Backend & DB

Specification

Table of Contents

[Product Brief 2](#_Toc3543829)

[Specific Requirements 4](#_Toc3543830)

# Product Brief

The general architecture of the app looks as follows:

RW

**Backend**

- Endpoints  
- Authn/Authz  
- E2e Encryption  
- Logging  
- Auditing

**DB**

- Encryption  
- Auditing

*Everything is trackable over time*

Web app   
(React+Redux)

RW

iPhone

RW

Android  
phone

WO

**Devices**   
(smart scales, wearables, etc.)

The main components are:

* **Apps**
  + Web app (written in ReactJS+Redux)
  + Native mobile apps (Android/Java and iOS/Swift) as front ends.
  + The apps have a **RW (read-write)** relationship with the backend
* **Devices**
  + Smart devices emitting data to the backend
  + Devices have **WO (write only)** relationship with the backend. They emit (a lot of) data that is streamed to and recorded in the backend.
* **Backend**
  + The backend consists of a C# layer (business logic + db access) and DB
  + The C# layer exposes endpoints that can be accessed by the apps and by the devices.
  + All data exchange with the backend is encrypted.
  + Data is stored encrypted in the database too, all all times
  + All data access is audited. This is important and enables GDPR compliance.

# Specific Requirements

1. Everything is a trackable over time
   1. The obvious things 🡪 weight, height, etc.
   2. The non-obvious things 🡪 started smoking, stopped smoking, had a sex change, started a therapy, had an immunization, etc.
2. Everything is plottable over time
   1. We plan on having charts for everything.
3. The backend should be able to ingest large amounts of data
   1. For example, if I connect my Apple Watch to the system, I may be getting heart rate data. I may be getting 1000s of incoming measurements per hour per user.
4. The backend should be able to generate aggregate data for large populations, in near real-time, on demand.
   1. For example, I may want to show the average BMI of all Caucasian males between the age of 40-49 superimposed on top of my BMI (to compare myself with others)
5. All PII (personally identifiable information) data must be encrypted, and all data access must be encrypted.
6. All data access is audited:
   1. We will have a write only table where we store information about all data access (when, who, what)
7. See additional requirements for HIPAA and GDPR compliance
   1. This is very important and must be taken into account as we design the backend
   2. Right to be forgotten, etc.
8. Redundancy and alarms
   1. We have alarms configured to allow us to monitor the health of the backend
   2. We have full data redundancy