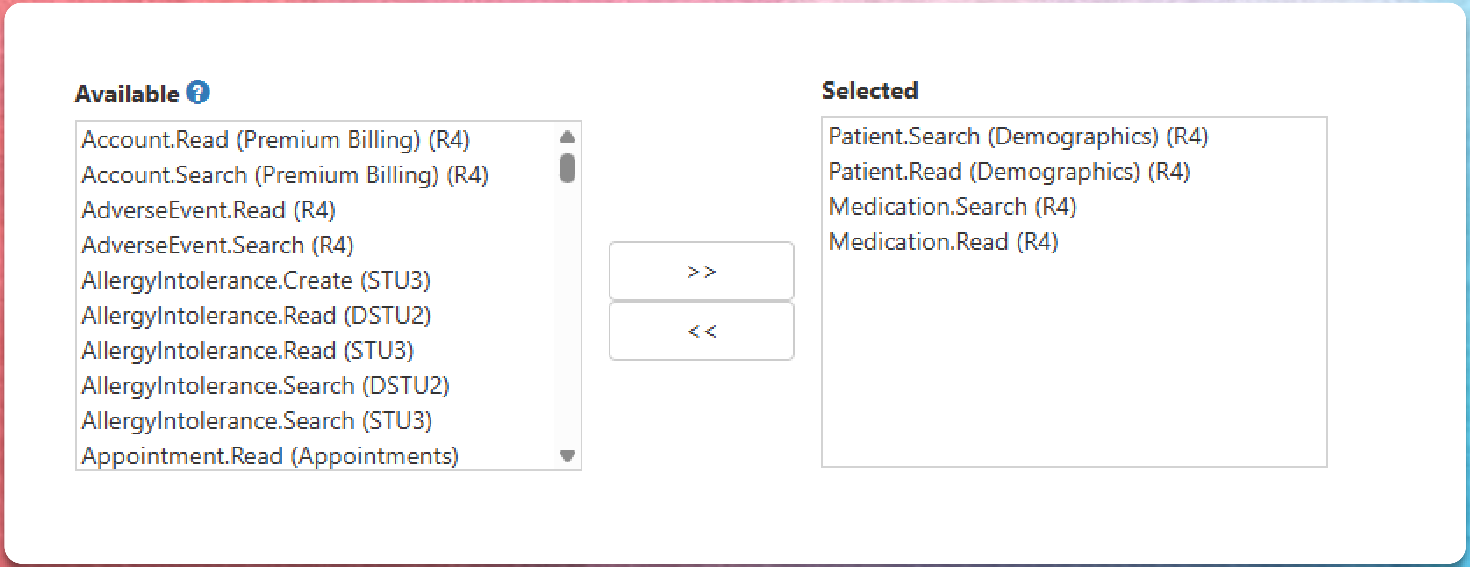
FUTURE

Client Registration

with **Open.Epic**

Step:

1. User Registration
2. **Client Registration**
3. Data Request
4. Authentication
5. Patient Matching
6. Consent & Authorization
7. Data Exchange



Available

- Account.Read (Premium Billing) (R4)
- Account.Search (Premium Billing) (R4)
- AdverseEvent.Read (R4)
- AdverseEvent.Search (R4)
- AllergyIntolerance.Create (STU3)
- AllergyIntolerance.Read (DSTU2)
- AllergyIntolerance.Read (STU3)
- AllergyIntolerance.Search (DSTU2)
- AllergyIntolerance.Search (STU3)
- Appointment.Read (Appointments)

Selected

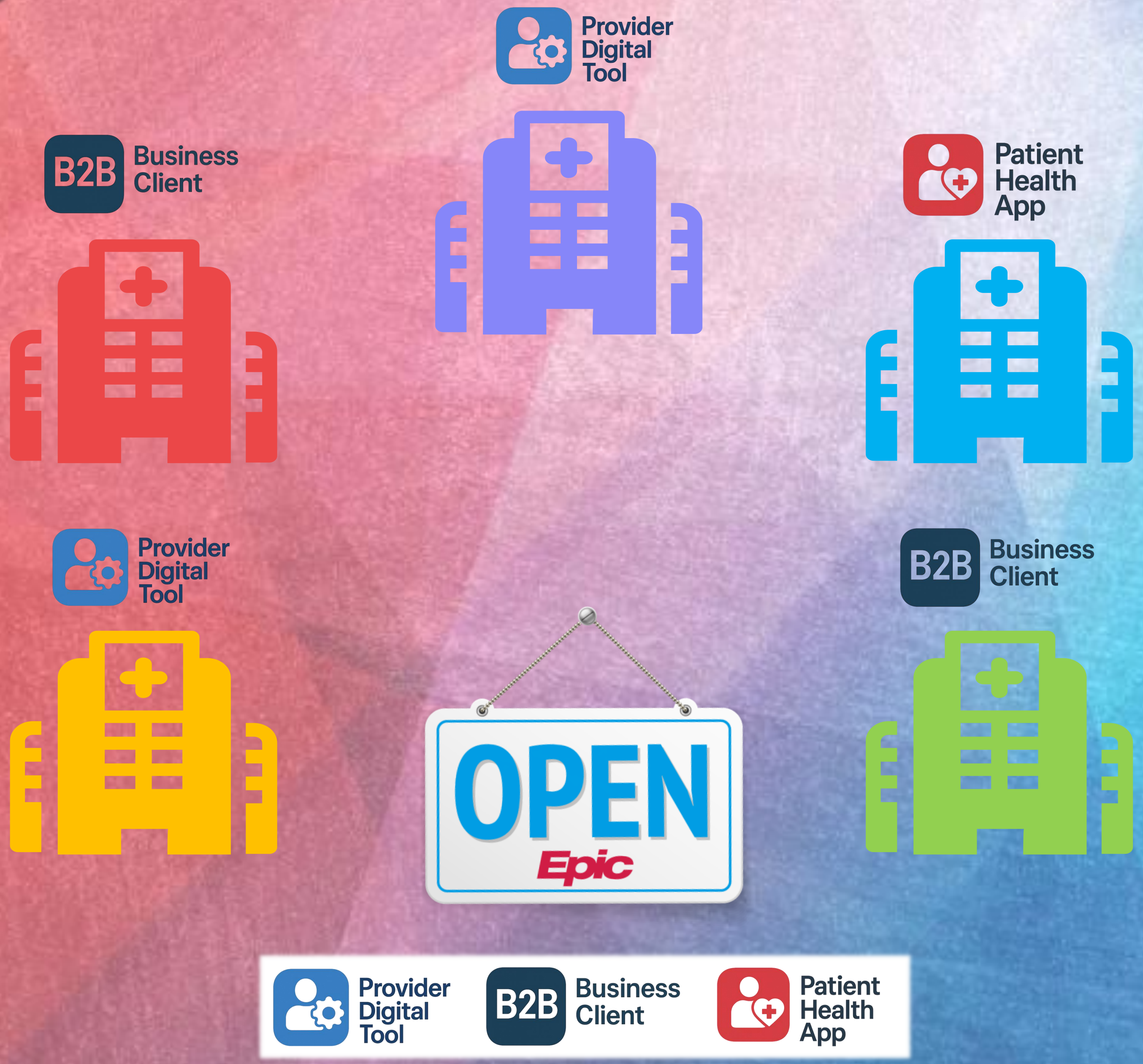
- Patient.Search (Demographics) (R4)
- Patient.Read (Demographics) (R4)
- Medication.Search (R4)
- Medication.Read (R4)

Client Registration

with **Open.Epic**

Step:

1. User Registration
2. **Client Registration**
3. Data Request
4. Authentication
5. Patient Matching
6. Consent & Authorization
7. Data Exchange



Provider Digital Tool

B2B Business Client

Patient Health App

Provider Digital Tool

B2B Business Client

Provider Digital Tool

B2B Business Client

Patient Health App

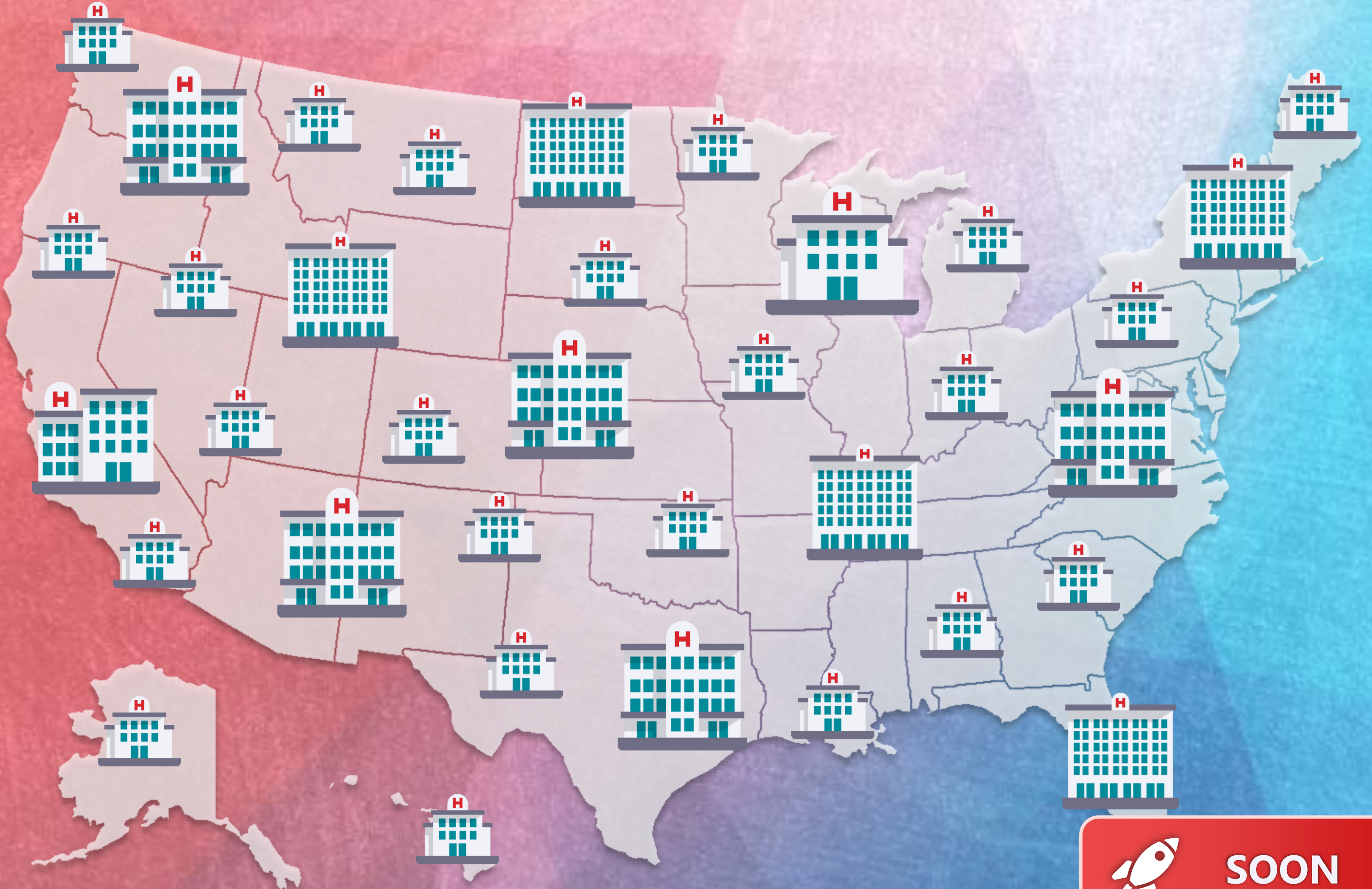
Dynamic Client Registration

with **TEFCA**

TEFCA℠

Step:

1. User Registration
2. **Client Registration**
3. Data Request
4. Authentication
5. Patient Matching
6. Consent & Authorization
7. Data Exchange



SOON

Client Onboarding

with **TEFCA**

Step:

1. User Registration
2. **Client Registration**
3. Data Request
4. Authentication
5. Patient Matching
6. Consent & Authorization
7. Data Exchange

Health Client
TEFCA SM

SOON

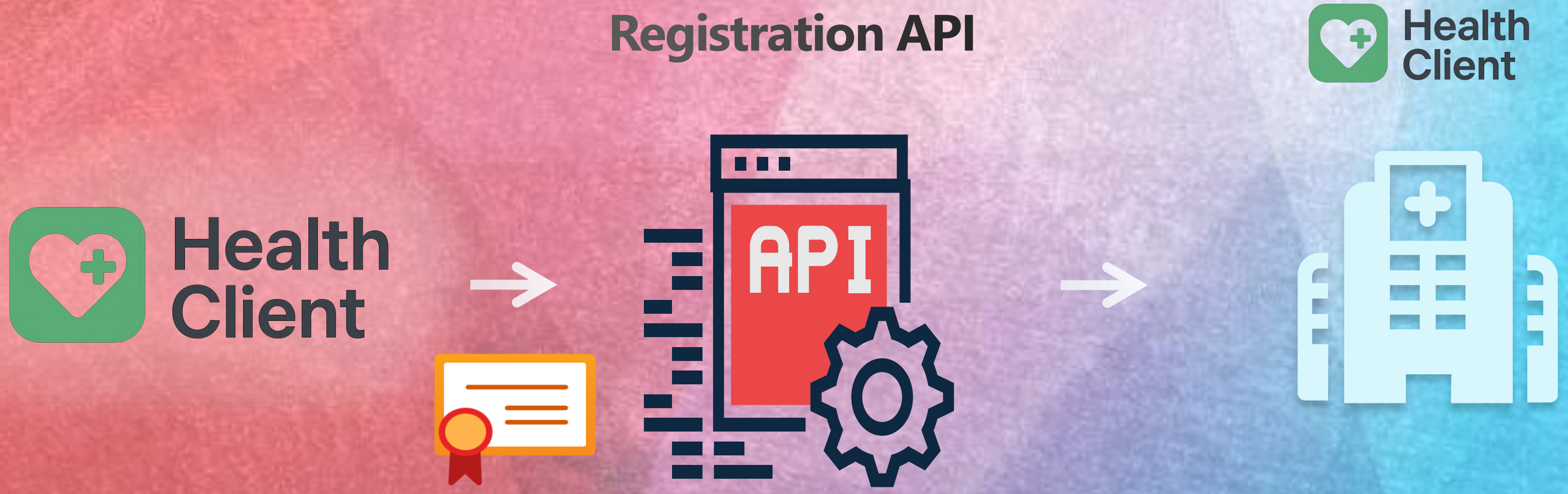
Dynamic Client Registration

with **TEFCA**

TEFCA℠

Step:

1. User Registration
2. **Client Registration**
3. Data Request
4. Authentication
5. Patient Matching
6. Consent & Authorization
7. Data Exchange



SOON

Client Registration

*Which **Path Do I Take?***

Step:

1. User Registration
2. **Client Registration**
3. Data Request
4. Authentication
5. Patient Matching
6. Consent & Authorization
7. Data Exchange

TEFCA℠

Scale

Features

Cost

Data Request

with **Auth Code Flow**

Step:

1. User Registration
2. Client Registration
3. **Data Request**
4. Authentication
5. Patient Matching
6. Consent & Authorization
7. Data Exchange

Patient Health App

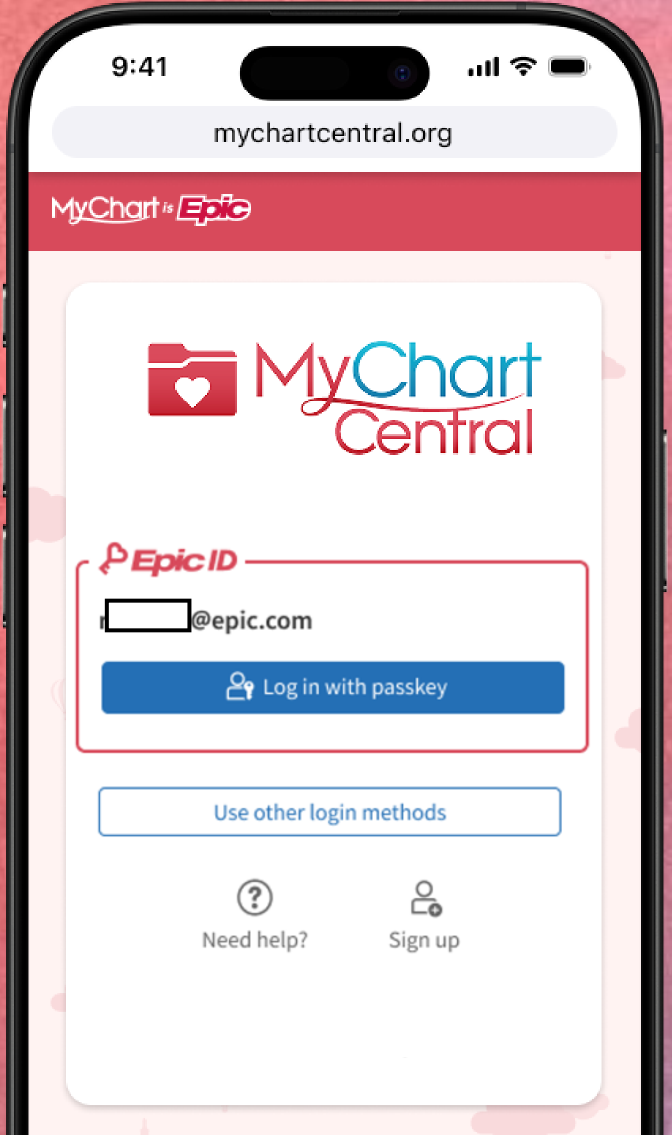
Provider Digital Tool

Authentication

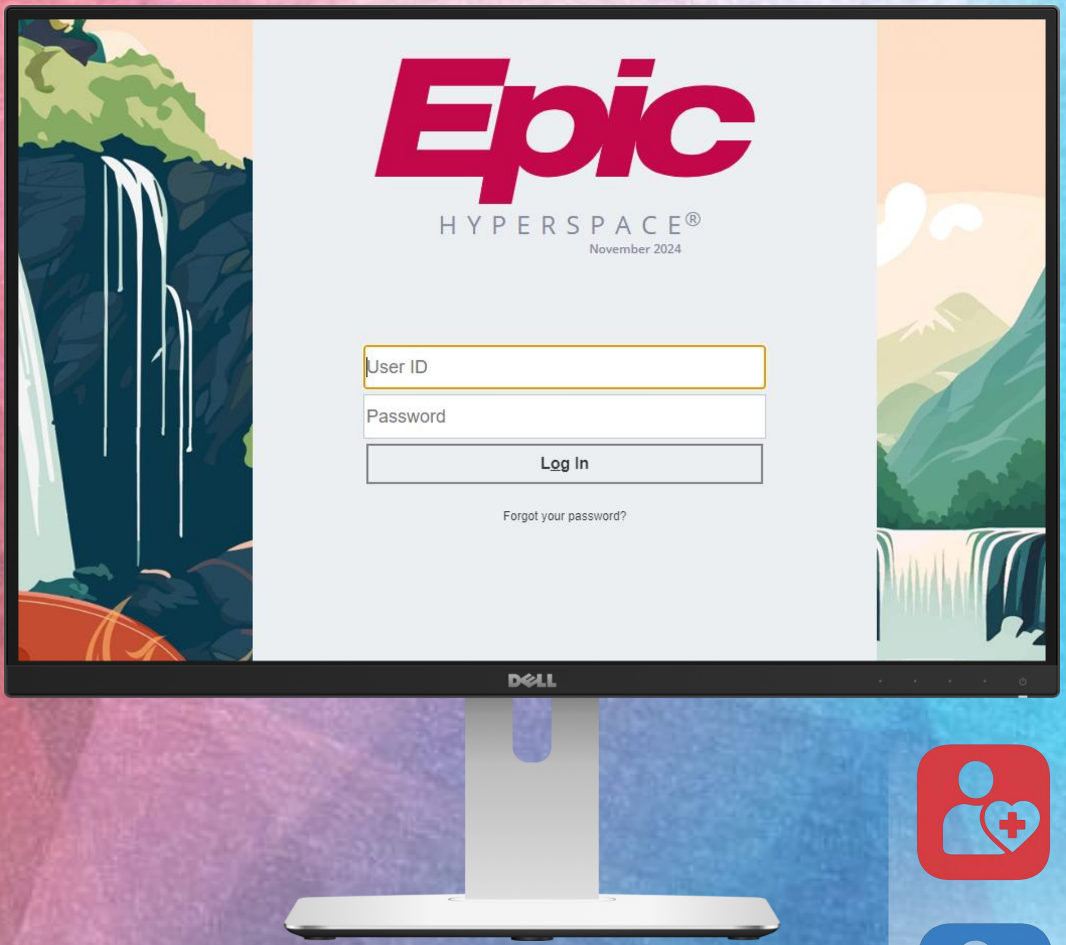
for End Users

Step:

1. User Registration
2. Client Registration
3. Data Request
4. **Authentication**
5. Patient Matching
6. Consent & Authorization
7. Data Exchange



[redacted]@epic.com



Patient Health App

Provider Digital Tool

Fewer Clicks

with SMART SSO

Step:

1. User Registration
2. Client Registration
3. Data Request
4. **Authentication**
5. Patient Matching
6. Consent & Authorization
7. Data Exchange

SMART®

Provider Digital Tool

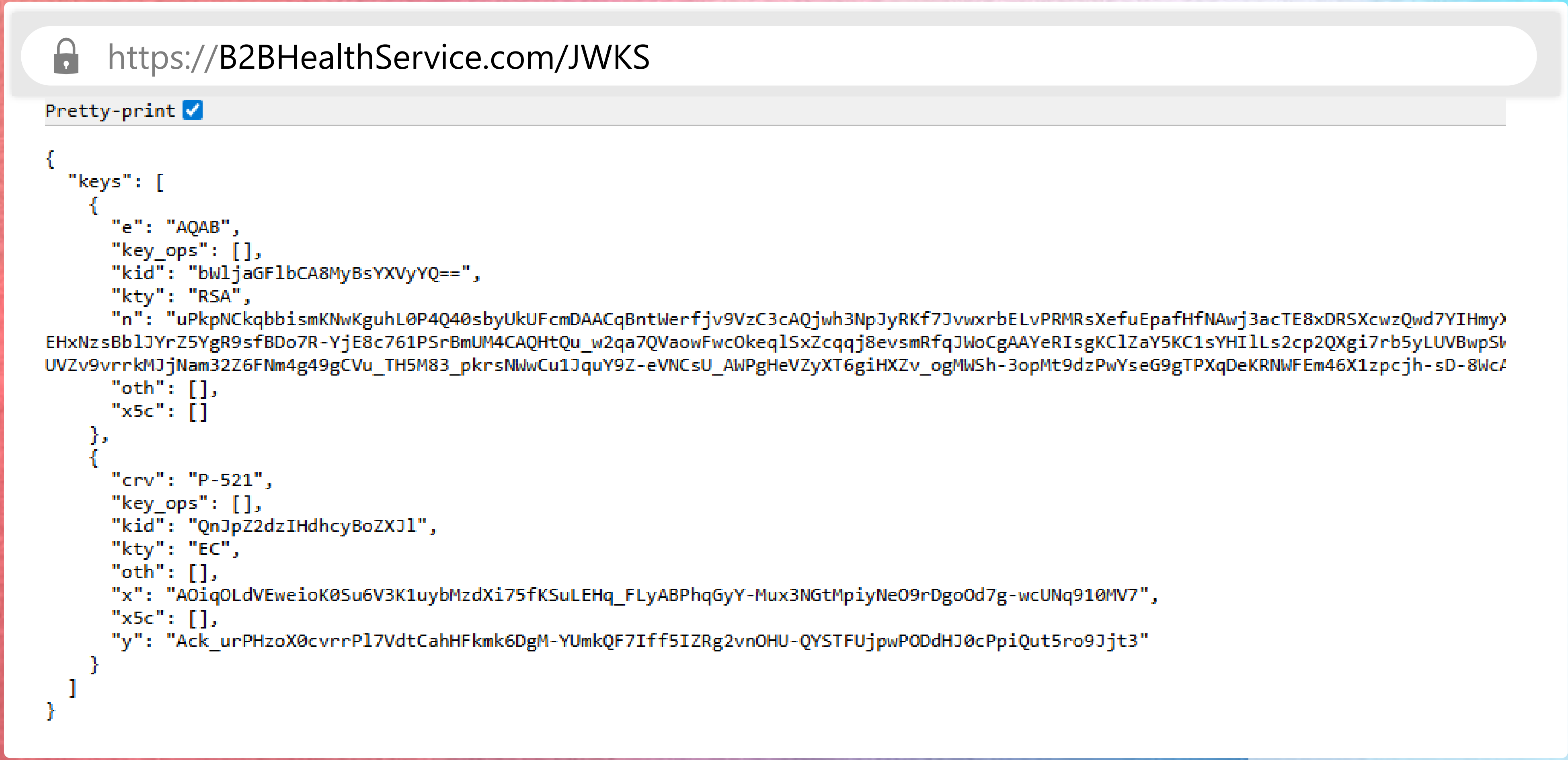
Patient Health App

Authentication

with Client Credentials

Step:

1. User Registration
2. Client Registration
3. Data Request
4. **Authentication**
5. Patient Matching
6. Consent & Authorization
7. Data Exchange



https://B2BHealthService.com/JWKS

Pretty-print ☑

```
{
  "keys": [
    {
      "e": "AQAB",
      "key_ops": [],
      "kid": "bWljaGFlbCA8MyBsYXVyYQ==",
      "kty": "RSA",
      "n": "uPkpNCkqbbismKNwKguhL0P4Q40sbyUkUFcmDAACqBntWerfjv9VzC3cAQjwh3NpJyRKf7JvwxrbELvPRMRsXefuEpafHfNAwj3acTE8xDRSXcwzQwd7YIHmy
EHxNzsBblJYrZ5YgR9sfBDo7R-YjE8c761PSrBmUM4CAQHtQu_w2qa7QVaowFwcOkeqlSxZcqqj8evsmRfqJWoCgAAYeRIsgKClZaY5KC1sYHIlLs2cp2QXgi7rb5yLUVBwpS
UVZv9vrrkMJjNam32Z6FNm4g49gCVu_TH5M83_pkrsNWwCu1JquY9Z-eVNCsU_AWPgHeVZyXT6giHXZv_ogMWSh-3opMt9dzPwYseG9gTPXqDeKRNWFEm46X1zpcjh-sD-8Wc
      "oth": [],
      "x5c": []
    },
    {
      "crv": "P-521",
      "key_ops": [],
      "kid": "QnJpZ2dzIHdhcyBoZXJl",
      "kty": "EC",
      "oth": [],
      "x": "AOiqOLdVEweioK0Su6V3K1uybMzdXi75fKSuLEHq_FLyABPhqGyY-Mux3NGtMpiyNeO9rDgoOd7g-wcUNq910MV7",
      "x5c": [],
      "y": "Ack_urPHzoX0cvrrPl7VdtCahHFkmk6DgM-YUmkQF7Iff5IZRg2vnOHU-QYSTFUjpwPODdHJ0cPpiQut5ro9Jjt3"
    }
  ]
}
```

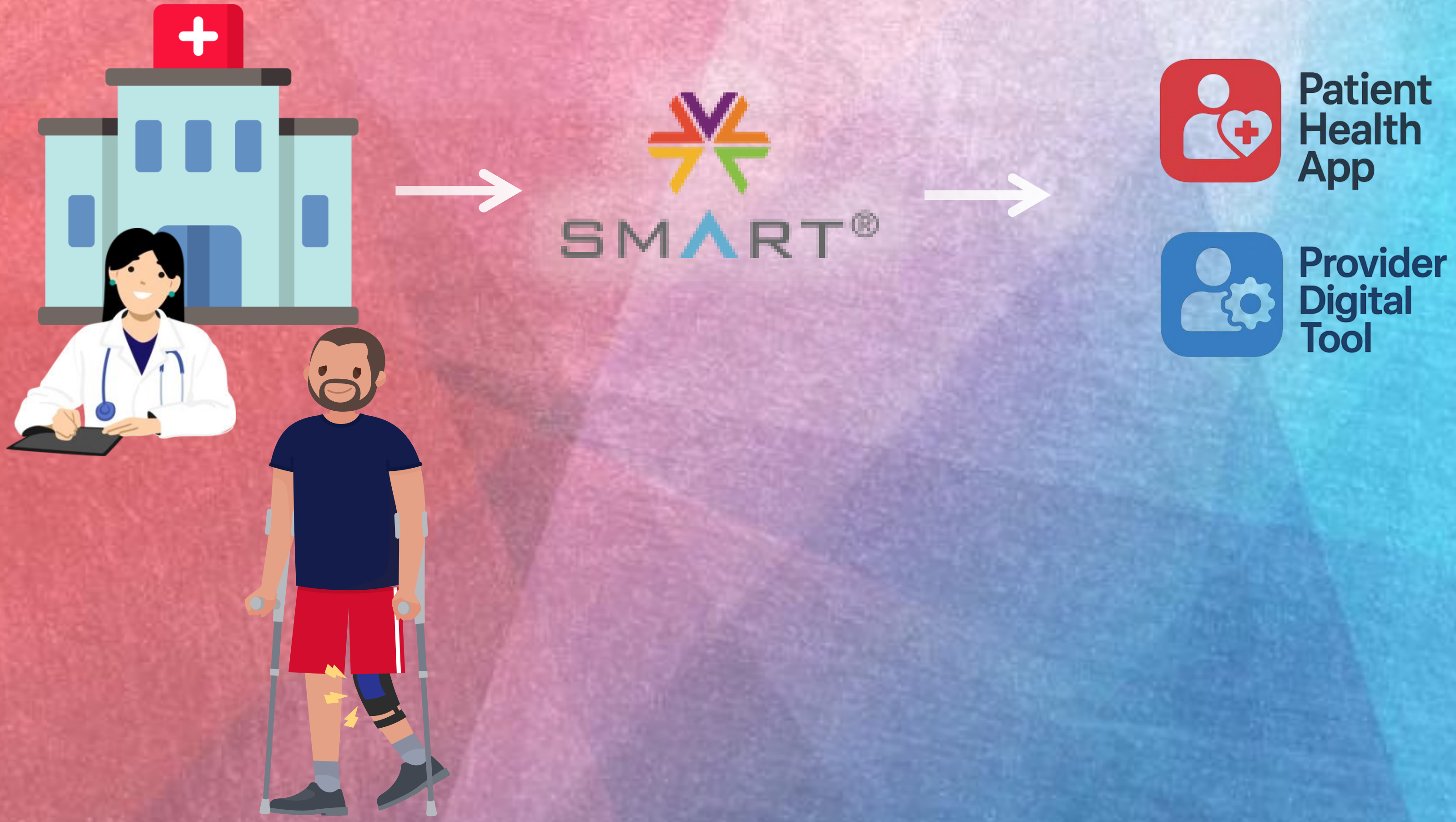
B2B Business Client

Patient Matching

with **SMART**

Step:

1. User Registration
2. Client Registration
3. Data Request
4. Authentication
5. **Patient Matching**
6. Consent & Authorization
7. Data Exchange



Patient Health App

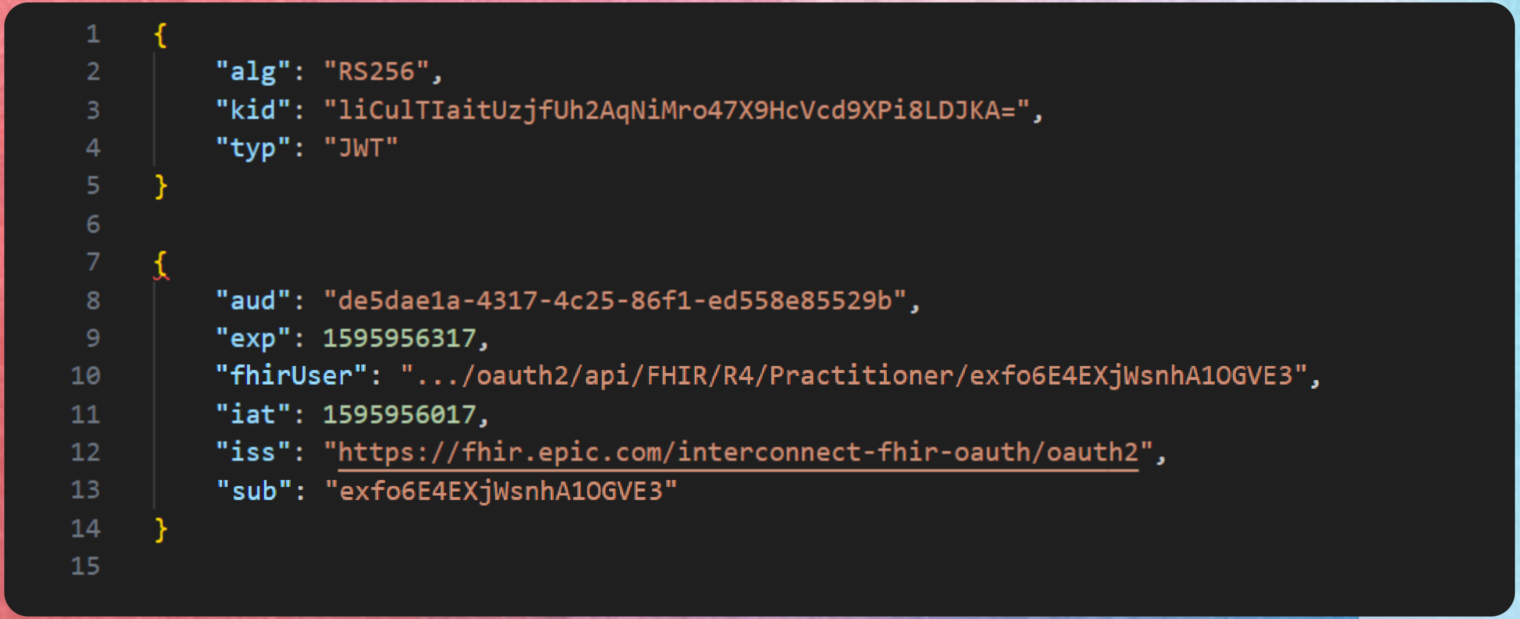
Provider Digital Tool

User Matching

with OIDC

Step:

1. User Registration
2. Client Registration
3. Data Request
4. Authentication
5. **Patient Matching**
6. Consent & Authorization
7. Data Exchange



```
{
    "alg": "RS256",
    "kid": "liCulTIaitUzjfUh2AqNiMro47X9HcVcd9XPi8LDJKA=",
    "typ": "JWT"
}

{
    "aud": "de5dae1a-4317-4c25-86f1-ed558e85529b",
    "exp": 1595956317,
    "fhirUser": ".../oauth2/api/FHIR/R4/Practitioner/exfo6E4EXjWsnhA1OGVE3",
    "iat": 1595956017,
    "iss": "https://fhir.epic.com/interconnect-fhir-oauth/oauth2",
    "sub": "exfo6E4EXjWsnhA1OGVE3"
}
```

Patient Health App

Provider Digital Tool

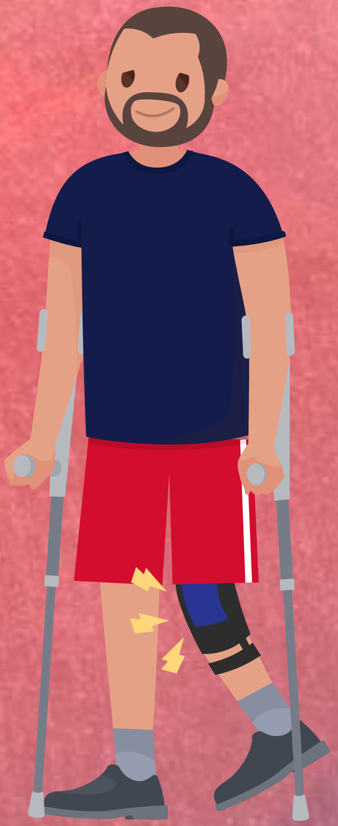
User Matching

with **FHIR**

Step:

1. User Registration
2. Client Registration
3. Data Request
4. Authentication
5. **Patient Matching**
6. Consent & Authorization
7. Data Exchange

Patient



Practitioner

RelatedPerson

Patient Health App

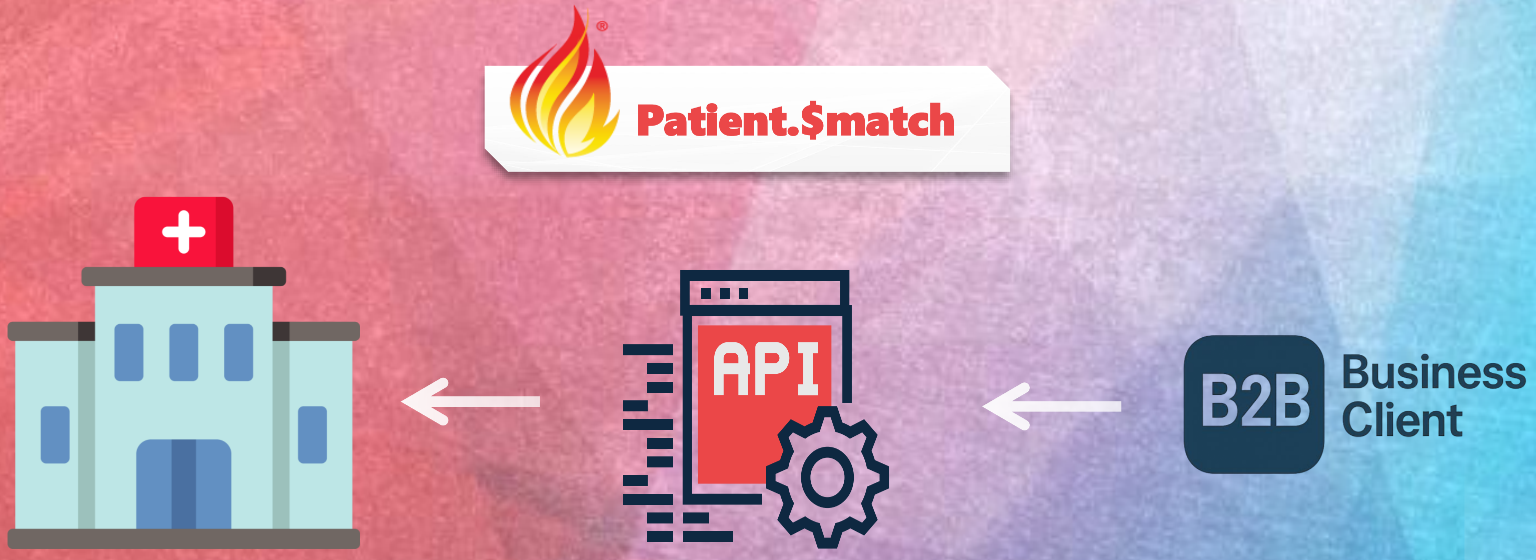
Provider Digital Tool

Patient Matching

with **FHIR $match**

Step:

1. User Registration
2. Client Registration
3. Data Request
4. Authentication
5. **Patient Matching**
6. Consent & Authorization
7. Data Exchange



Which patient matches these demographics?

Consent & Authorization

for **Patients**

Step:

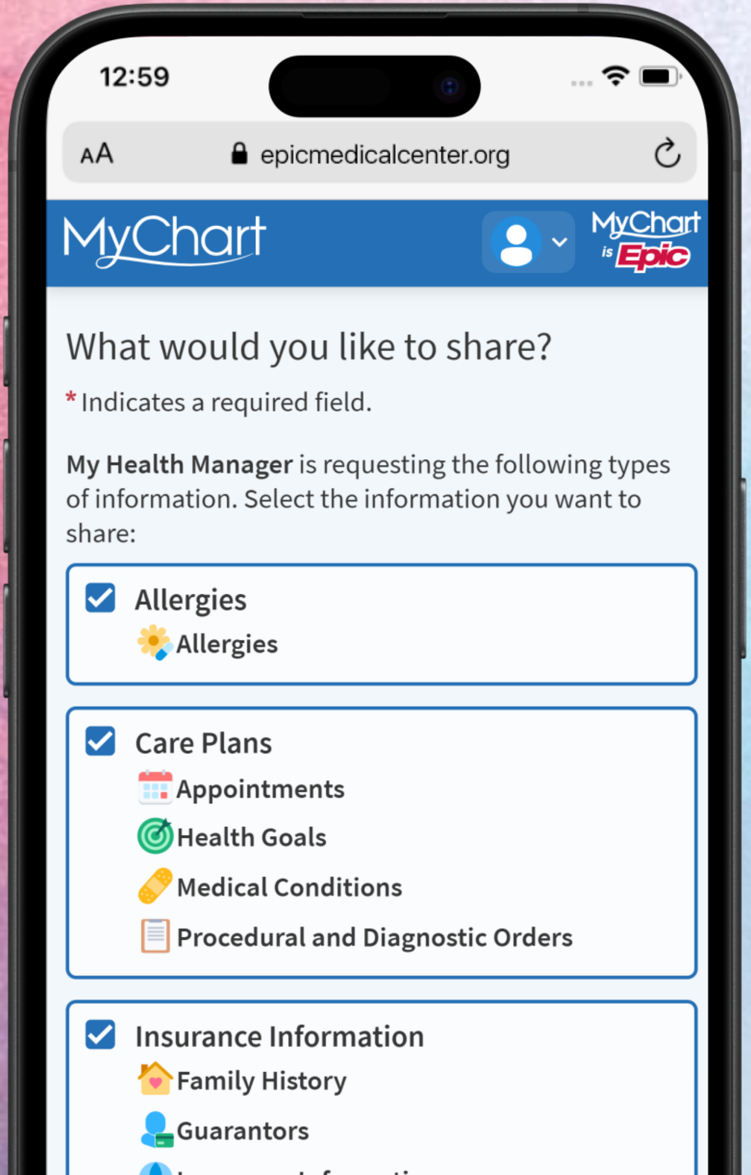
1. User Registration
2. Client Registration
3. Data Request
4. Authentication
5. Patient & User Matching
6. **Consent & Authorization**
7. Data Exchange

What is being asked?

SMART scopes made patient friendly

What is it used for?

How the application is using the data



What would you like to share?

*Indicates a required field.

My Health Manager is requesting the following types of information. Select the information you want to share:

☑ Allergies
- Allergies

☑ Care Plans
- Appointments
- Health Goals
- Medical Conditions
- Procedural and Diagnostic Orders

☑ Insurance Information
- Family History
- Guarantors

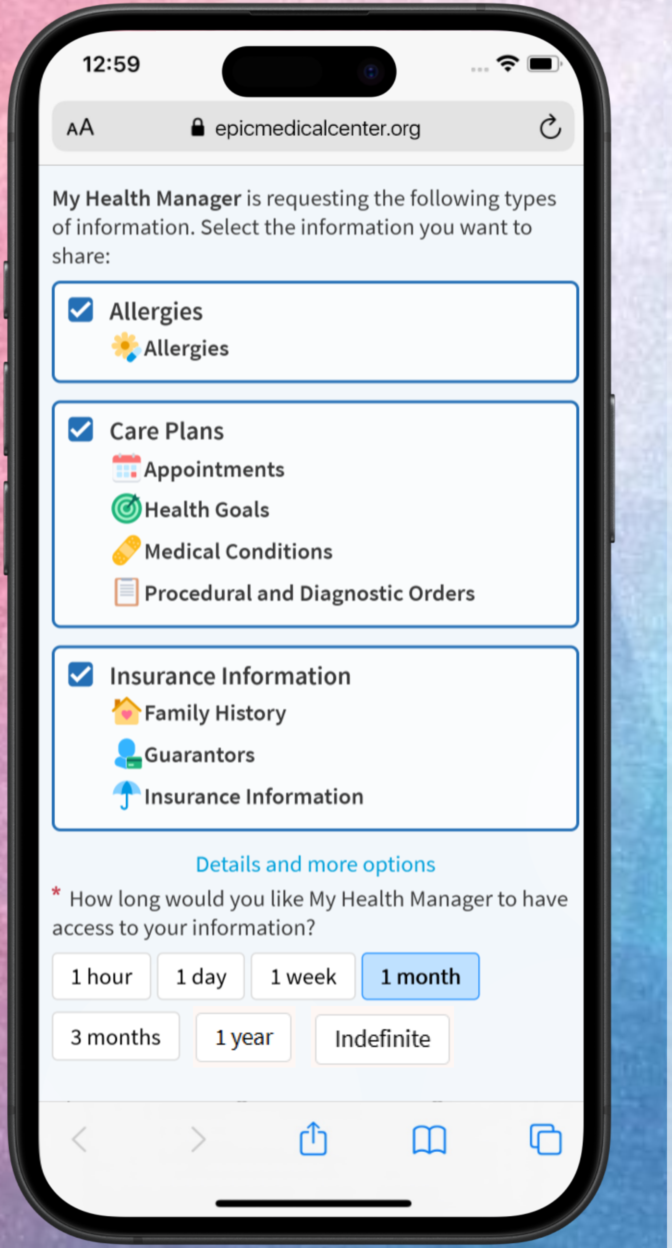
Patient Health App

Streamlined Access

with **Auth Code Flow**

Step:

1. User Registration
2. Client Registration
3. Data Request
4. Authentication
5. Patient & User Matching
6. **Consent & Authorization**
7. Data Exchange


12:59

AA epicmedicalcenter.org

My Health Manager is requesting the following types of information. Select the information you want to share:

☑ Allergies
- Allergies

☑ Care Plans
- Appointments
- Health Goals
- Medical Conditions
- Procedural and Diagnostic Orders

☑ Insurance Information
- Family History
- Guarantors
- Insurance Information

Details and more options

* How long would you like My Health Manager to have access to your information?

1 hour | 1 day | 1 week | [✓ 1 month]

3 months | 1 year | Indefinite

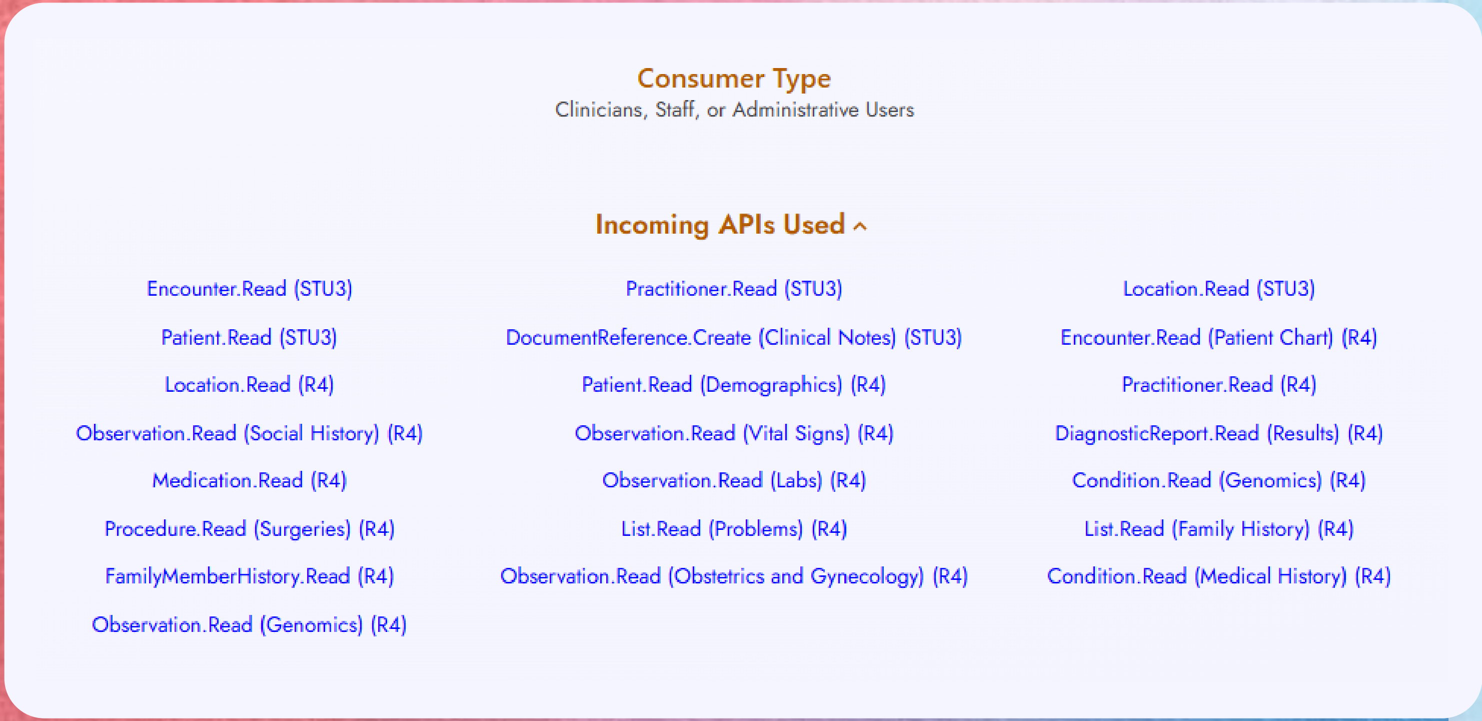
Patient Health App

Consent & Authorization

for Provider Organizations

Step:

1. User Registration
2. Client Registration
3. Data Request
4. Authentication
5. Patient Matching
6. **Consent & Authorization**
7. Data Exchange



Consumer Type

Clinicians, Staff, or Administrative Users

Incoming APIs Used ^

Encounter.Read (STU3)

Patient.Read (STU3)

Location.Read (R4)

Observation.Read (Social History) (R4)

Medication.Read (R4)

Procedure.Read (Surgeries) (R4)

FamilyMemberHistory.Read (R4)

Observation.Read (Genomics) (R4)

Practitioner.Read (STU3)

DocumentReference.Create (Clinical Notes) (STU3)

Patient.Read (Demographics) (R4)

Observation.Read (Vital Signs) (R4)

Observation.Read (Labs) (R4)

List.Read (Problems) (R4)

Observation.Read (Obstetrics and Gynecology) (R4)

Location.Read (STU3)

Encounter.Read (Patient Chart) (R4)

Practitioner.Read (R4)

DiagnosticReport.Read (Results) (R4)

Condition.Read (Genomics) (R4)

List.Read (Family History) (R4)

Condition.Read (Medical History) (R4)

Provider Digital Tool

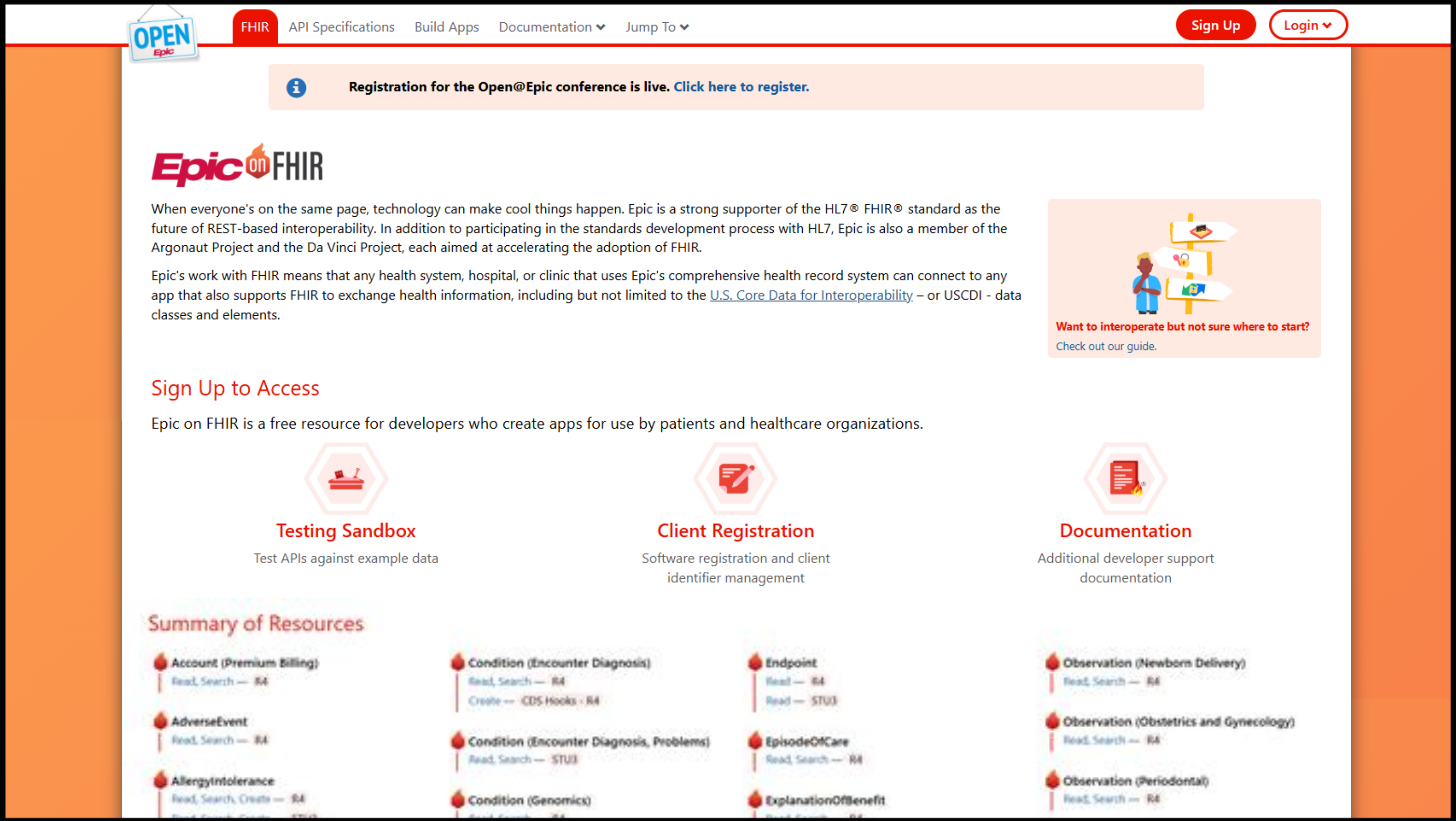
B2B Business Client

Data Exchange

with **FHIR APIs**

Step:

1. User Registration
2. Client Registration
3. Data Request
4. Authentication
5. Patient & User Matching
6. Consent & Authorization
7. **Data Exchange**



Registration for the Open@Epic conference is live. **Click here to register.**

Epic on FHIR

When everyone's on the same page, technology can make cool things happen. Epic is a strong supporter of the HL7® FHIR® standard as the future of REST-based interoperability. In addition to participating in the standards development process with HL7, Epic is also a member of the Argonaut Project and the Da Vinci Project, each aimed at accelerating the adoption of FHIR.

Epic's work with FHIR means that any health system, hospital, or clinic that uses Epic's comprehensive health record system can connect to any app that also supports FHIR to exchange health information, including but not limited to the U.S. Core Data for Interoperability – or USCDI - data classes and elements.

Want to interoperate but not sure where to start?
Check out our guide.

Sign Up to Access

Epic on FHIR is a free resource for developers who create apps for use by patients and healthcare organizations.

Testing Sandbox
Test APIs against example data

Client Registration
Software registration and client identifier management

Documentation
Additional developer support documentation

Summary of Resources

Account (Premium Billing)
Read, Search — R4

AdverseEvent
Read, Search — R4

AllergyIntolerance
Read, Search, Create — R4

Condition (Encounter Diagnosis)
Read, Search — R4
Create — CDS Hooks - R4

Condition (Encounter Diagnosis, Problems)
Read, Search — STU3

Condition (Genomics)

Endpoint
Read — R4
Read — STU3

EpisodeOfCare
Read, Search — R4

ExplanationOfBenefit

Observation (Newborn Delivery)
Read, Search — R4

Observation (Obstetrics and Gynecology)
Read, Search — R4

Observation (Periodontal)
Read, Search — R4

Context Syncing
with **FHIR**

Step:

1. User Registration
2. Client Registration
3. Data Request
4. Authentication
5. Patient & User Matching
6. Consent & Authorization
7. **Data Exchange**

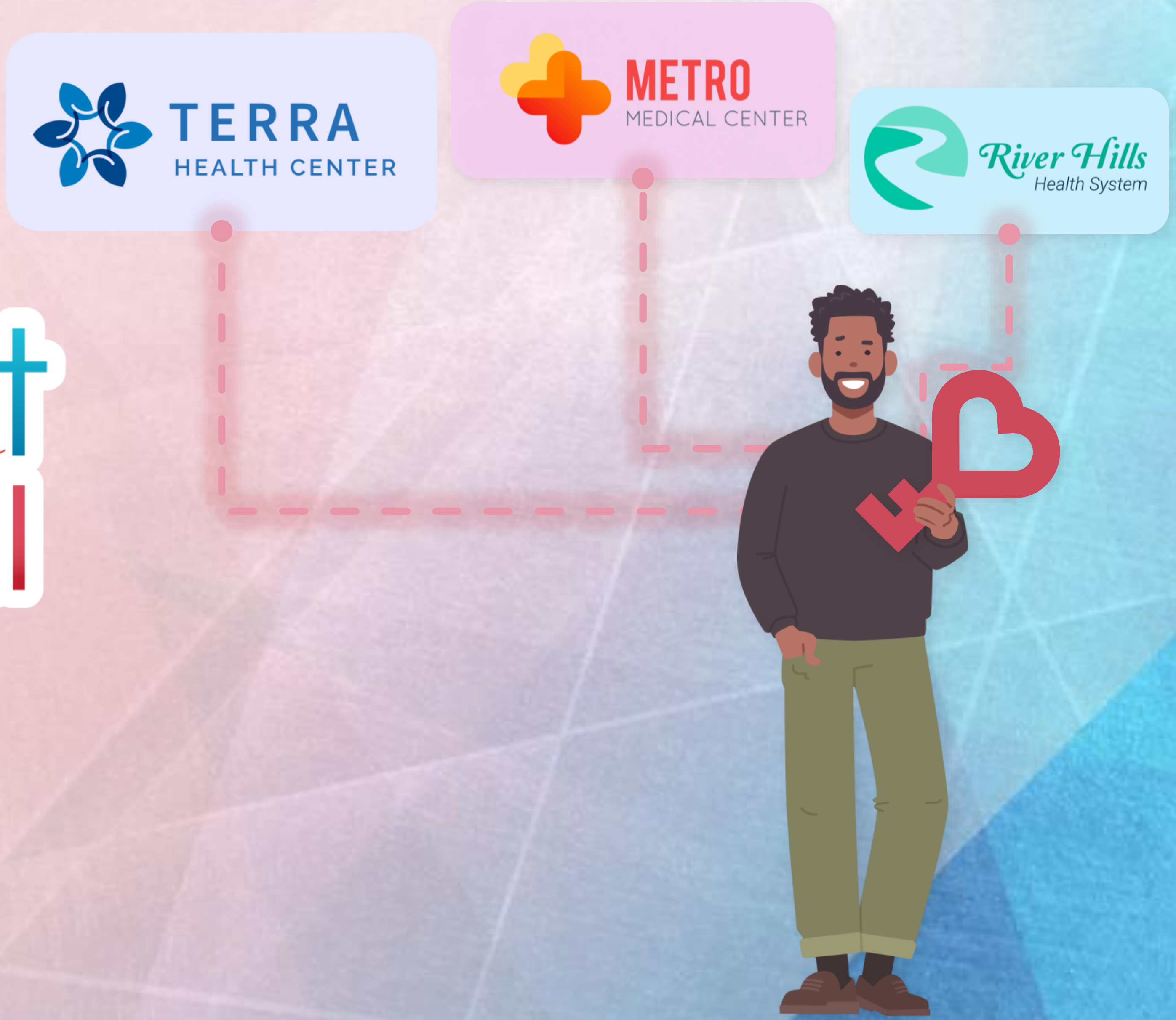
SMART®

FHIRcast

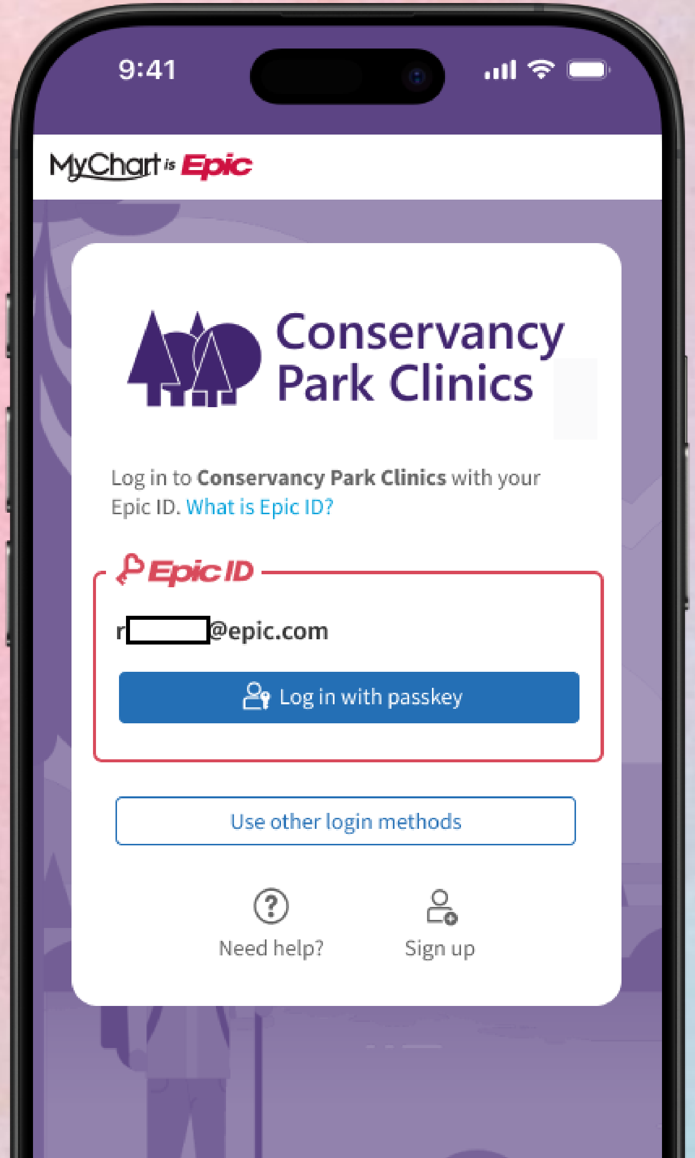
CDS HOOKS™

Patient-Facing Authorization with MyChart Central

MyChart Central



One Tap with Your Epic ID


9:41

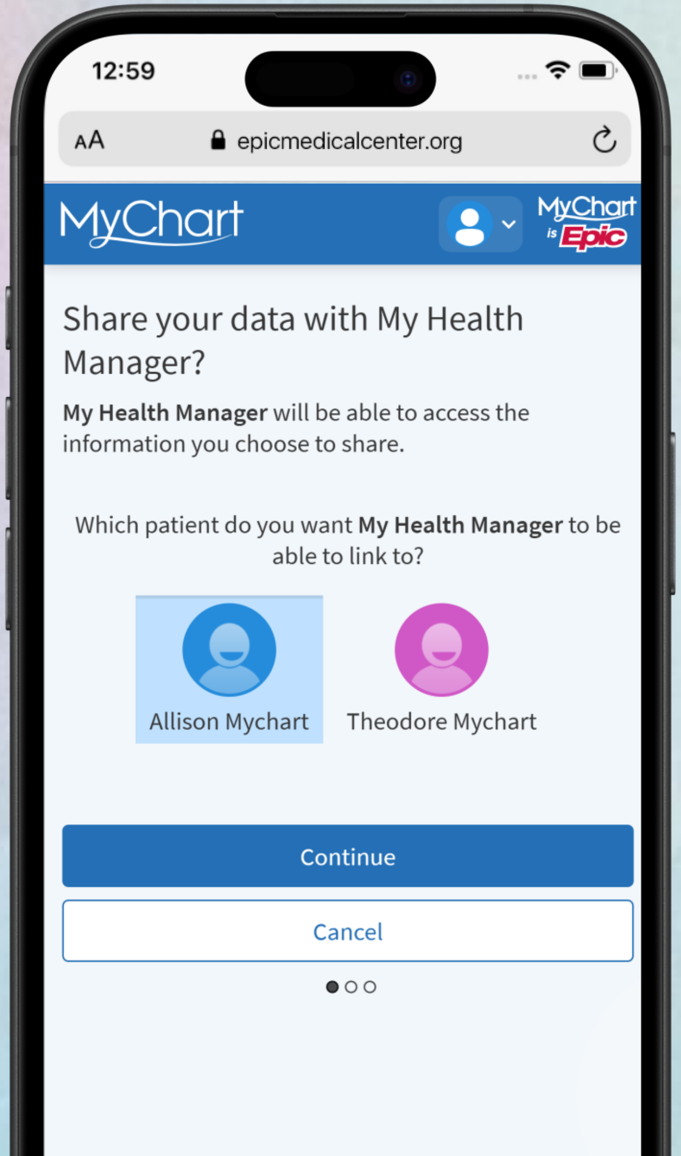
MyChart is Epic

Conservancy Park Clinics

Log in to **Conservancy Park Clinics** with your Epic ID. What is Epic ID?

Epic ID

r[redacted]@epic.com


12:59

AA epicmedicalcenter.org

MyChart

MyChart is Epic

Share your data with My Health Manager?

My Health Manager will be able to access the information you choose to share.

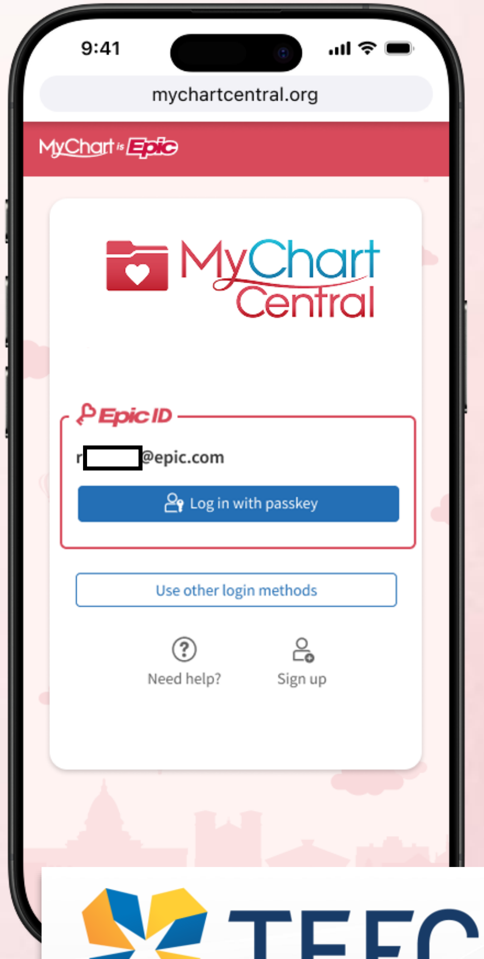
Which patient do you want **My Health Manager** to be able to link to?

Allison Mychart

Theodore Mychart

NOV 2025

Streamlined Authorization with Epic ID



9:41

mychartcentral.org

MyChart by Epic

MyChart Central

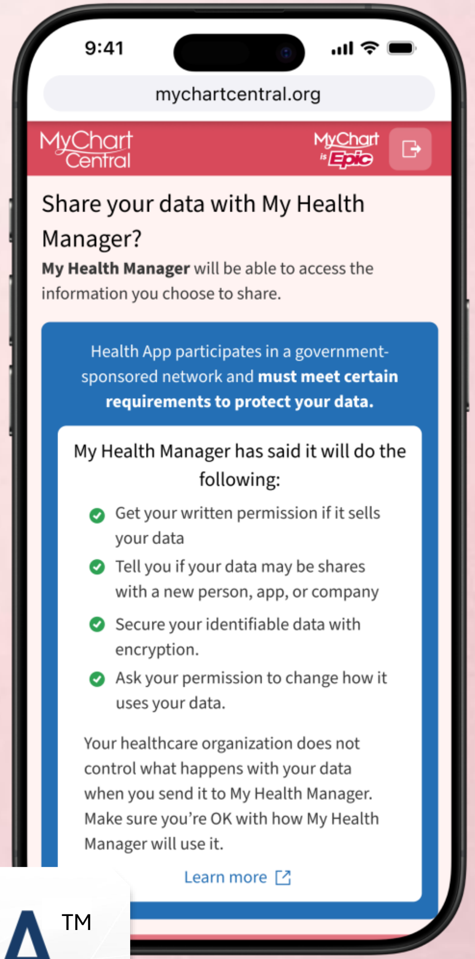
Epic ID

r[redacted]@epic.com

Log in with passkey

Use other login methods

Need help? Sign up



9:41

mychartcentral.org

MyChart Central MyChart by Epic

Share your data with My Health Manager?

My Health Manager will be able to access the information you choose to share.

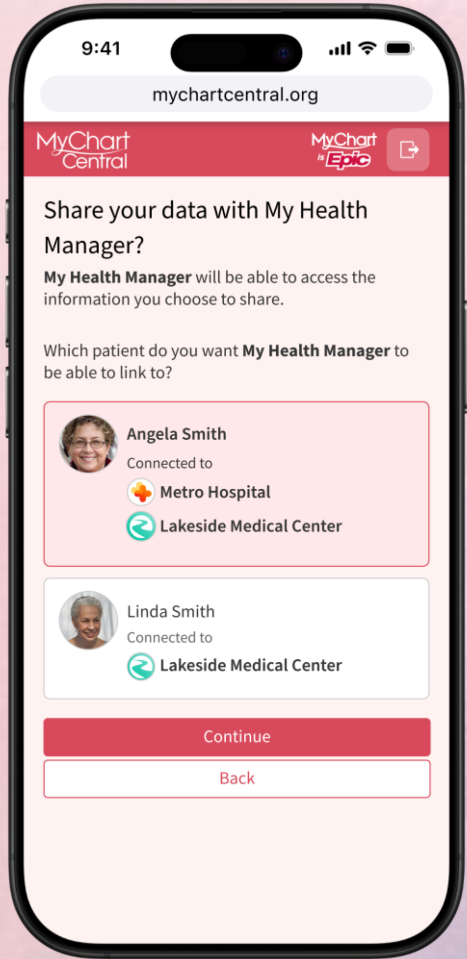
Health App participates in a government-sponsored network and **must meet certain requirements to protect your data.**

My Health Manager has said it will do the following:

- ✓ Get your written permission if it sells your data
- ✓ Tell you if your data may be shares with a new person, app, or company
- ✓ Secure your identifiable data with encryption.
- ✓ Ask your permission to change how it uses your data.

Your healthcare organization does not control what happens with your data when you send it to My Health Manager. Make sure you're OK with how My Health Manager will use it.

Learn more



9:41

mychartcentral.org

MyChart Central MyChart by Epic

Share your data with My Health Manager?

My Health Manager will be able to access the information you choose to share.

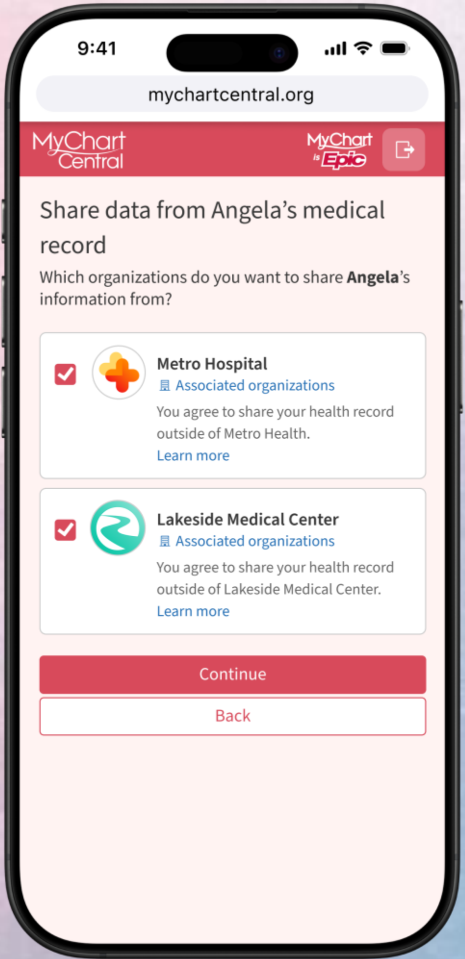
Which patient do you want **My Health Manager** to be able to link to?

Angela Smith
Connected to
Metro Hospital
Lakeside Medical Center

Linda Smith
Connected to
Lakeside Medical Center

Continue

Back



9:41

mychartcentral.org

MyChart Central MyChart by Epic

Share data from Angela's medical record

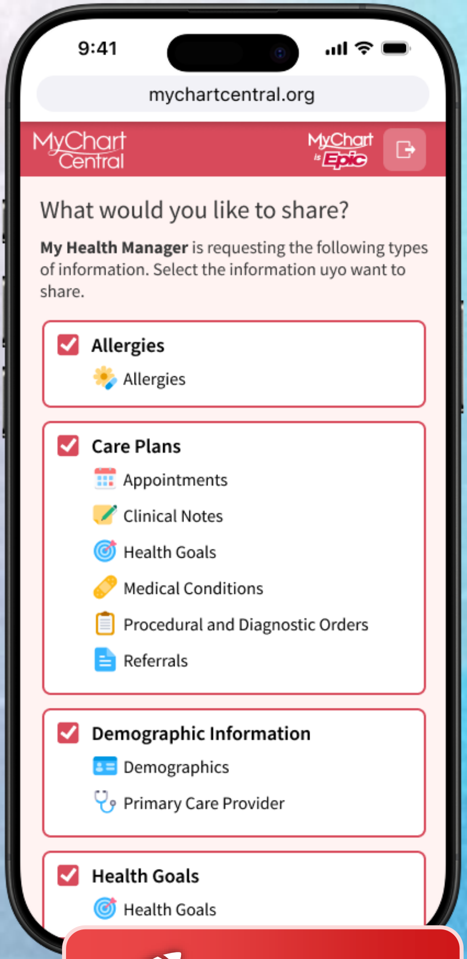
Which organizations do you want to share **Angela**'s information from?

☑ Metro Hospital
Associated organizations
You agree to share your health record outside of Metro Health.
Learn more

☑ Lakeside Medical Center
Associated organizations
You agree to share your health record outside of Lakeside Medical Center.
Learn more

Continue

Back



9:41

mychartcentral.org

MyChart Central MyChart by Epic

What would you like to share?

My Health Manager is requesting the following types of information. Select the information uyo want to share.

☑ **Allergies**
- Allergies

☑ **Care Plans**
- Appointments
- Clinical Notes
- Health Goals
- Medical Conditions
- Procedural and Diagnostic Orders
- Referrals

☑ **Demographic Information**
- Demographics
- Primary Care Provider

☑ **Health Goals**
- Health Goals

TEFCA™

2026