HIMSS18 The leading health information and technology conference

WHERE THE WORLD CONNECTS FOR HEALTH

Conference & Exhibition | March 5–9, 2018

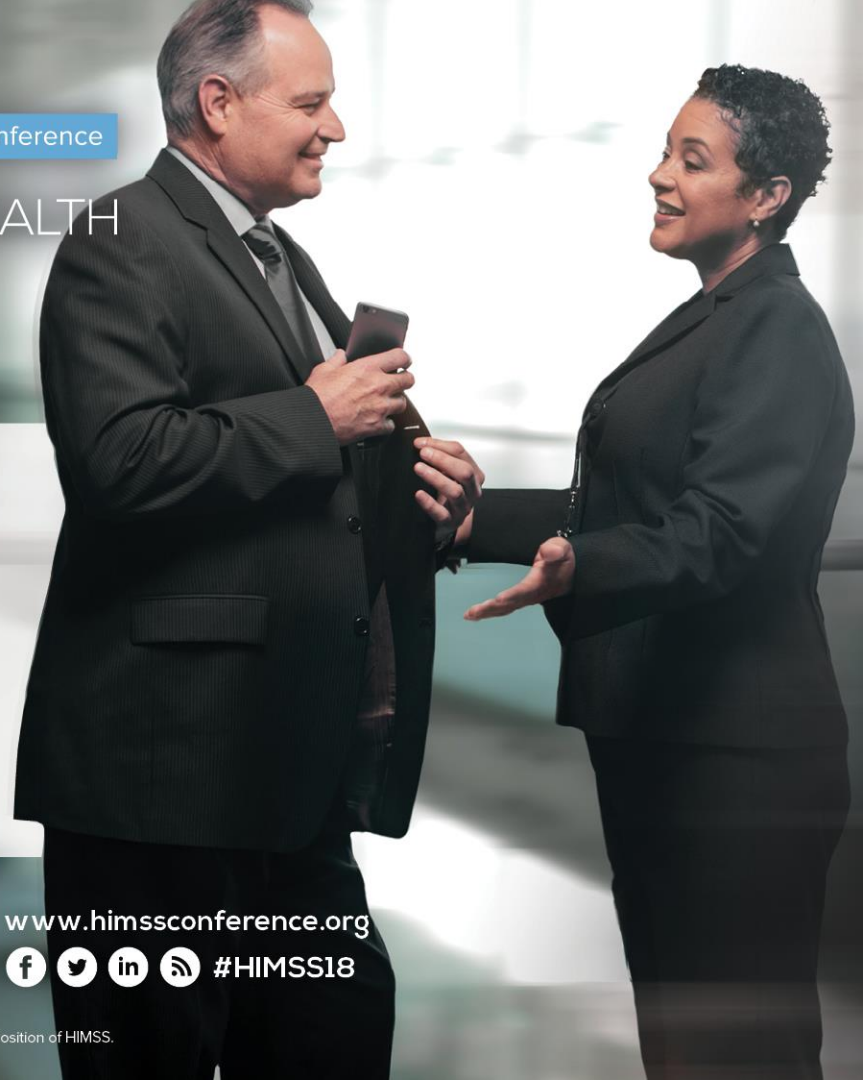
Las Vegas | Venetian – Palazzo – Sands Expo Center

Deploying A Holistic Identity Management

Session 27, March 6, 2018

Spencer L SooHoo, PhD Cedars-Sinai Health System (CSHS)

Kat Megas, MS National Institute of Standards and Technology (NIST)



COMMITMENT

www.himssconference.org

#HIMSS18

Conflict of Interest

Spencer L SooHoo, PhD
Has no real or apparent conflicts of interest to report.

Kat Megas, MS
Has no real or apparent conflicts of interest to report.

Agenda

- Background
- Problem Statement
- Use Case
- Architecture: **S**ingle-**F**ederated **I**dentity **L**ogin for **E**HR (Single-FILE)
- Benefits
- Trust Frameworks
- Governance and Privacy
- Identity Proofing
- Challenges/Lessons Learned
- Questions

Learning Objectives

- Explain the importance of a holistic identity and access management system
- Define the benefits of a federated, multi-factor authentication system
- Recognize the lessons learned from the design and implementation of a holistic identity and access management system

Background: Collaborative Effort

National Institute of Standards and Technology (NIST)

- National Strategy for Trusted Identities in Cyberspace (NSTIC)
- Federated Identity in Healthcare Pilot Program

Office of the National Coordinator for Health Technology (ONC)

- Improve health outcomes/quality and lower costs through health information technology
- Develop Lessons Learned Model Practice for Federated Identity in Healthcare

Cedars-Sinai Health System (CSHS)

- Academic Medical Center
- Focus on high-quality patient care, research, and education

Background: Trusted Identities Pilots

"Individuals and organizations employ secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation."

Background: Impact of the Pilots and their Partners

over **9.6 million** individuals impacted

200+ partner organizations convened

advances across **12** market sectors

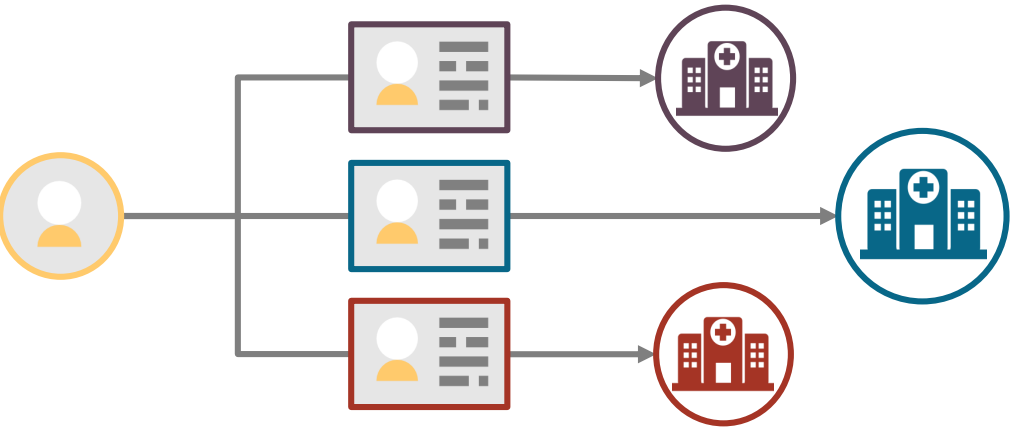
development of **16** multi-factor authentication solutions

Since 2011, the Pilot Program has seeded the market with trusted identity solutions across a number of verticals and industries, providing funding to 24 pilots to address barriers in the Identity Ecosystem and catalyze the marketplace of solutions.

#HIMSS18

Background: Proliferation of Identity Silos in Healthcare

- **March 2016:** NIST, in coordination with ONC, issues a Federal Funding Opportunity to pilot a federated identity system in healthcare.



- Different healthcare systems often have an Electronic Health Record (EHR) system that will likely be **independent implementations.**
  - *Separate login credentials* for each EHR system, subject to different complexity rules and password lifetimes.
  - These factors may *discourage using one or both systems*.

Background: Cedars-Sinai, NIST, ONC Collaboration

- **September 2016:** Cedars-Sinai Health System wins the pilot award to implement a federated identity, single sign on, multi-factor authentication solution across distinct healthcare systems for patients and providers.
- Solution proposed:
  - Intended to simplify patient transition from an acute-care setting, to post-acute care settings.
  - Patients and providers will have a single federated credential.
- Objective: Provide better access to information to improve quality of care.

Partners will collaborate and create a Lessons Learned Model Practice for Federated Identity in Healthcare.

Use Case:

Transition of Patients from Acute-Care to Post-Acute Care

California Rehabilitation Institute

Cedars-Sinai Medical Center

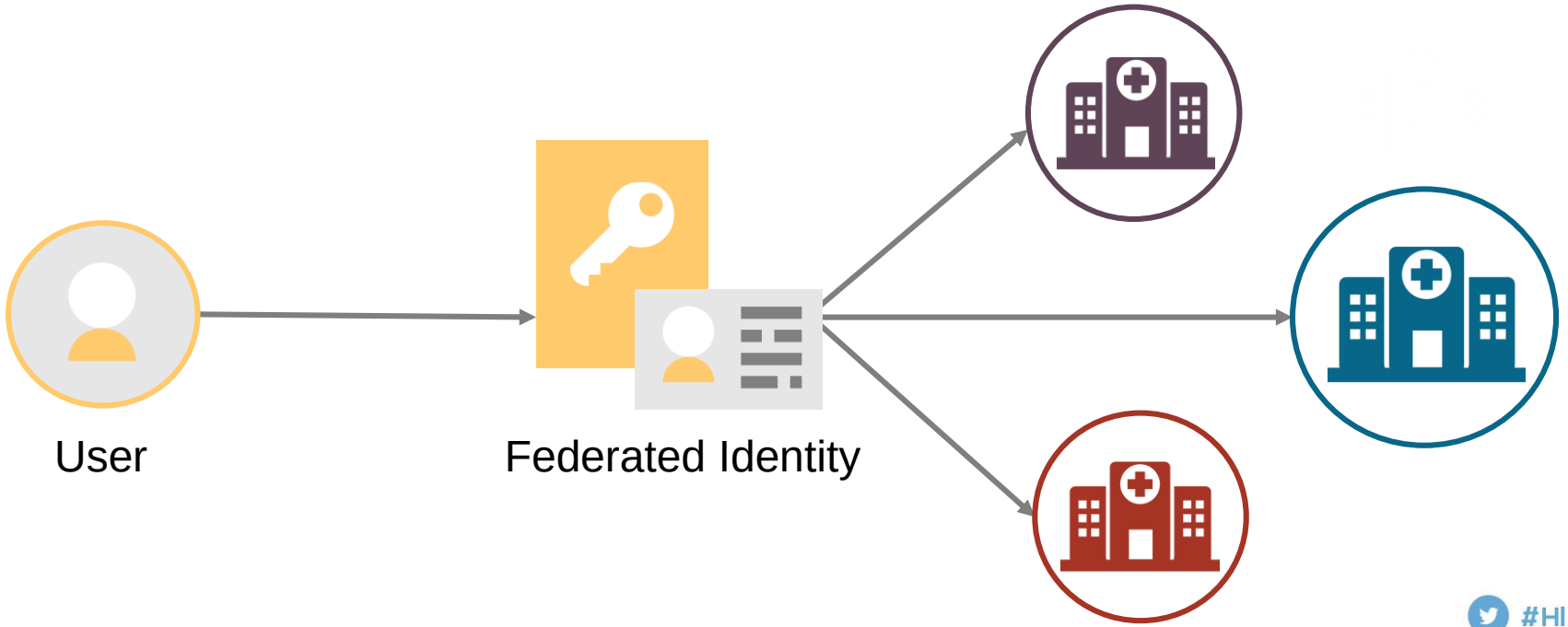
- **Ease of access** to all records is important to:
  - patients (or proxy)
  - providers that provide care at multiple facilities with unique EHR implementations
- **Real-time access** to up-to-date and detailed historical information is essential for optimal patient care.
  - **Access to information prior to transition of care** is required for smoother patient hand offs
  - **Delay of several hours** between transfer of patient and availability of summary data at California Rehabilitation Institute's EHR implementation
  - **Medication reconciliation** is critical for continuity of care.

Architecture: Single-FILE Overview

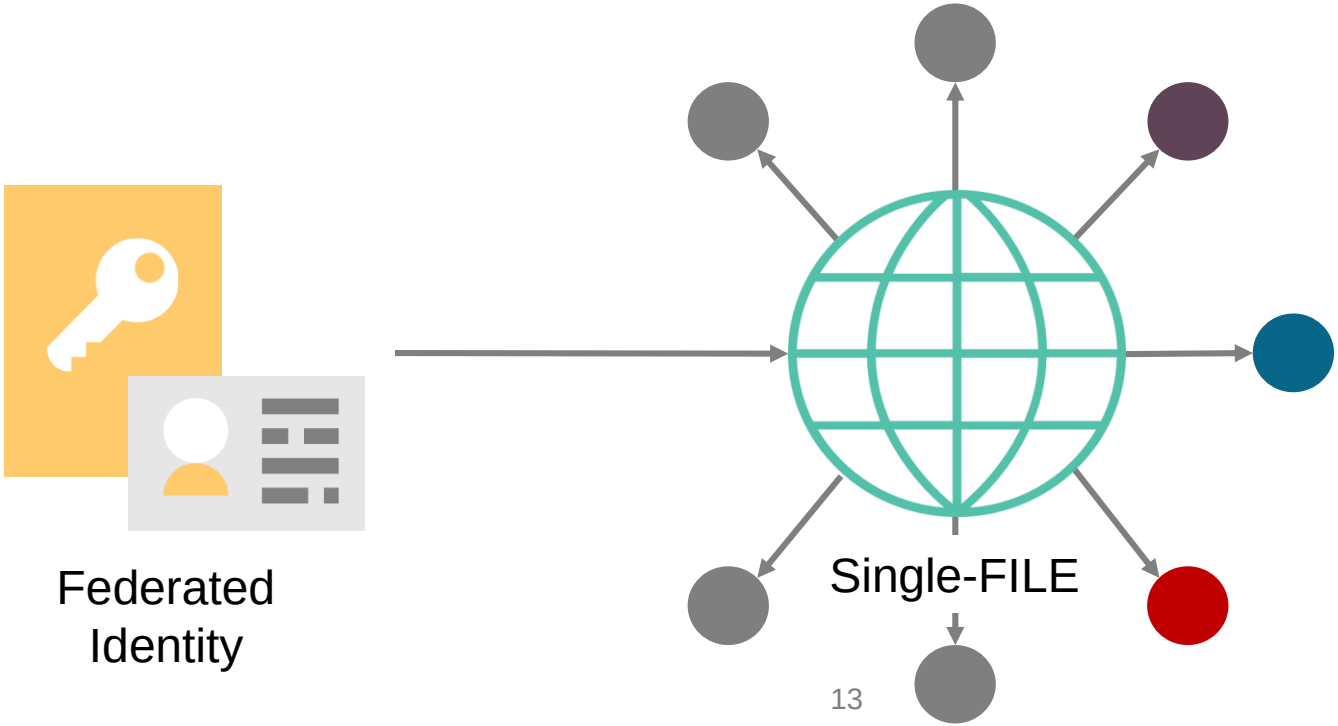
Use standards-based technology for Single Sign-On integration for patients and providers to use a single identity to access multiple, distinct EHR implementation

- Addresses both patients and providers
- Both Cedars-Sinai and California Rehabilitation Institute use Epic for EHR
- Multi-factor Authentication mandatory for providers, optional for patients
- Providers must pick an institutional credential for the federated credential
- Patients can use existing MyChart credential, social credential, or create Single-FILE credential
- Robust Identity Verification implemented to ensure privacy

Architecture: Federated Model

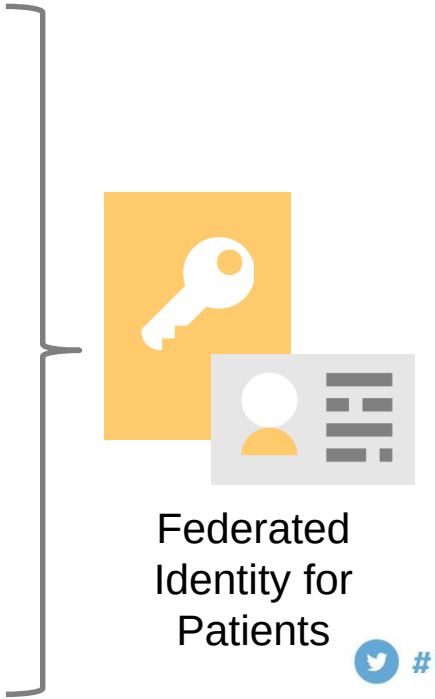


Architecture: Identity Broker Function



Architecture: Federated Identity for Patients

- Social Credential: Facebook or Google
- Institution Credential: Cedars-Sinai or Cal Rehab My Chart credentials
- Single-FILE Managed Credential



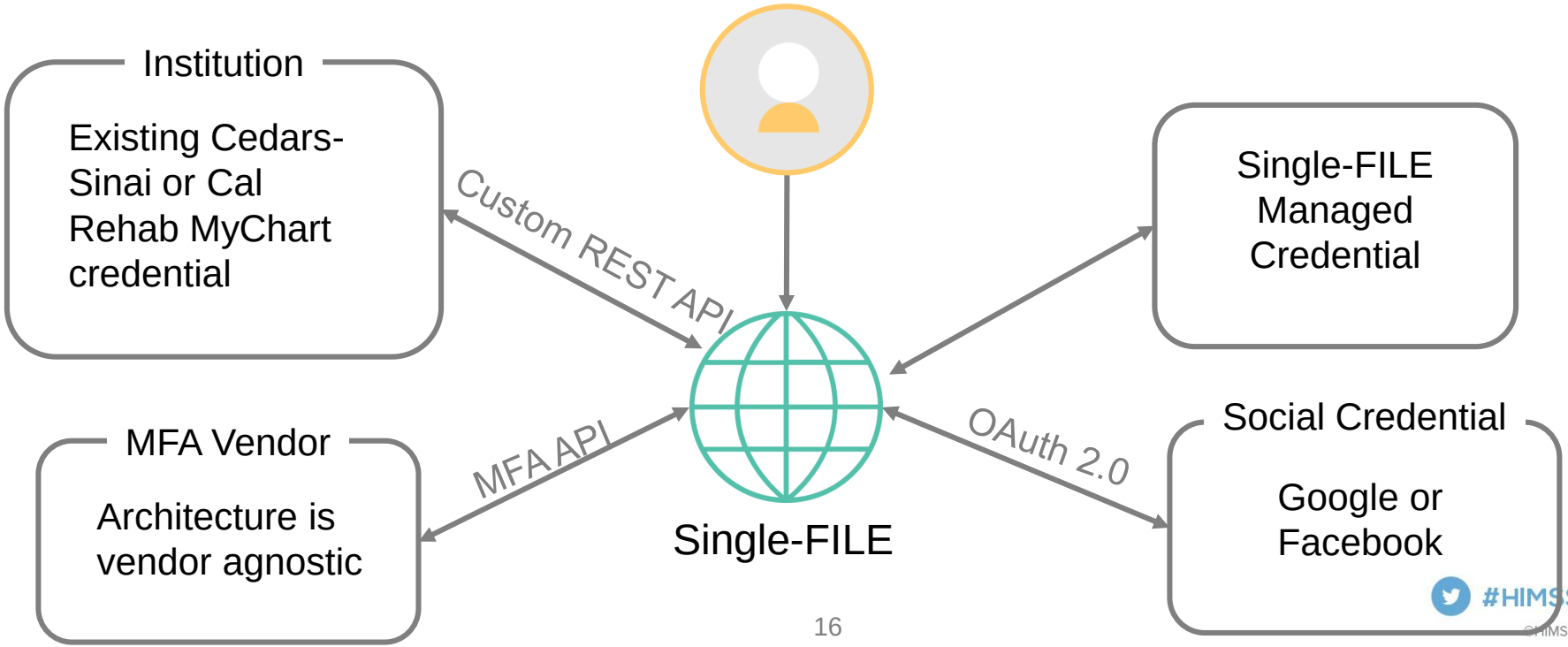
Architecture: Federated Identity for Providers

Institution Credential

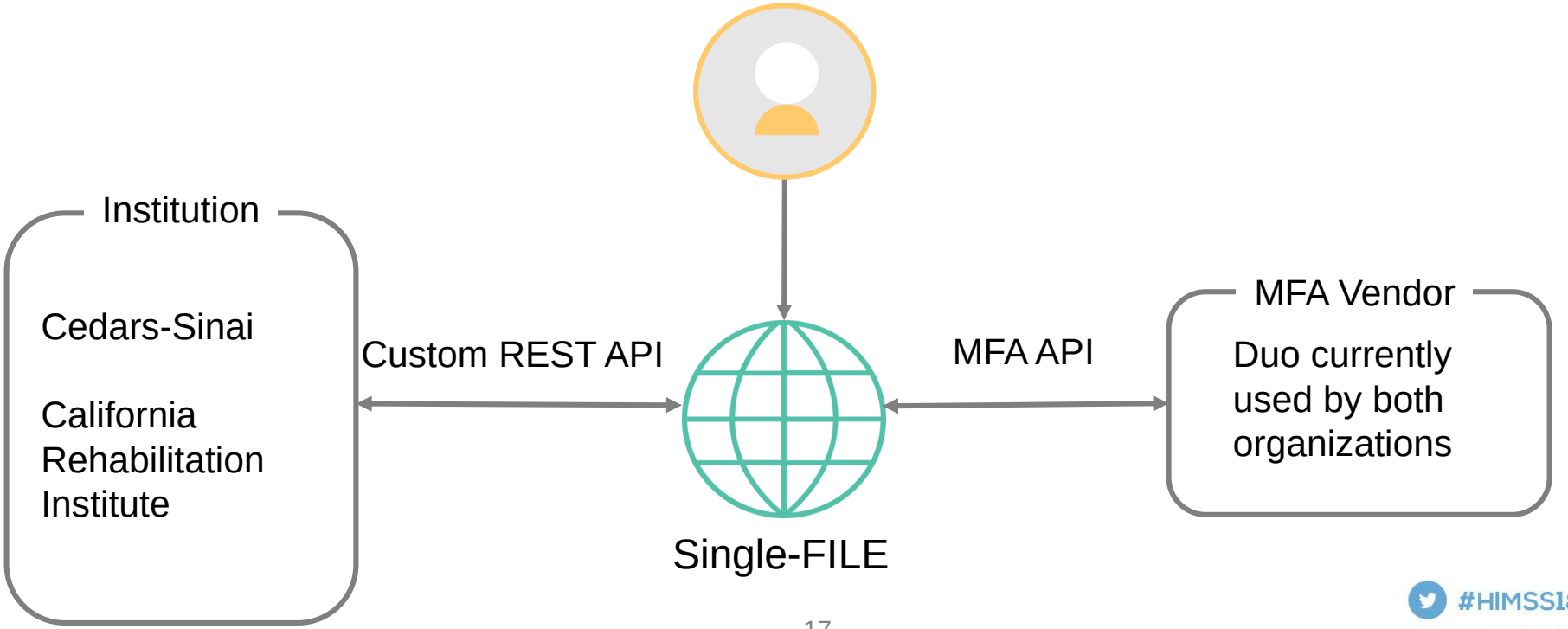
Provider selects either
Cedars-Sinai or Cal Rehab Credential

Federated Identity for Providers

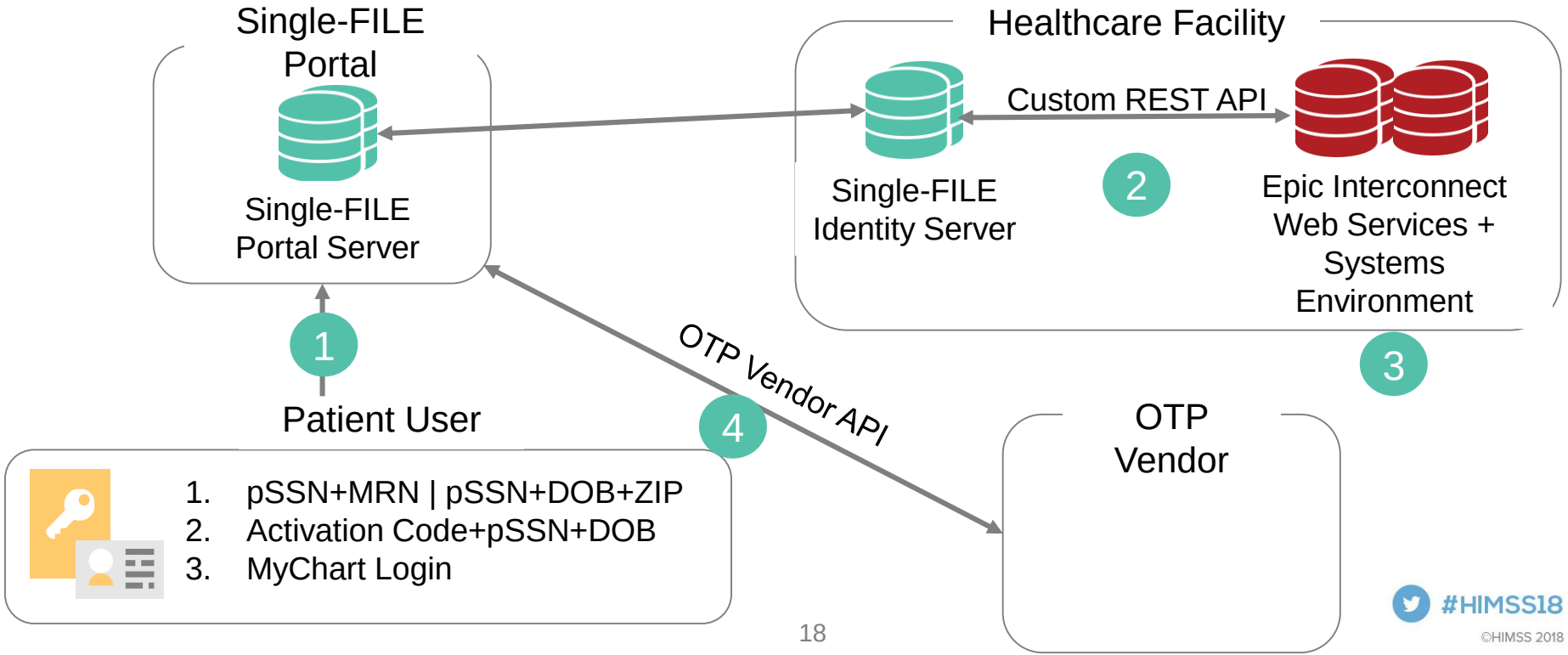
Architecture: Authentication Broker for Patients



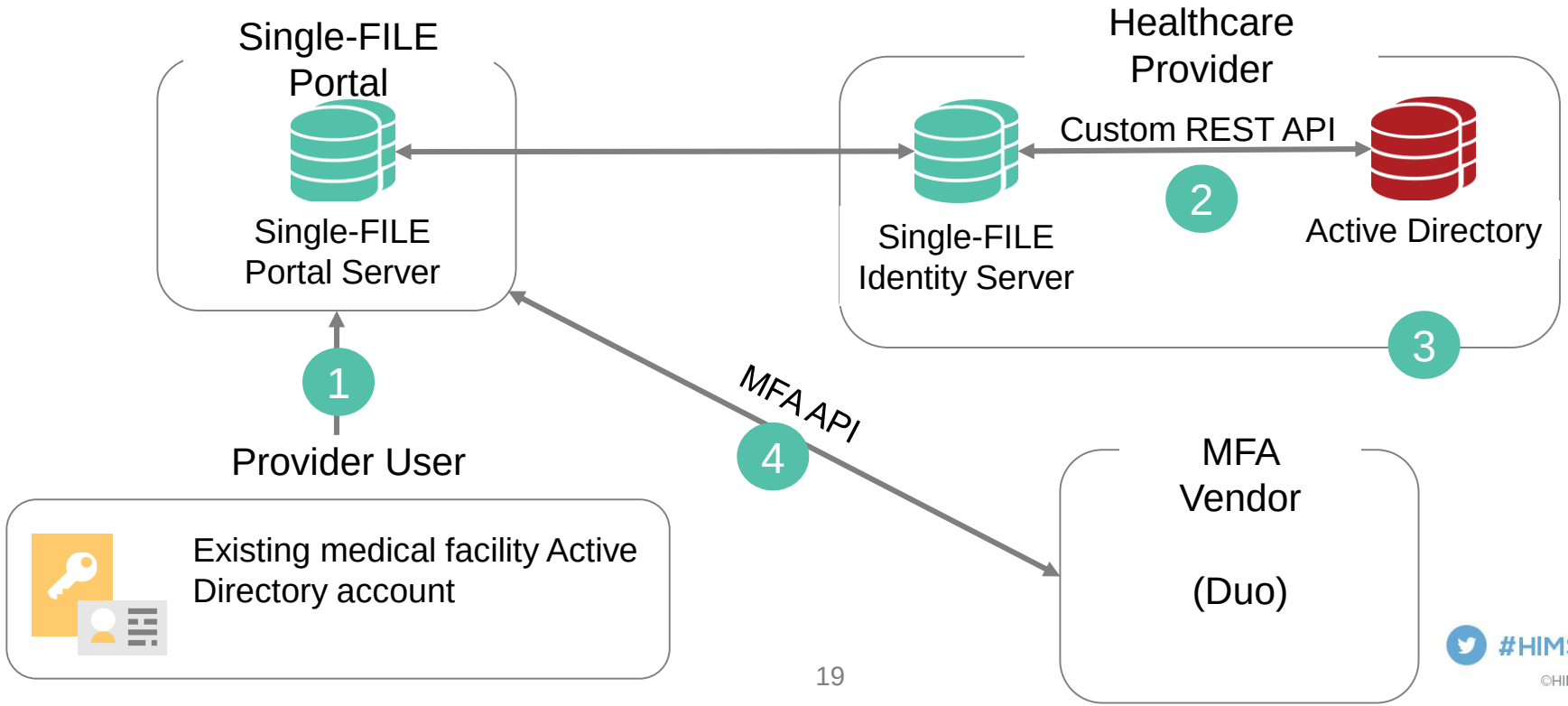
Architecture: Authentication Broker for Providers



Architecture: Identity Verification for Patients



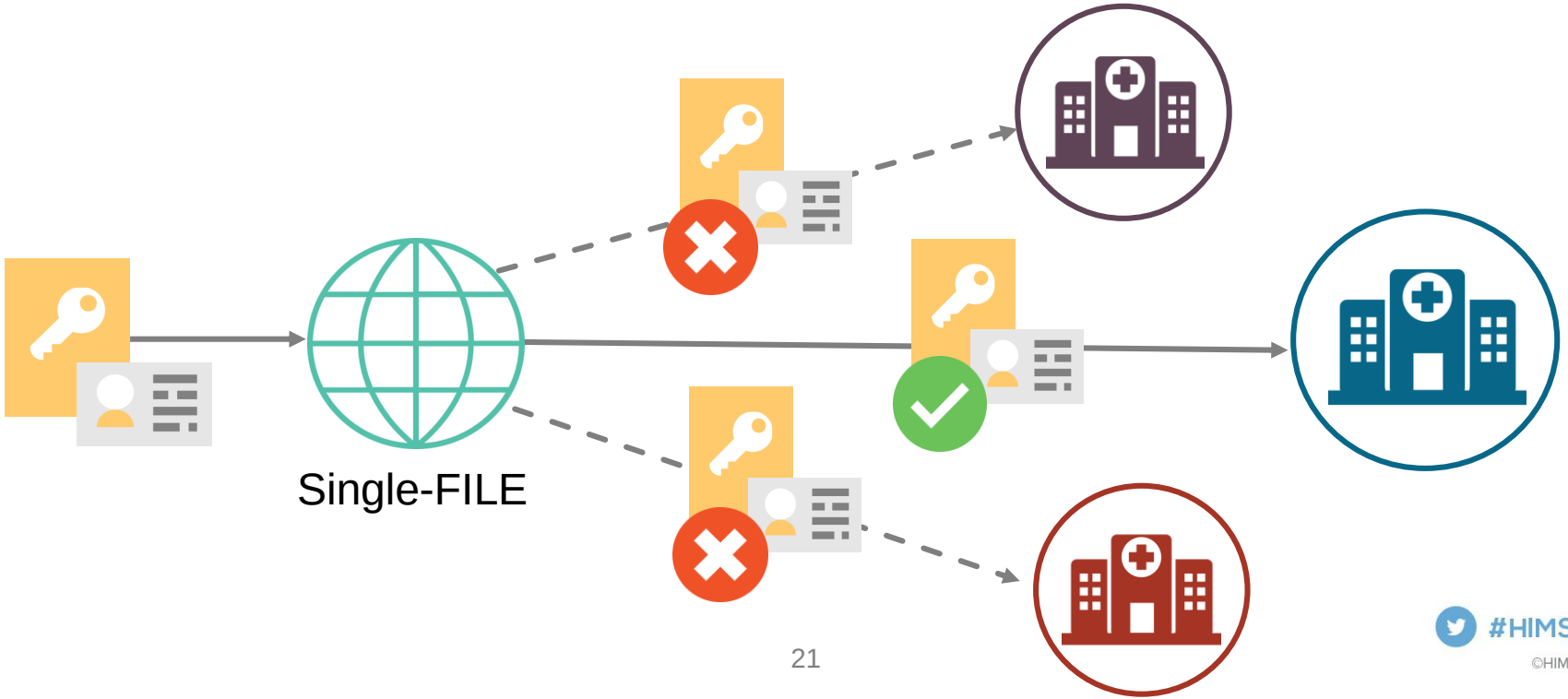
Architecture: Identity Verification for Providers

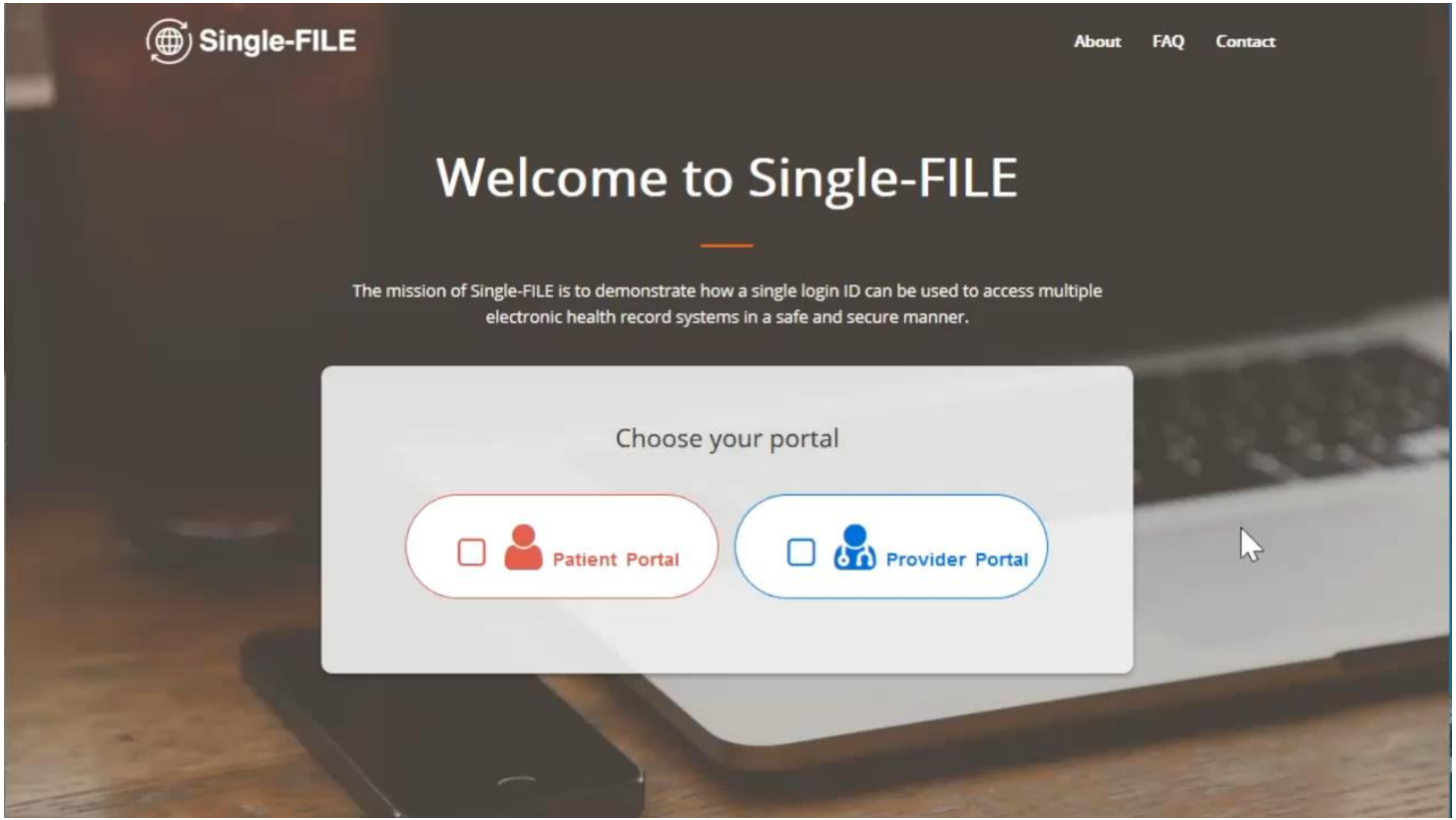


Architecture: Multifactor Authentication Platform

- Patients
  - SMS Text message verification
  - Phone call and passcode verification
  - Authy OneTouch App (Twilio push notification and token codes)
  - Google Authenticator
- Providers
  - Duo Push
  - Duo Token Passcode

Architecture: Single Sign-On Facility Authorization




Single-FILE
About
FAQ
Contact
Welcome to Single-FILE
The mission of Single-FILE is to demonstrate how a single login ID can be used to access multiple electronic health record systems in a safe and secure manner.
Choose your portal
Patient Portal
Provider Portal

Benefits

Privacy enhancing

- Pseudonymous access
- Identity verification (OTP)
- Reduce risk of identity theft

Healthcare operations

- Medical risk reduction due to better access to information
- Distribute costs for shared infrastructure through a federated model

User convenience

- Reduce the strain of remembering multiple logins
- Provide secured access to multiple EHR systems
- Simplify healthcare provider workflows

Security enhancing

- MFA option for patients/MFA required for providers
- Standardize methods for identity proofing and conformance monitoring

"On the Internet, nobody knows you're a dog."

"How do I know that the identity you created is one that I can *trust*?"

Trust Frameworks

Identity Federation

- An individual can use a credential from one issuer with another relying party.

Trust Frameworks

- Rules that define the business, legal, and technical requirements
- Enables members of a federation to trust a credential from another issuer for:
    - Conducting identity management responsibilities
    - Sharing identity information
    - Using identity information that has been shared with them
    - Protecting and securing identity information
    - Performing specific roles within the federation
    - Managing liability and legal issues

Governance and Privacy

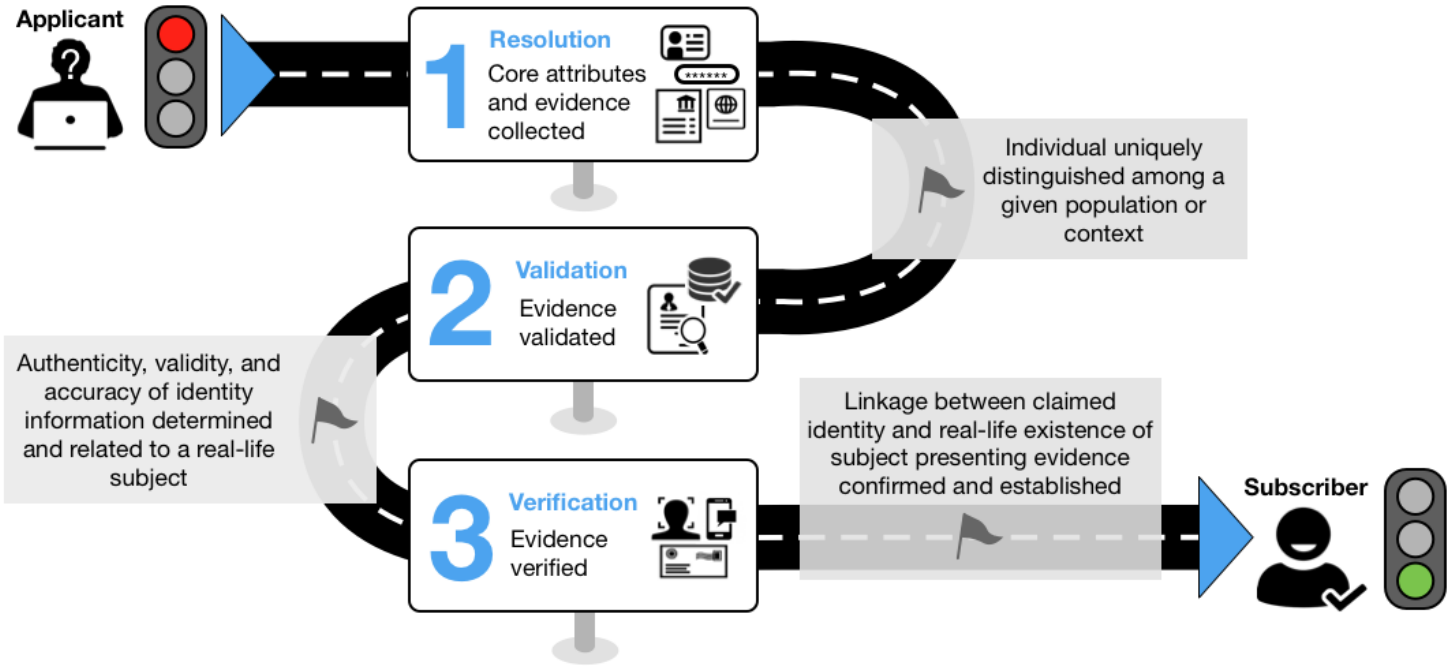
Create a framework to allow healthcare providers to become a CSP for tech companies developing patient and provider facing healthcare applications

Enforce a uniform set of standards for identity proofing, conformance monitoring, and identity management for healthcare

Advance the development of connectivity to third party healthcare applications aimed at improving wellness and enhancing the delivery of care

Identity Proofing

- NIST 800-63A Digital Identity Guidelines: Enrollment and Identity Proofing
- HIMSS Patient Portal Identity Proofing and Authentication



Identity Proofing

Identity Assurance Levels (IAL)

IAL 1

IAL 2

IAL 3

Identity Proofing

Patient Identity 'Proofing' in Healthcare Operations

		Requirement	Identity
	**Treatment**	Obtain enough unique identifiers to ensure that diagnostics and treatments are being provided to the correct person and have the ability to contact them.	• Name • DOB • Telephone #/e-mail
	**Payment**	Prevent fraudulent claims and improve the ability to collect for services tendered	• Insurance Policy • Driver's License • SSN • Address (Zip)
	**Operations**	Track patients through various phases of care within the system	Create a unique Medical Record Number (MRN) that is facility specific

Identity Proofing:

Competing Factors for Increasing IAL in Healthcare

- Identity management system exists for employees/providers
- EHR serves as proxy for patient identity management
  - Designed for Treatment, Payment, and Operations (TPO)
  - Not designed for identity management
  - Lack of fields to capture specific identity proofing pieces
- Operations needs to incorporate robust identity validation and verification as part of workflow
- Implementation of biometrics may decrease options of access due to increased technology requirements

Healthcare Specific Legal & Policy Issues

- **Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524**
  - HIPAA requires that patients be able to access copies of their health data
  - Cases where a patient's identity cannot be verified*: can't do pseudonymous identities without having actual identity*
- **Children's Online Privacy Protection Rule (COPPA)**
  - Allows a parent to have access to the medical records about his or her child under age 13, as his or her minor child's personal representative
  - Parents and legal guardians must request *proxy access*

Challenges/Lessons Learned: Operations

- Expertise and authority needed to make decisions are **compartmentalized** within organizations and varies amongst organizations
- Implementation staff not necessarily aware of or able to influence policy decision
- Project complexity affected by **organizational structure/priorities**
  - Each participating organization needs to be on **versions** of software that support the common standard used
  - Cost of frequent upgrades can lead to **skipping intermediate versions--> impact on project plans/interoperability**
- Provider organization **implementation may lag** significantly

Challenges/Lessons Learned: Technology

- Technology platform **interdependencies** (different software vendors)
- Security & privacy **best practices are evolving**, may not be supported by healthcare technology vendors in a timely fashion
- EHR landscape changes rapidly
  - Epic upgrade supported standards-based SAML for SSO after project initiation
  - Epic Care Everywhere-Happy Together available after project initiation
    - Allows for single patient credential at other independent healthcare provider Epic sites
    - Single-FILE will allow use of social credential and MFA

Challenges/Lessons Learned: Trust Framework

- Trust Framework concepts **novel** to health care
- Privacy Risk Assessment Methodology (PRAM) process **less structured** in healthcare & **focused on compliance**

Acknowledgments

- **NIST**
- **ONC**
- **Select Medical and the California Rehabilitation Institute**

The Cedars-Sinai Team

Core Project Team
Anil Goud
Rick Riggs
Ben Robbins
Pam Roberts
Donaldo Rodriguez
Spencer SooHoo
Lyna Truong

Development Team
Ajay Arora
Hammad Ausaf
Marcin Bauer
Brian Haigh
Greg Huang
Matthew McLaughlin
Harold Moyse
Marc Trotoux
Richard Villaran

UX Consultant
Nelly Jacobo
Matthew Pufall

Network Security
David Murray

Citrix Engineering
Mike Chin
Zacharias Edakkara

Epic DBA Team
Mike Khuong
Andrew Lee

Questions?

Spencer L SooHoo
spencer.soohoo@csmc.edu

Kat Megas
katerina.megas@nist.gov

Funded by NIST Award 70NANB16H252