What is CardinalKit?
Overview of iOS/GCP Framework

Welcome!

https://cardinalkit.org/

Oliver Aalami, MD
aalami@stanford.edu
Ingredients of a Digital Health App

Doctor Dmitri

1. Has idea and wants to test it
2. Has to figure out what platform to use
3. Has to think about what metrics to use, and how to define them
4. Has to develop a spec sheet
5. IRB approval
6. Design clinical study
7. Manage these engineers
8. Hire engineers
9. Get funding
10. Security approval
11. Test software
12. Fix bugs
13. Validation study
14. Do research
Stakeholders

- Researcher
- Developer
- Privacy Officer
- End-User
- University

Risk Management
That’s a tall order!
The road ahead is long and expensive.
The road ahead is long and expensive.

84% of all health apps need 2 years until launch. The average development time is 15 months.

How many months did/will you invest in the development of your last/current mHealth app until launch?
So we built a cable-car.
Introducing

cardinalkit

An Open-Source Platform & Codebase for Digital Health Research and Applications
What is CardinalKit?

- Compliant starting point for mHealth Researcher
  - Save $150,000
  - Save 18 months development time
- leverages existing code to connect critical services
- HealthKit, ResearchKit, Bluetooth Sensor Harness
- Fork & Customize for quick iteration

- Scalable University IT managed back-end
  - Access controls, low maintenance & overhead, BAA
  - Analytics
  - Staging & Production Environment
The **cardinalkit** framework

**Frontend**
- iOS
- ResearchKit
- HealthKit
- Bluetooth
- watchOS
- CoreMotion (sensors)

**Backend**
- Google Cloud
- Cloud Identity
- Cloud Storage
- Google BigQuery
- Firestore

...and more!
Data Pipeline and Architecture

Wearables

Bluetooth pairing

iOS data encryption at rest

Two factor authentication (biometric)

Data sharing permissions

Firebase SDK / HTTPS

Cloud Identity Authentication

Serverless backend

Manage users and groups

Two factor authentication

GCP services (BigQuery, etc.)

SOM managed instance

Custom rules / IAM

Stanford managed

Two factor authentication

Own BAA
The cardinalkit framework is just PART of the HIPAA equation.

The 7 Elements of HIPAA Compliance

1. Implementing written policies, procedures, and standards of conduct.
2. Designating a compliance officer and compliance committee.
3. Conducting effective training and education.
4. Developing effective lines of communication.
5. Conducting internal monitoring and auditing.
7. Responding promptly to detected offenses and undertaking corrective action.

Ref: https://compliancy-group.com/what-is-hipaa-compliance/

More info about Google Cloud and HIPAA Compliance can be found here:
https://cloud.google.com/security/compliance/hipaa
# Shared Responsibility Matrix

<table>
<thead>
<tr>
<th></th>
<th>Server</th>
<th>Mobile App</th>
<th>Patient</th>
<th>Team</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Rule</strong></td>
<td>Data Encryption at rest</td>
<td>Data Encryption at rest / in flight</td>
<td></td>
<td>BAA</td>
</tr>
<tr>
<td></td>
<td>Data center / infrastructure / operations security standards - annual security audits</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Privacy Rule</strong></td>
<td>2-factor authentication</td>
<td>Data Access Permissions</td>
<td>Obtain consent to collect and share data</td>
<td>Access Controls</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Breach Notification Rule</strong></td>
<td>Breach Notification</td>
<td></td>
<td></td>
<td>Breach Notification</td>
</tr>
</tbody>
</table>

CardinalKit

Developer
# Shared Responsibility Matrix

<table>
<thead>
<tr>
<th>Security Rule</th>
<th>Server</th>
<th>Mobile App</th>
<th>Web App</th>
<th>Patient</th>
<th>Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Encryption at rest</td>
<td>Data Encryption at rest</td>
<td>Encryption</td>
<td>BAA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data center / infrastructure / operations security standards - annual security audits</td>
<td>BAA training</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy Rule</td>
<td>2-factor authentication</td>
<td>Data Access Permissions</td>
<td>2-factor auth</td>
<td>Obtain consent to collect and share data</td>
<td>Access Controls</td>
</tr>
<tr>
<td>Breach Notification Rule</td>
<td>Breach Notification</td>
<td></td>
<td></td>
<td></td>
<td>Breach Notification</td>
</tr>
</tbody>
</table>

CardinalKit  Developer  University IT
@ Stanford
Partner with University Research IT

https://med.stanford.edu/mhealth.html
Stanford Medicine mHealth platform

A powerful, and capable HIPAA-compliant platform for mobile studies

The mHealth Platform is a set of HIPAA-compliant services operated and maintained by Research IT to provide a secure place for mobile applications to store data and perform tasks that cannot be accomplished directly on a device.

Two different architectures are supported. The original platform supports BridgeSDK based client mobile apps and a newer platform supports Firebase SDK based apps.

The first version of the mHealth Platform (v1) provides services for mobile applications to handle participant sign up, email verification, consent, and participation status. It also provides services for getting sensor and participant data off the device and into our environment. Data can be accessed via dashboards or downloaded via researcher APIs. The mHealth Platform has been used in support of large-scale population health studies such as MyHeartCounts, and targeted research studies such as STREAM (Studying TRiggers in Everyday Activity for Migraine).

The next generation of the mHealth Platform (v2), adds support for Google’s Firestore database via the Firebase SDK, and related services such as identity management.

Co-created with our community

Research IT has collaborated with the Stanford Byers Center for BioDesign to ensure the new Open Source mobile development framework CardinalKit is pre-integrated with the mHealth v2 Platform to make it easier, faster, and cheaper than ever to build new mobile applications for research.

https://med.stanford.edu/mhealth.html
Recap

Saves you 18 months of design and development
Saves you $150,000 in development cost

What you get:
● Basic Application to start with
● 2FA Authentication
● Modern and scalable architecture
● Secure GCP schema
● Data pipeline and integrity (heart rate, steps, activity etc.)
● Informed Consent
● HIPAA - ready (compliance involves more than code)
● Community of mHealth developers
● Native HealthKit, CareKit integration
● Open mHealth mobile/wearable data interoperability
● FHIR data store
Thank You!

Contact Info:
Oliver Aalami, MD
aalami@stanford.edu
Data Pipeline and Architecture

Mobile App

- Accelerometer
- Gravity
- Rotation
- Steps
- Heart Rate
- Flights Climbed
- Distance Walked
- Activity Classifications
- Exercise Completion Data

AdCol
- Rotation
- Gravity
- Steps
- Heart Rate
- Distance Walked
- Activity Classifications
- Exercise Completion Data

Images
- Video
- Apple Health Records
- HealthStore
- Survey Data
- Active Task Data
- Location Data
- Consent
- Name/Phone/Email

FireStore SDK + Google Identity SDK

Active Tasks
- Messages
- Notifications
- Surveys

Google Cloud
- Firestore Cloud Functions (consent server)
- Google Identity
- Google BigTable
- Google PubSub
- Google Cloud AutoML

Management Dashboard

ETL

SOM Network / Research IT Managed - "mHealth Platform"

ETL

- Jupiter on Google Cloud / Kubernetes
- NERO on Google Cloud / Kubernetes
- Google Cloud AutoML

RIT Managed IAM/Access Layer

Stanford Researcher
Data Pipeline and Architecture

StrokeCoach Data Flow

PHI FREE ZONE

HIPAA ZONE

Stanford Hospital / Stanford Stroke Clinic

User ID : Patient Name

Stanford Box (HIPAA Compliant)
ISO & SOC Compliant for Privacy and Security
(see more: https://firebase.google.com/support/privacy)