PERSONAL HEALTH RECORD

Private, encrypted, distributed, health and medical data

“Medical devices and EHR systems are notoriously vulnerable to remote compromise”

James Scott, Senior Fellow, Institute for Critical Infrastructure Technology

Motivation

People want to:

- Access all their health data at anytime and from anywhere.
- Secure and protect their data and avoid unauthorized access to it.
- Control who they share their data with, when, and for how long.
- Easily share some of their data with 3rd party software and services anonymously.

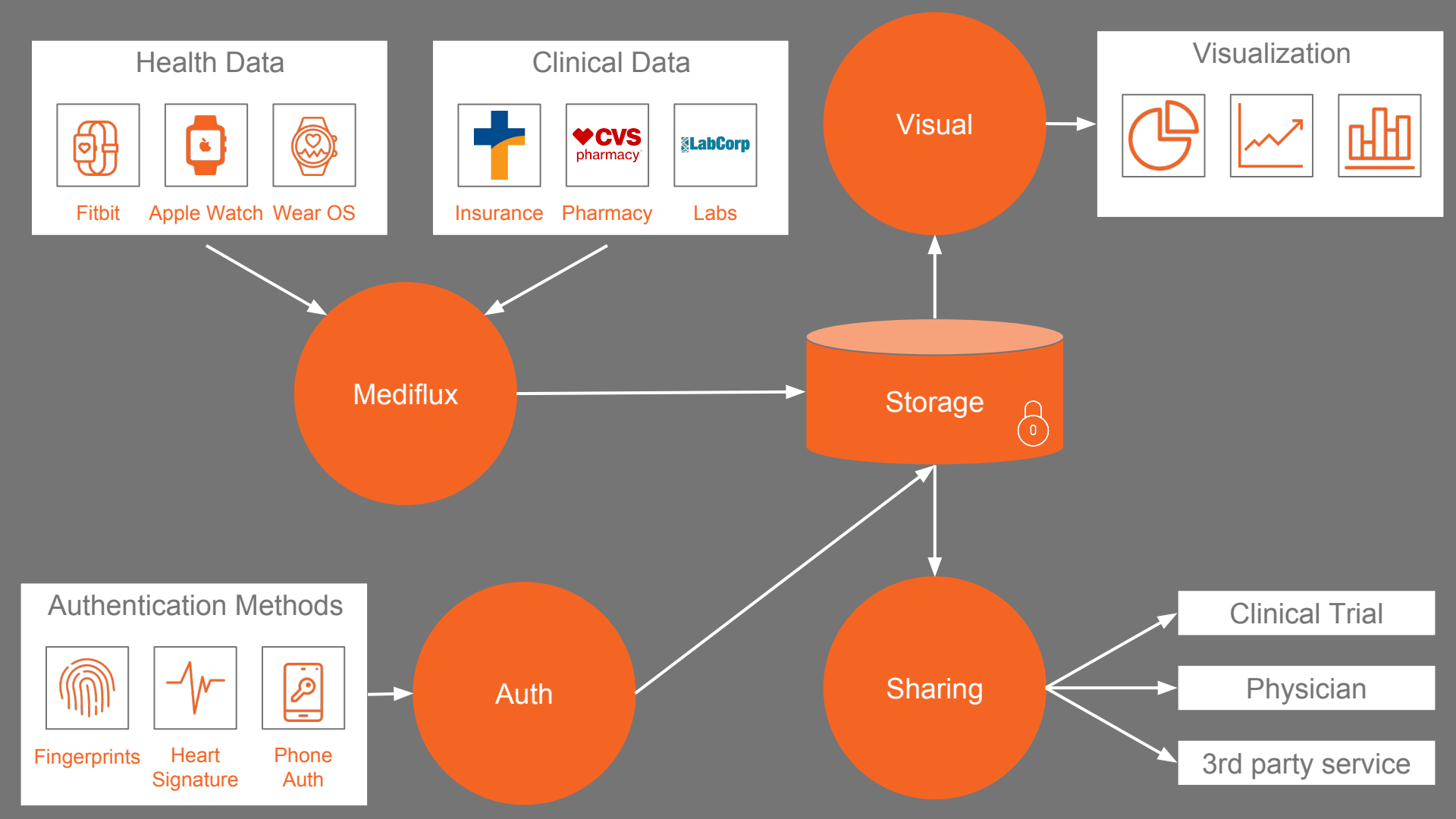
Project Scope

Design and implement a complete open source personal health record solution that can be accessed from a mobile device and allows the user to control access to it . The solution should achieve high security and clinical interoperability that supports patients, caregivers, clinicians, researchers, scientists, and public health organizations. The solution consists of different self-contained modules developers can use inside their own projects separately.

DESIGN

Designing the solution

- This project shall result in a design of a complete solution.
- This project shall be modular and each module shall be independent enough to be customized if needed and used by any other project.
- This project shall inspire to innovate the way health and medical data is stored, accessed, shared, and displayed.
- This project shall allow the user to import their data, keep it private, and share it anonymously.


Health Data
Fitbit
Apple Watch
Wear OS
Clinical Data
Insurance
Pharmacy
Labs
Visual
Visualization
Mediflux
Storage
Authentication Methods
Fingerprints
Heart Signature
Phone Auth
Auth
Sharing
Clinical Trial
Physician
3rd party service

Modules

- **Mediflux**: Uses health and clinical 3rd parties APIs to pull the user data and normalize it.
- **Authentication**: Authenticates the user using a variety of Auth methods to access the database.
- **Storage**: Stores pointers to the data or all the data in a decentralized, normalized, standard storage.
- **Visual**: Mobile and Web visual component to display the data in a simple way to help the user understand it.
- **Sharing**: Controls and manages data sharing.

Walkthrough

A user uses a mobile app to authenticate and access a Personal Medical Record. They can link as many clinical or health data sources to their account. Some data is then permanently stored anonymously in the secure distributed storage. For some data, such as fitness tracker data, a pointer is stored that allows the app to pull the data directly from the source. The user can share part or all the data with several recipient. The sharing can either be anonymous (clinical trial or research) or personal (physician, family). The user can stop or set the sharing to expire automatically.

Mediflux

- Uses 3rd party API/SDKs to import health and medical data from source providers (i.e wearables, medical, labs)
- Normalizes the data from different sources to output a unique interchangeable format.
- Combines the same data from different sources and filters it (i.e. steps data from Apple Watch and Fitbit)
- Authenticates the user with the data source providers and manage the auth tokens.

Storage

- Secure and protected.
- Always accessible.
- Transactions are public but identities are private.
- Storage account should have a dead man’s switch.

Authentication

- Secure authentication methods for mobile apps using biometrics.
- Authentication tokens are managed.

Sharing

- Gives access to selected portions of the storage.
- User can control shared access time.
- User can control shared recipients.
- Sharing access to the storage instead of transmitting data to minimize unauthorized access and accidental loss of data.

Visuals

- A set of mobile and web UI components designed to make it easy for the user to understand their health and medical data.