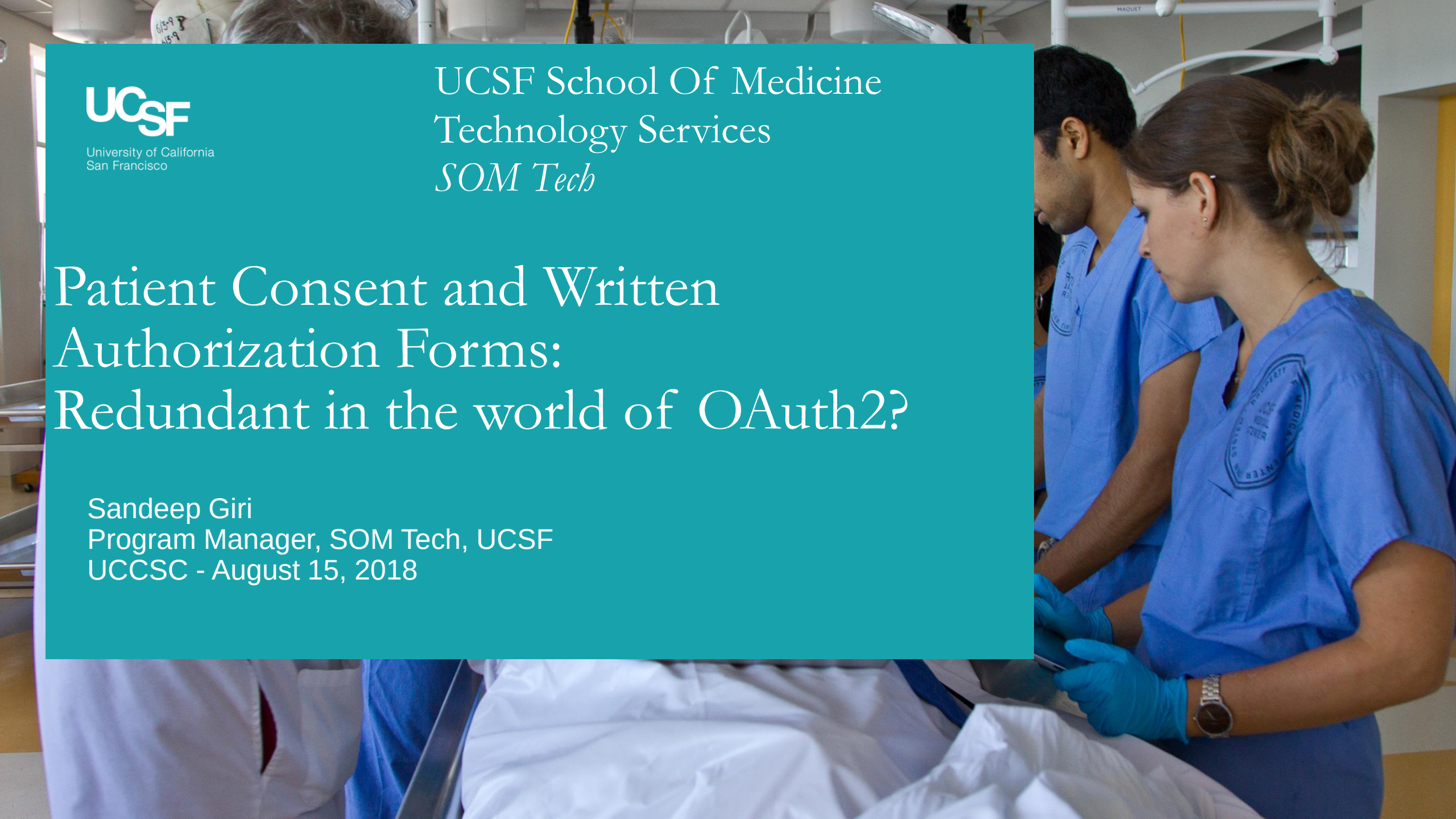


UCSF
University of California
San Francisco

UCSF School Of Medicine
Technology Services
SOM Tech

Patient Consent and Written Authorization Forms: Redundant in the world of OAuth2?

Sandeep Giri
Program Manager, SOM Tech, UCSF
UCCSC - August 15, 2018

Who is SOM Tech?

We are technology advocates.
Our broad technology expertise, deep knowledge of the UCSF ecosystem, and human-centered approach help you take innovative digital projects further, faster.

Agenda

- Use case for downloading / sharing PHI
- Requirement for capturing Patient Consent
- Current approach
- Alternate approach using Oauth
- Questions/Comments

- Paul: VA beneficiary living in Alaska.
- Not a lot of specialists at his local VA facility for him to see
- Frequently gets referred to local civilian specialists outside of VA

- Would like PHI generated by specialist shared with his VA providers
- Need to transfer information from specialist system to VA system

What records do you want? (Check appropriate boxes below):

Date(s) of Service: ____/____/____ through ____/____/____

☐ Discharge Summary ☐ Emergency Room Records ☐ Operative/Procedure Reports ☐ Billing Records

☐ Test Results (X-Rays, Lab/Pathology Results) Please specify: _____

☐ Other (Immunization Records, Medication Lists) Please specify: _____

How would you like your records delivered?

☐ Paper

☐ Home Delivery

☐ In-Person Pickup

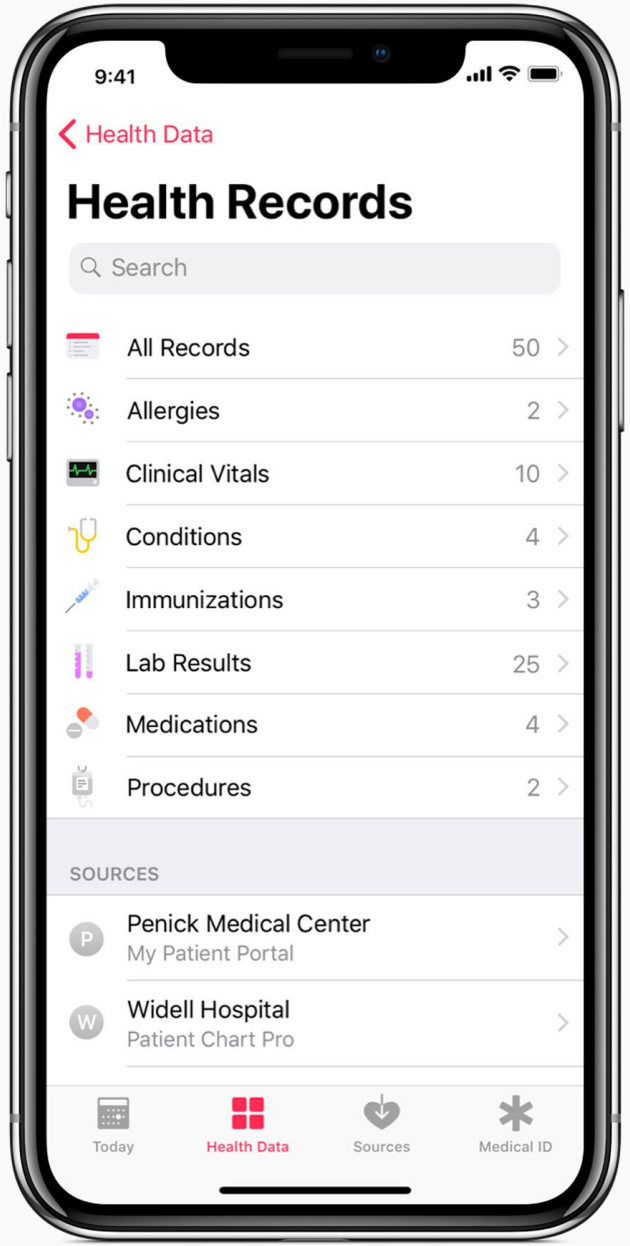
☐ Electronic (Email, USB, CD, Portal, Other) Please specify: _____

Where do you want the information sent? (Fill in boxes below):

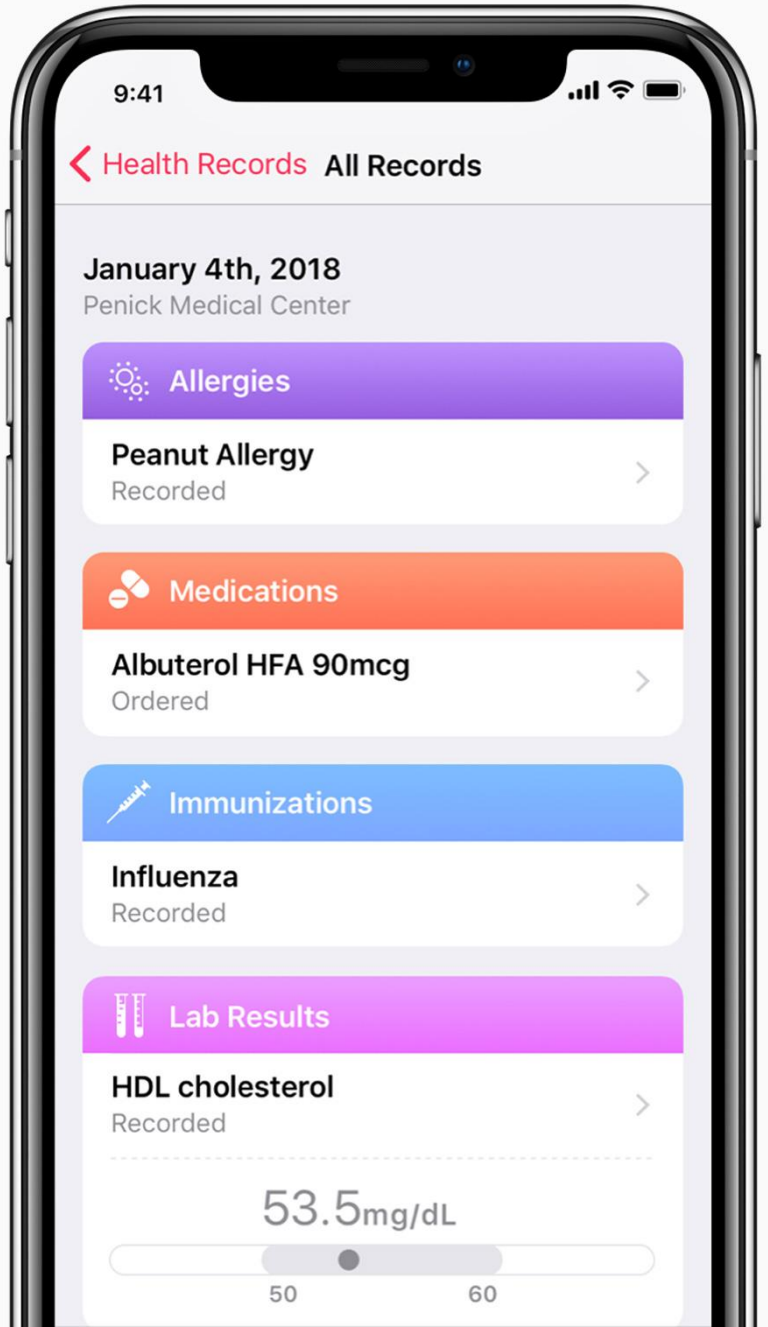
ORGANIZATION NAME should provide my records to: ☐ Self ☐ Personal Representative (indicated below)

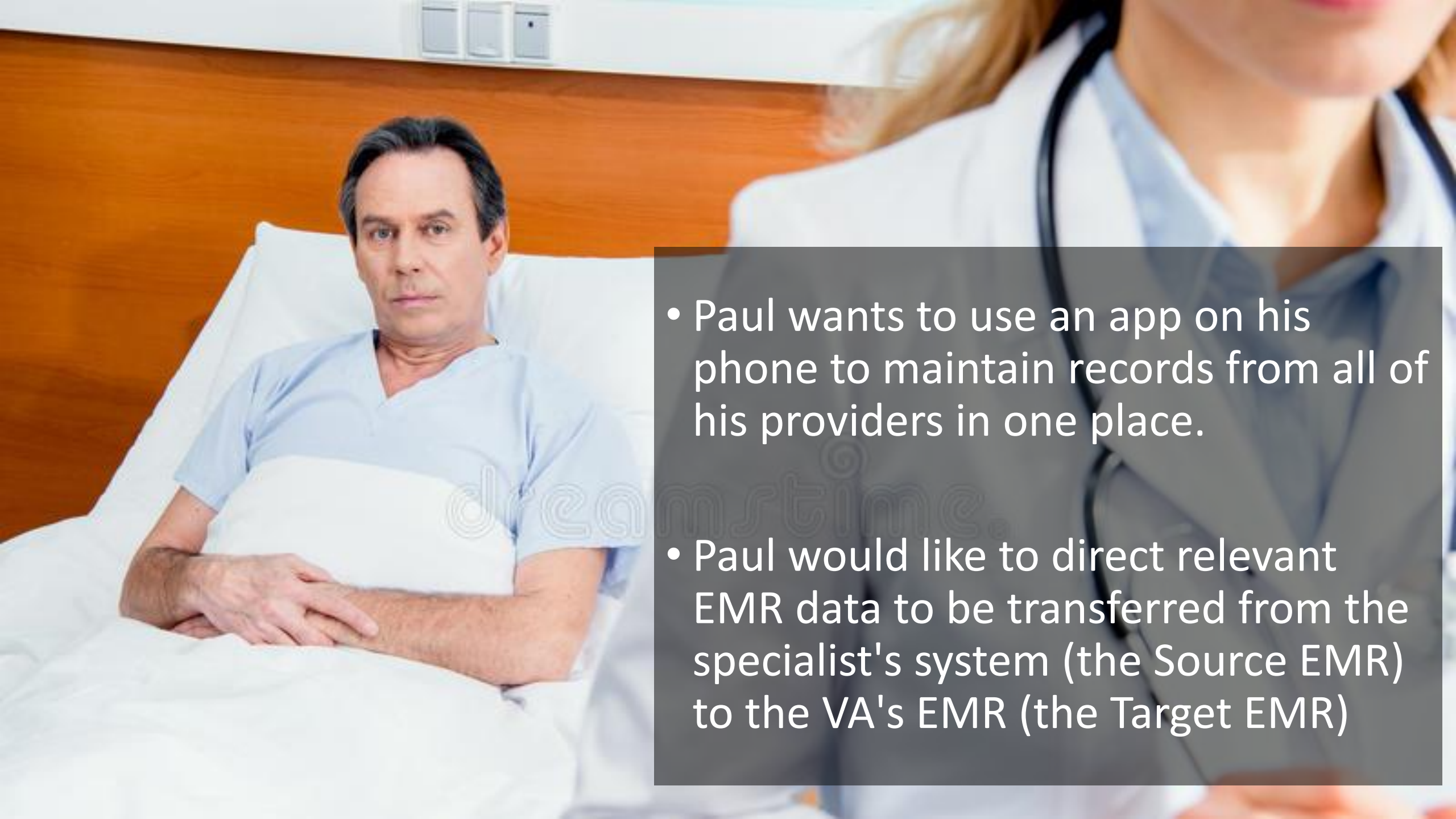
Recipient Name:	Recipient Phone: Recipient Fax:
Recipient Mailing Address:	Recipient E-mail (if applicable):


This CD contains
the personal health records of:
Paul Q.
• Insert into the inner ring of the CD drive.
If Mac user, CD must be opened manually.
MEDICAL RECORD
CD.COM™
Safely Control Your
Health Records!



.. but wait, didn't Apple just announce.. ?





- Paul wants to use an app on his phone to maintain records from all of his providers in one place.
- Paul would like to direct relevant EMR data to be transferred from the specialist's system (the Source EMR) to the VA's EMR (the Target EMR)

FHIR | A Standard Way to Access Data in EHR

Fast Health Interoperability Resources (FHIR)

- RESTful API – How to access
- Clinical and administrative data definitions
- FHIR Profiles – How much of spec is supported

But legally, is it okay to send PHI to a patient-owned mobile app?

Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524

- The Privacy Rule generally **requires** HIPAA covered entities (health plans and most health care providers) to provide individuals, upon request, with access to the protected health information (PHI)

- This includes the right to inspect or obtain a copy, or both, of the PHI, as well as to direct the covered entity to transmit a copy to a designated person or entity of the individual's choice

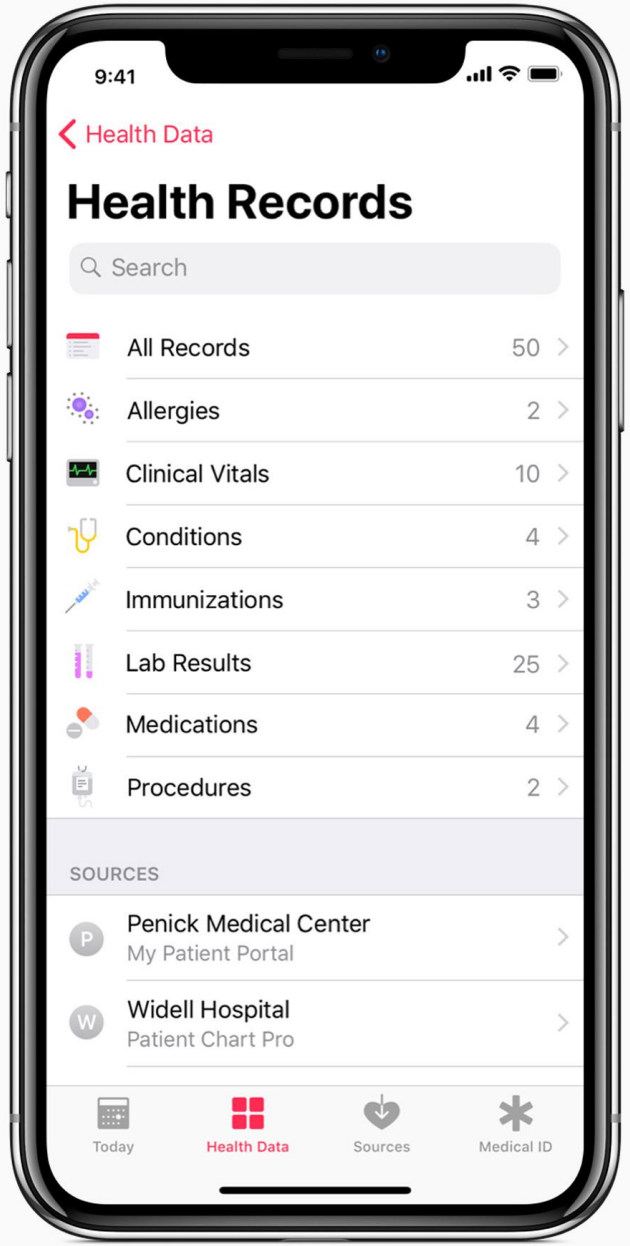
https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524

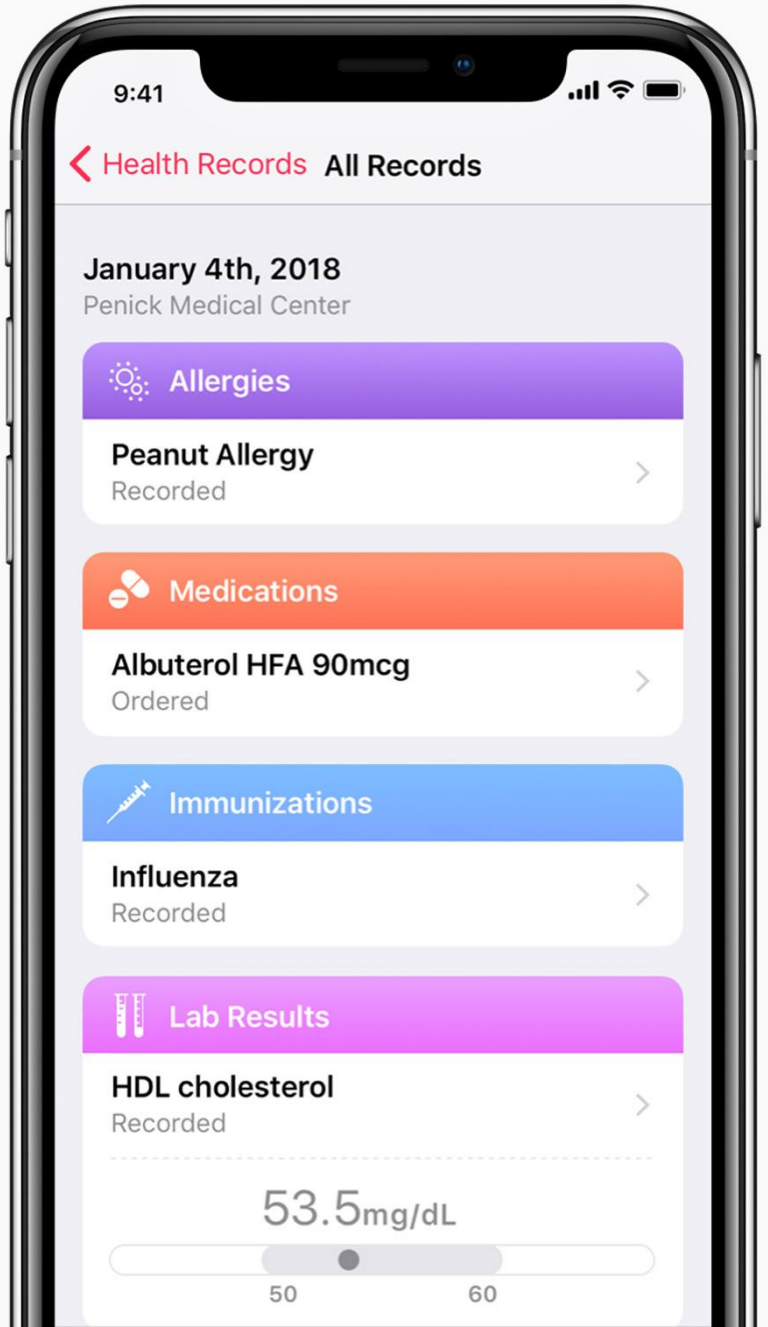
- A covered entity **may** require individuals to request access in writing, provided the covered entity informs individuals of this requirement.

- The Privacy Rule **requires** a covered entity to take reasonable steps to verify the identity of an individual making a request for access. The Rule does not mandate any particular form of verification (such as obtaining a copy of a driver's license), but rather generally leaves the type and manner of the verification to the discretion and professional judgment of the covered entity

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html



So, even if Paul wants to do this..



What records do you want? (Check appropriate boxes below):

Date(s) of Service: ____/____/____ through ____/____/____

☐ Discharge Summary ☐ Emergency Room Records ☐ Operative/Procedure Reports ☐ Billing Records

☐ Test Results (X-Rays, Lab/Pathology Results) Please specify: _____

☐ Other (Immunization Records, Medication Lists) Please specify: _____

How would you like your records delivered?

☐ Paper

☐ Home Delivery

☐ In-Person Pickup

He may still need to fill out this form!

☐ Electronic (Email, USB, CD, Portal, Other) Please specify: _____

Where do you want the information sent? (Fill in boxes below):

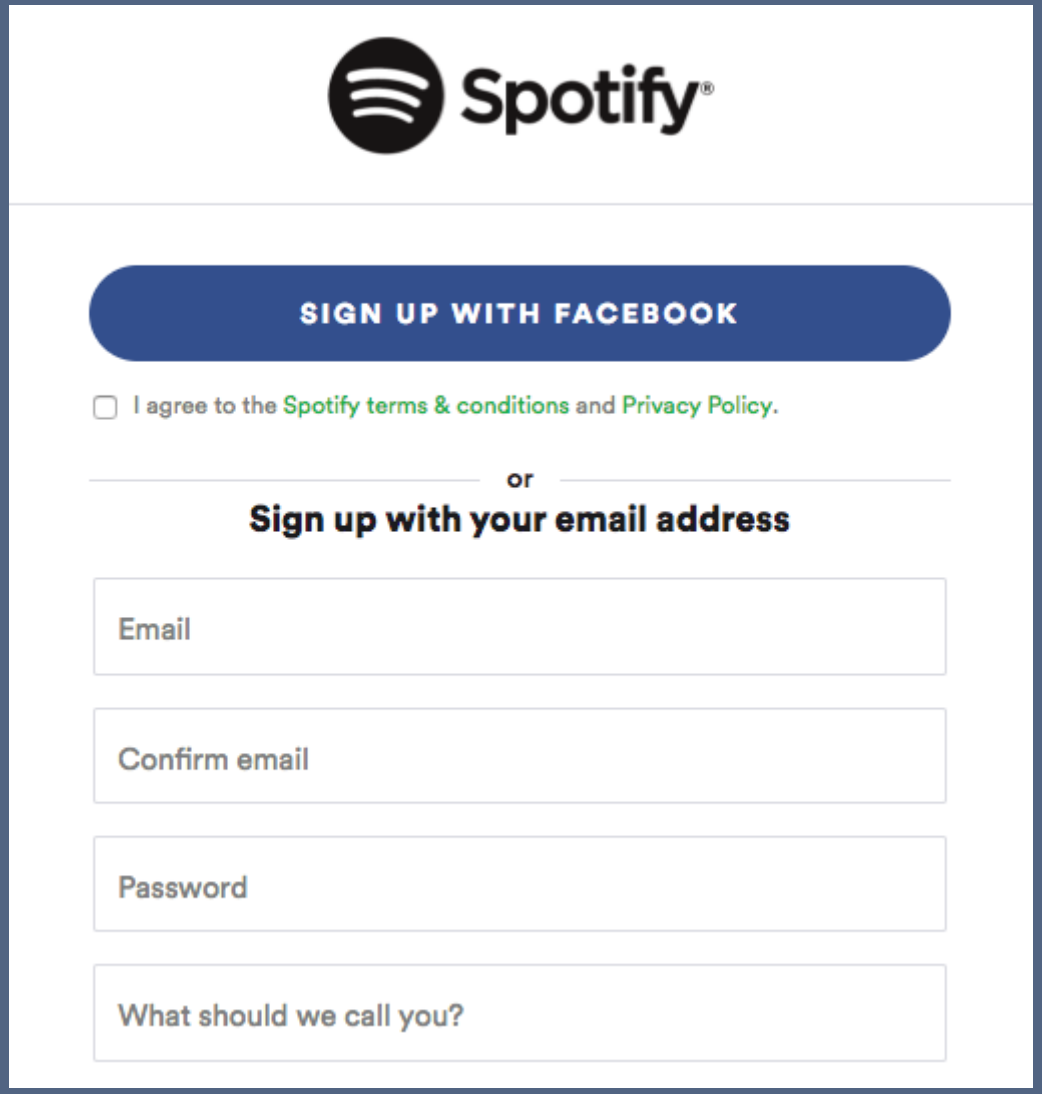
ORGANIZATION NAME should provide my records to: ☐ Self ☐ Personal Representative (indicated below)

Recipient Name:	Recipient Phone: Recipient Fax:
Recipient Mailing Address:	Recipient E-mail (if applicable):

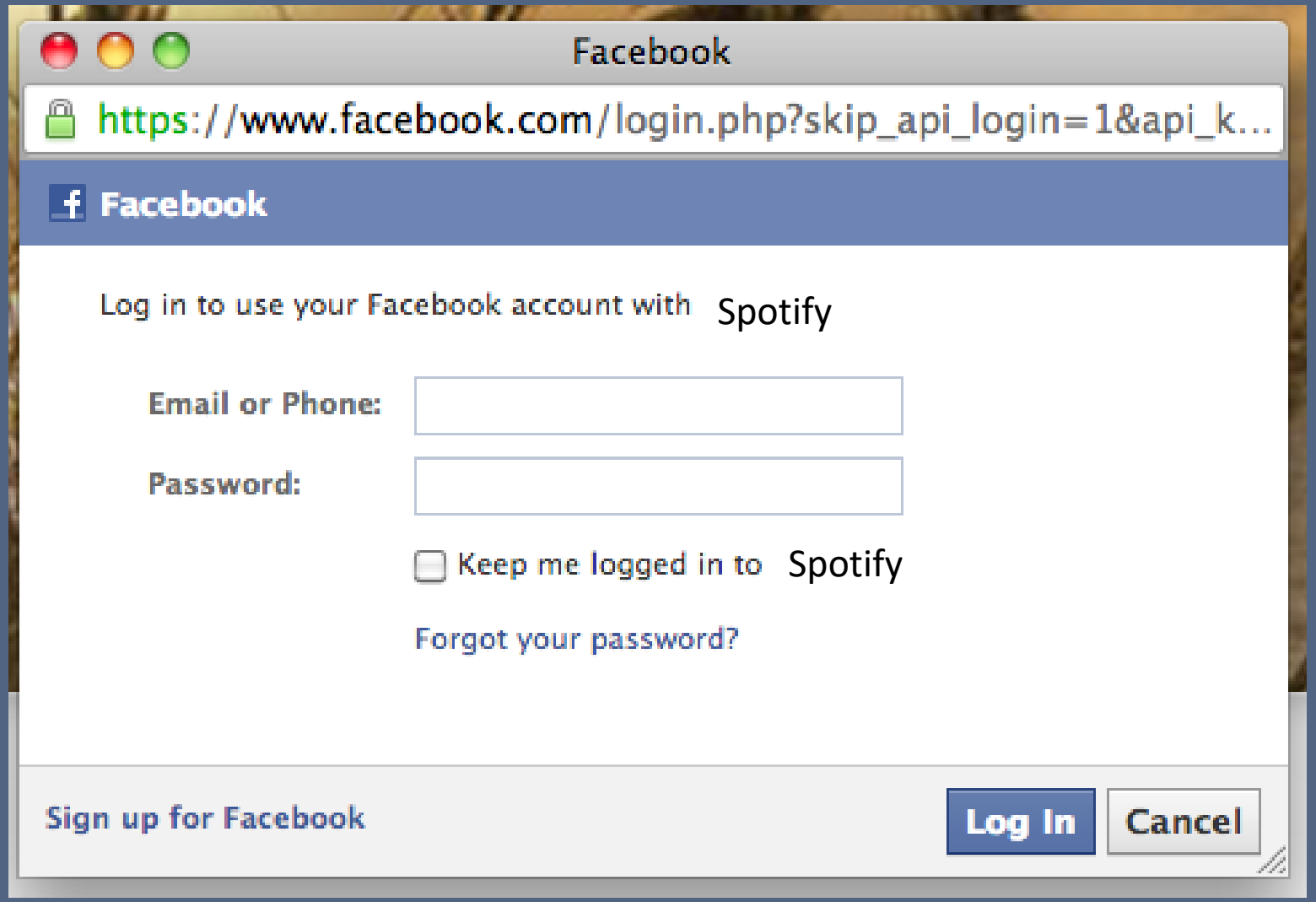
There has to be a better way..

.. enter OAuth

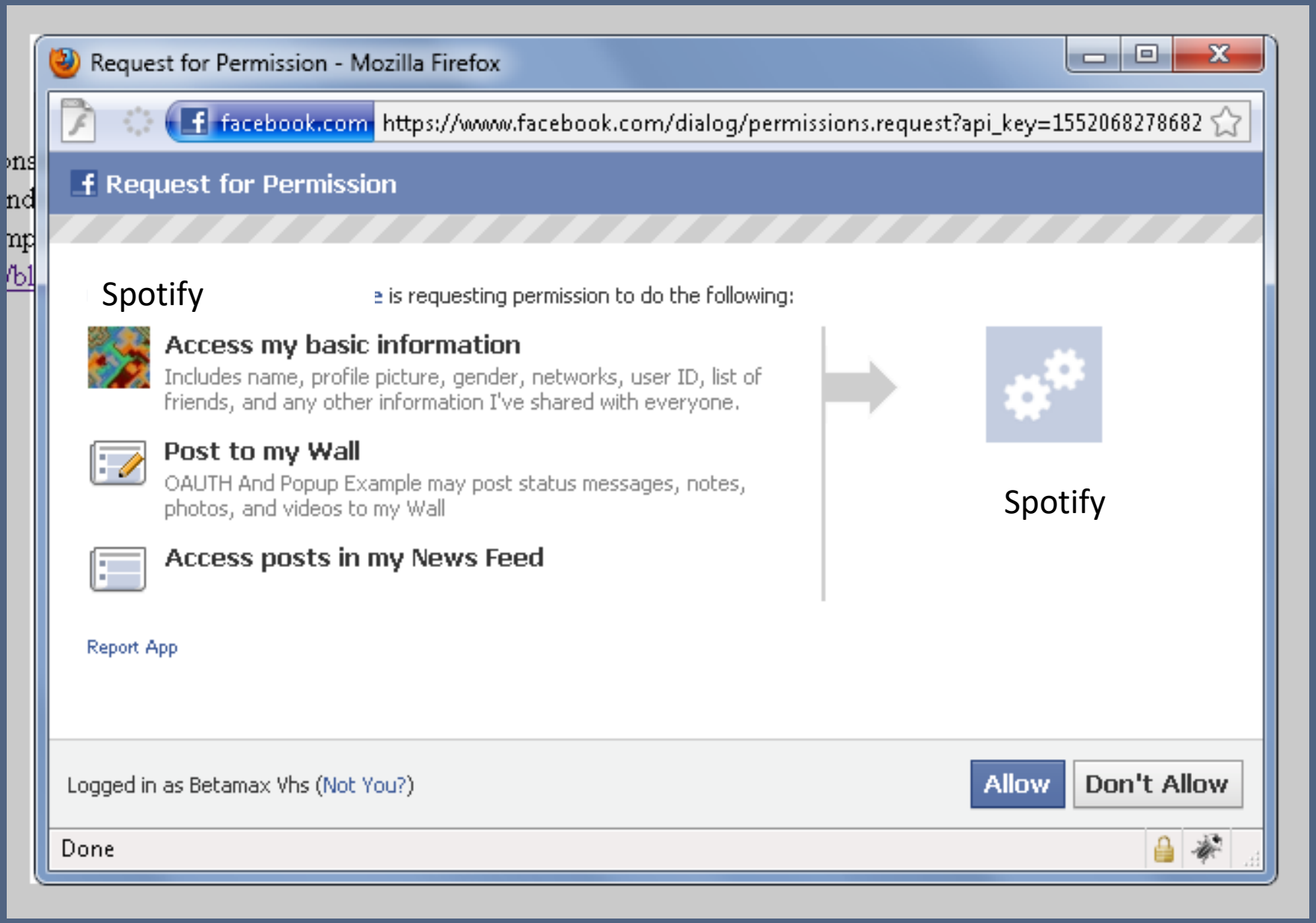
OAuth Primer –verify identify with trusted third party



OAuth Primer – Log into 3rd party authentication server



OAuth Primer – Specify information to share



OAuth with FHIR is no different

OAuth2: "two-legged auth"

Data Holder
EHR, Hospital, Clinic, Lab, Insurer, etc.

Authorize
(client secret)

Get /ehr/data

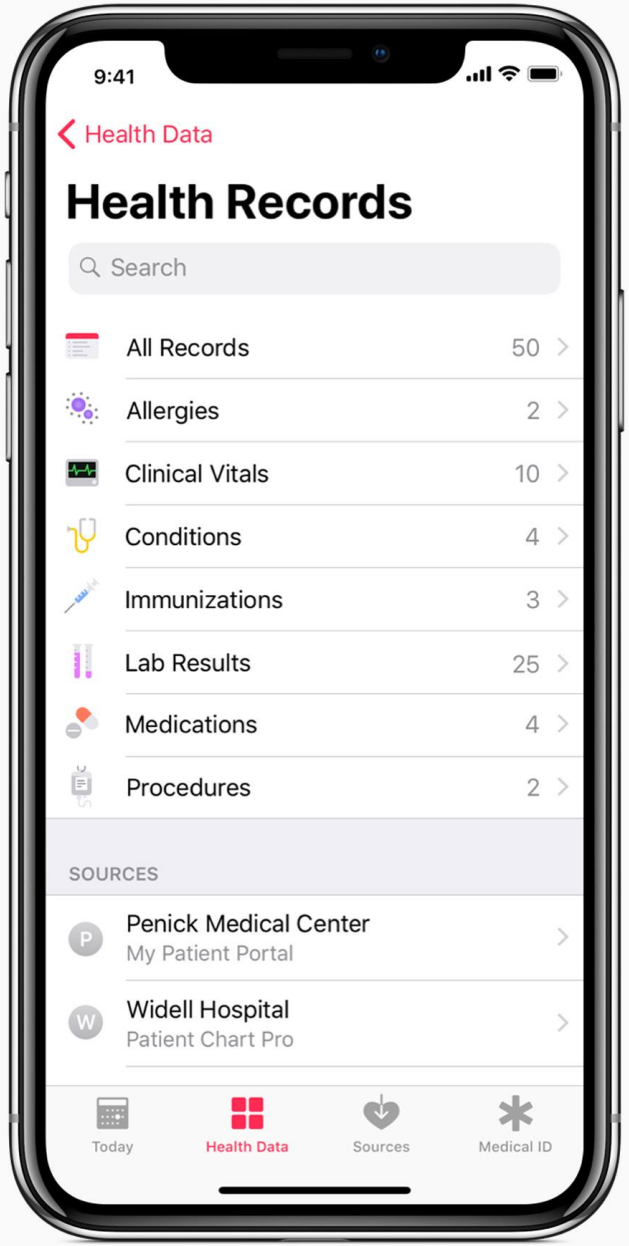
App
Decision Support, Visualization, eRx, etc.

Why not use OAuth Challenge Screen to capture Patient Consent?

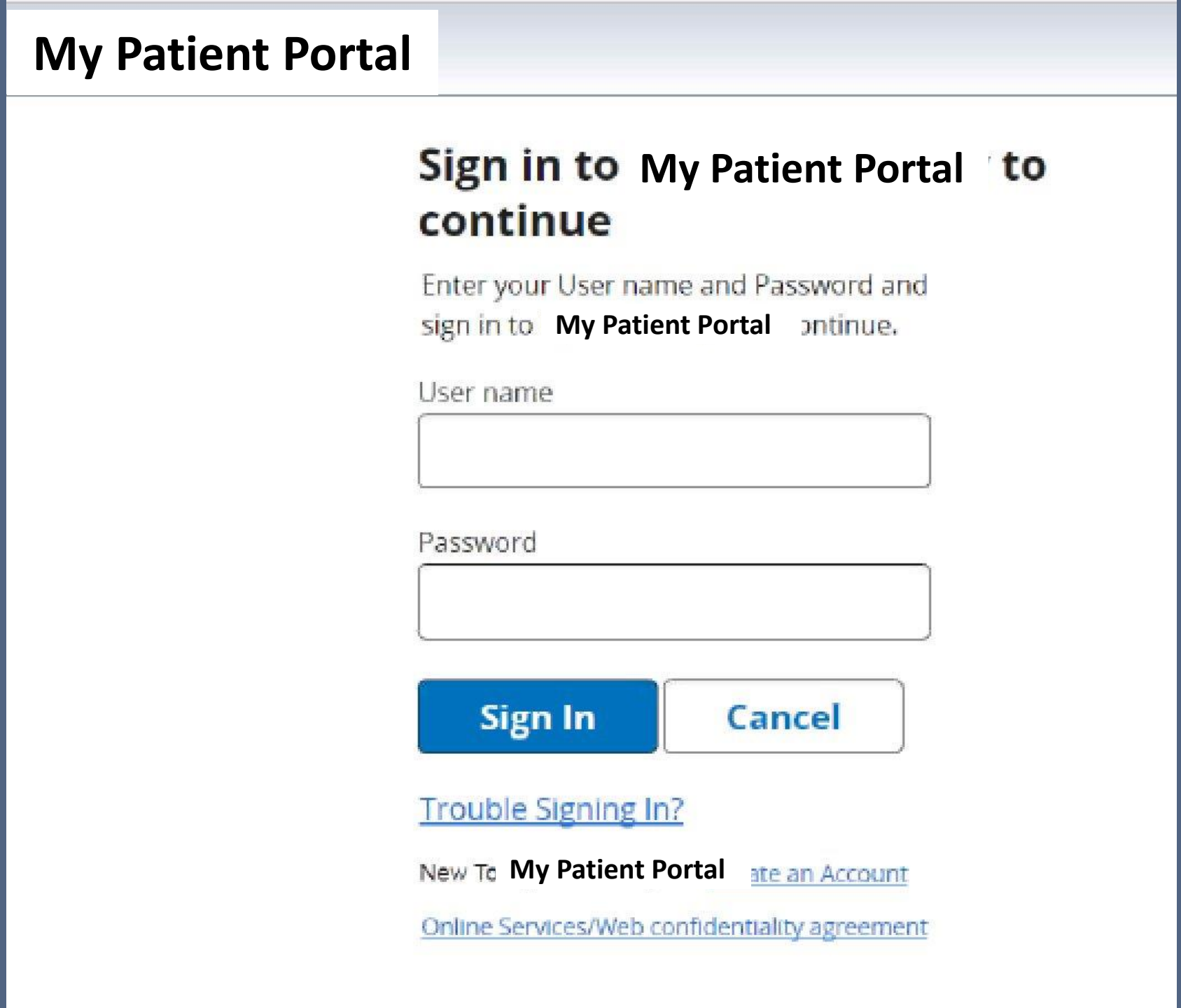
Suggested Approach

- Identify Authentication Server(s) to verify Patient Identify (e.g. Patient Portal)
- Configure Authorization Server to present OAuth Challenge screen that resembles Patient Consent form
  - Present simple options
    - Share Nothing (Default)
    - Share All PHI
    - Share PHI Not Marked “Restricted”
  - Involve Data Privacy and Governance group
- Standardize across digital health apps integrated with your EHR

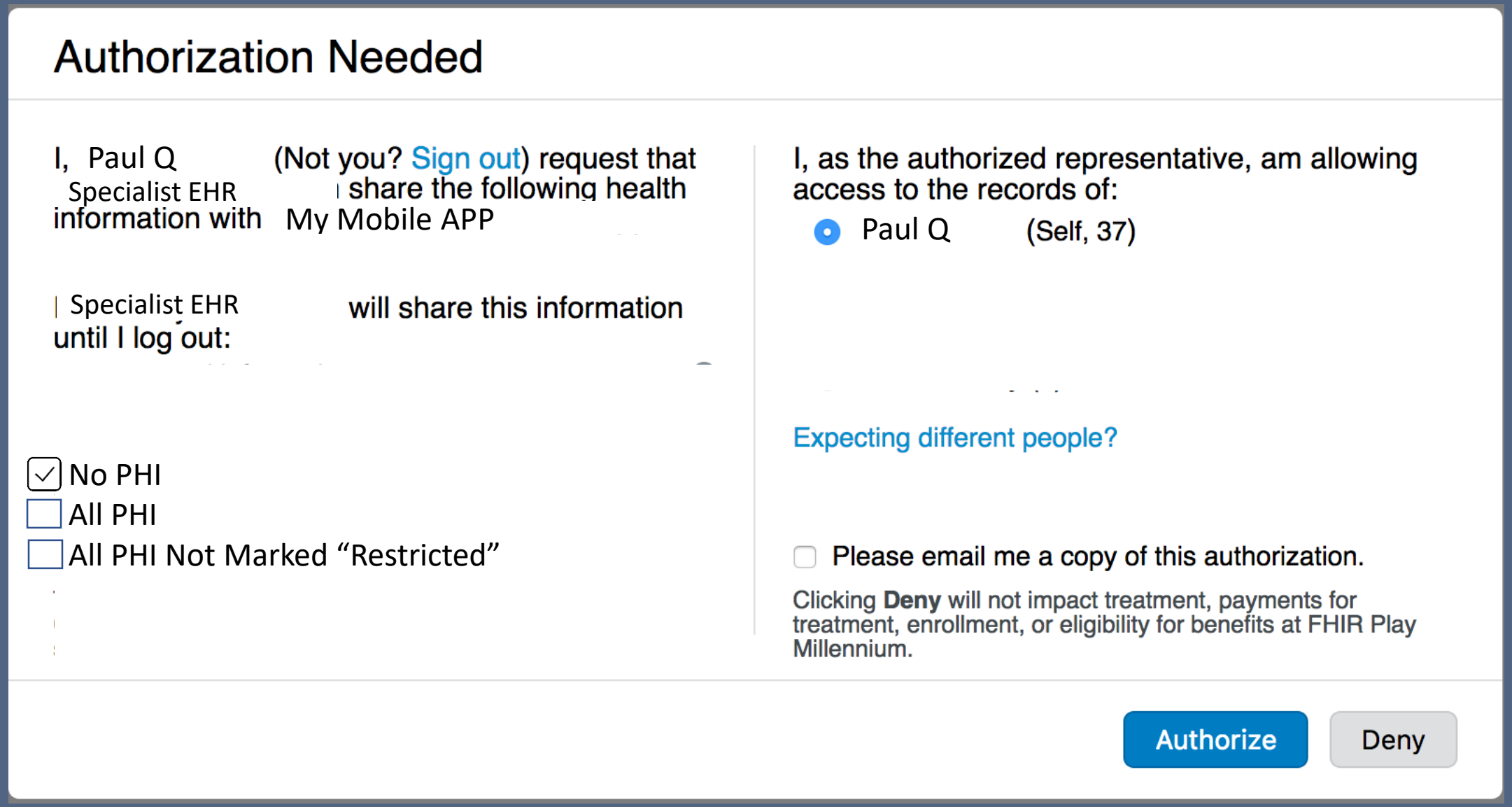
For Paul to use an app to download PHI from Specialist's EHR (or direct transfer of PHI to a 3rd party) ..



Verify identity against Specialist's patient portal



Specify which PHI to share with App



What records do you want? (Check appropriate boxes below):

Date(s) of Service: ____/____/____ through ____/____/____

☐ Discharge Summary ☐ Emergency Room Records ☐ Operative/Procedure Reports ☐ Billing Records

☐ Test Results (X-Rays, Lab/Pathology Results) Please specify: _____

☐ Other (Immunization Records, Medication Lists) Please specify: _____

How would you like your records delivered?

☐ Paper

☐ Home Delivery

☐ In-Person Pickup

☐ Electronic (Email, USB, CD, Portal, Other) Please specify: _____

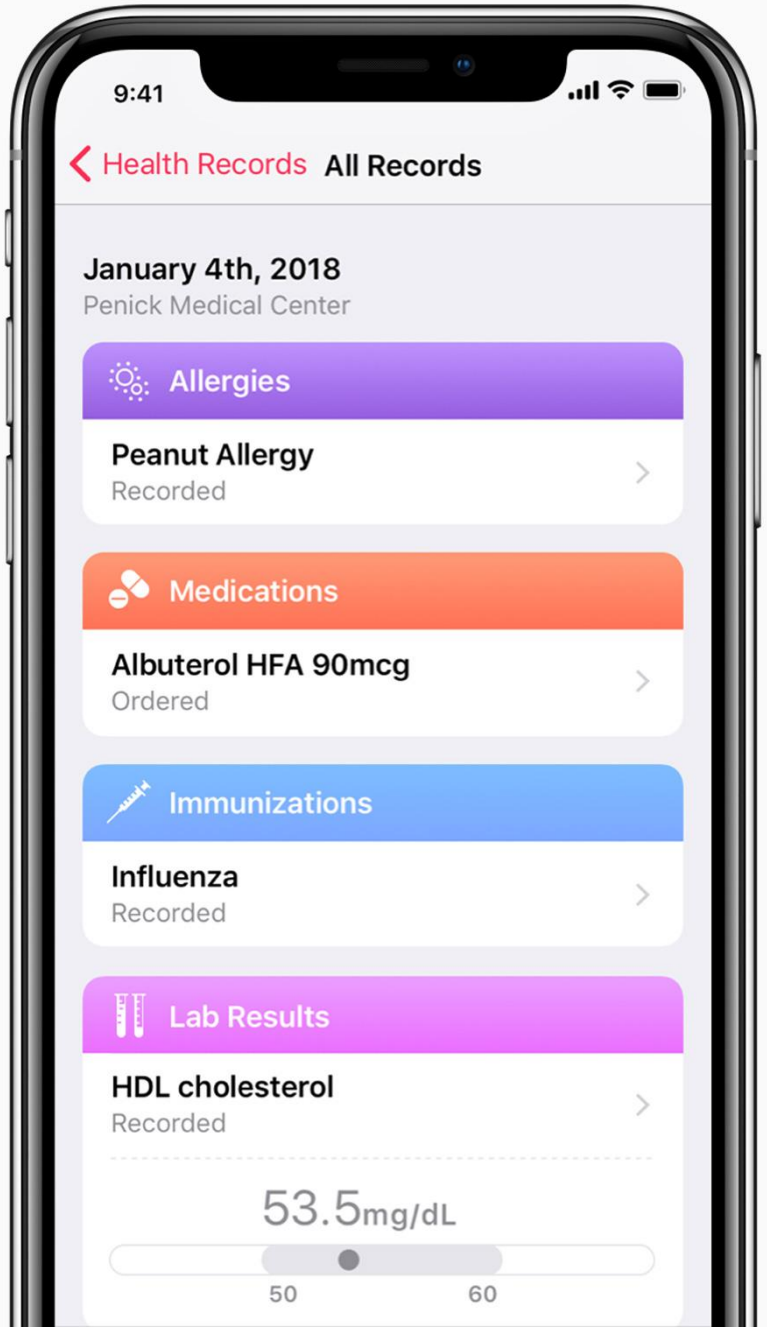
Look Similar?

Where do you want the information sent? (Fill in boxes below):

ORGANIZATION NAME should provide my records to: ☐ Self ☐ Personal Representative (indicated below)

Recipient Name:	Recipient Phone: Recipient Fax:
Recipient Mailing Address:	Recipient E-mail (if applicable):

Paul can then download PHI to mobile app, and view/share as desired



Questions/Comments?

Sandeep Giri

sandeep.giri@ucsf.edu