Privacy-preserving Based Access Control for Health Information Network

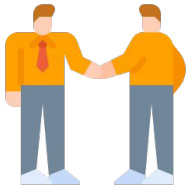
2020 Senior Project Proposal

Chidchanok B. 6088012
Ariza D. 6088037
Jiraput T. 6088198

Advisor : Dr. Ittipon Rassameeroj
Co Advisor : Lect. Pagaporn Pengsart

มหาวิทยาลัยมหิดล
คณะเทคโนโลยีสารสนเทศ
และการสื่อสาร

Agenda



01

INTRODUCTION

02

OBJECTIVES

03

BACKGROUNDS

04

SYSTEM DESIGN
IMPLEMENTATION

05

LIMITATIONS

01

Introduction

Problem Statement

- It is difficult for patients to access their medical information.
- Medical information has been treated poorly.
- Transferring data between hospitals is difficult.

HOSPITAL A

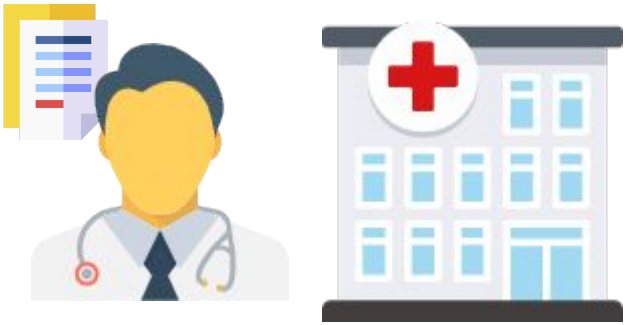
HOSPITAL B

HOSPITAL A

HOSPITAL B

HOSPITAL A

? HOSPITAL B



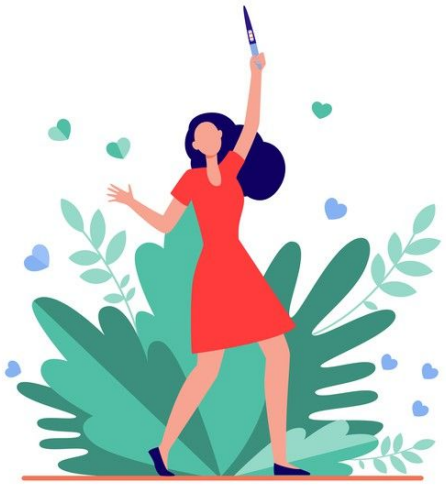
02
Objective

Objectives

1. To help patients gain the access to their medical information
2. To allow patients to give permission to medical staff before accessing their medical information.
3. To ensure the privacy of the patient's medical information

Expected Benefits

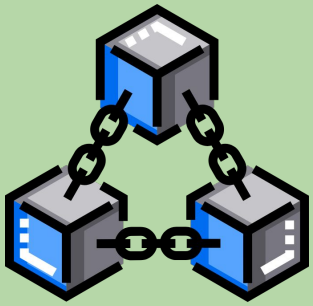
1) Enhance the privacy and security of the patient's data.
2) Patients can share information with specific medical staffs.
3) Provide accurate, up-to-date, complete patient's data.
4) Provide quick access to their medical record.
5) Minimize or no change at all to the existing hospital systems.



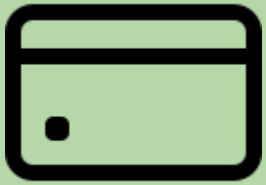
03
Backgrounds

Literature Review

“Privacy and Security”



BLOCKCHAIN

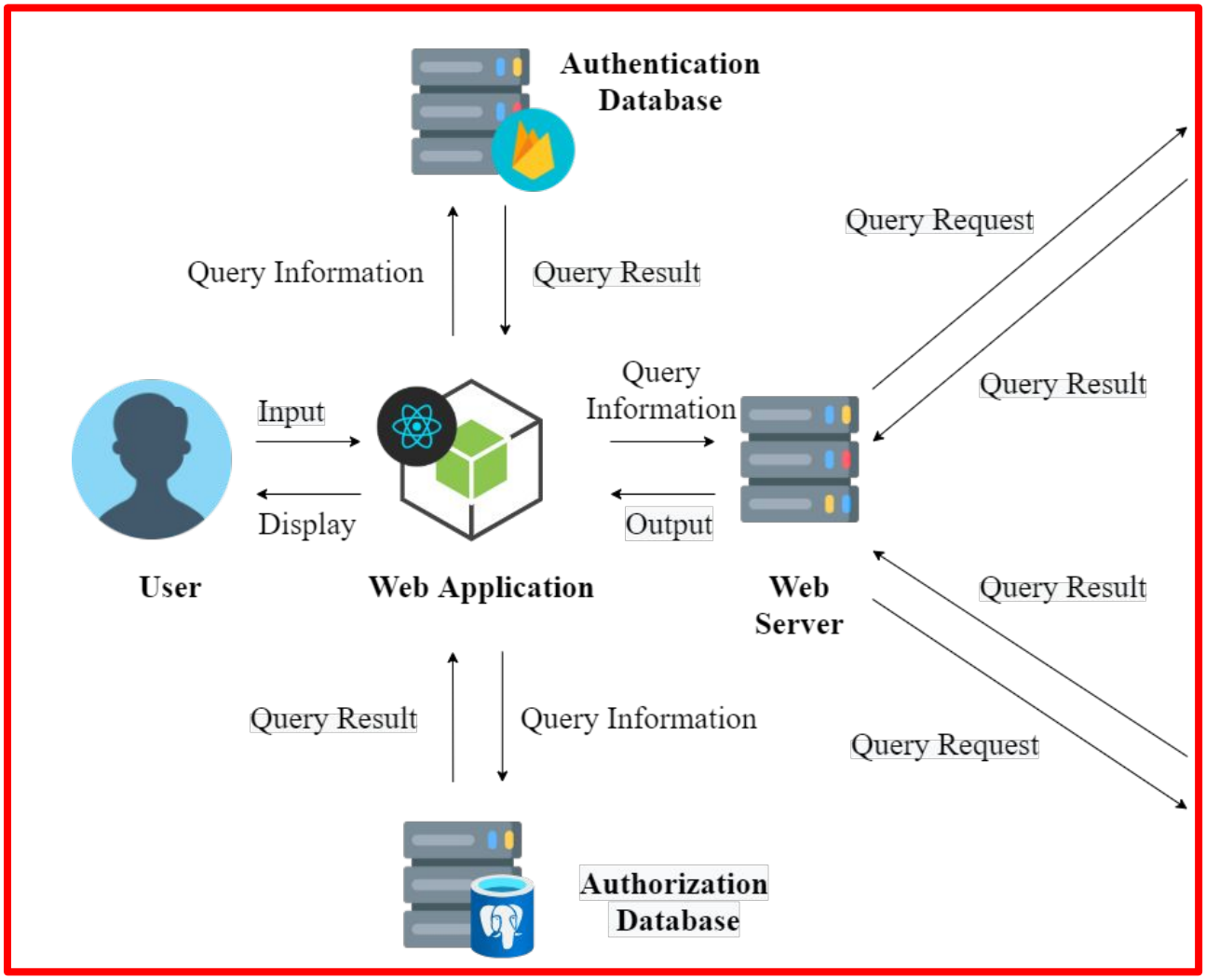


SMART CARD

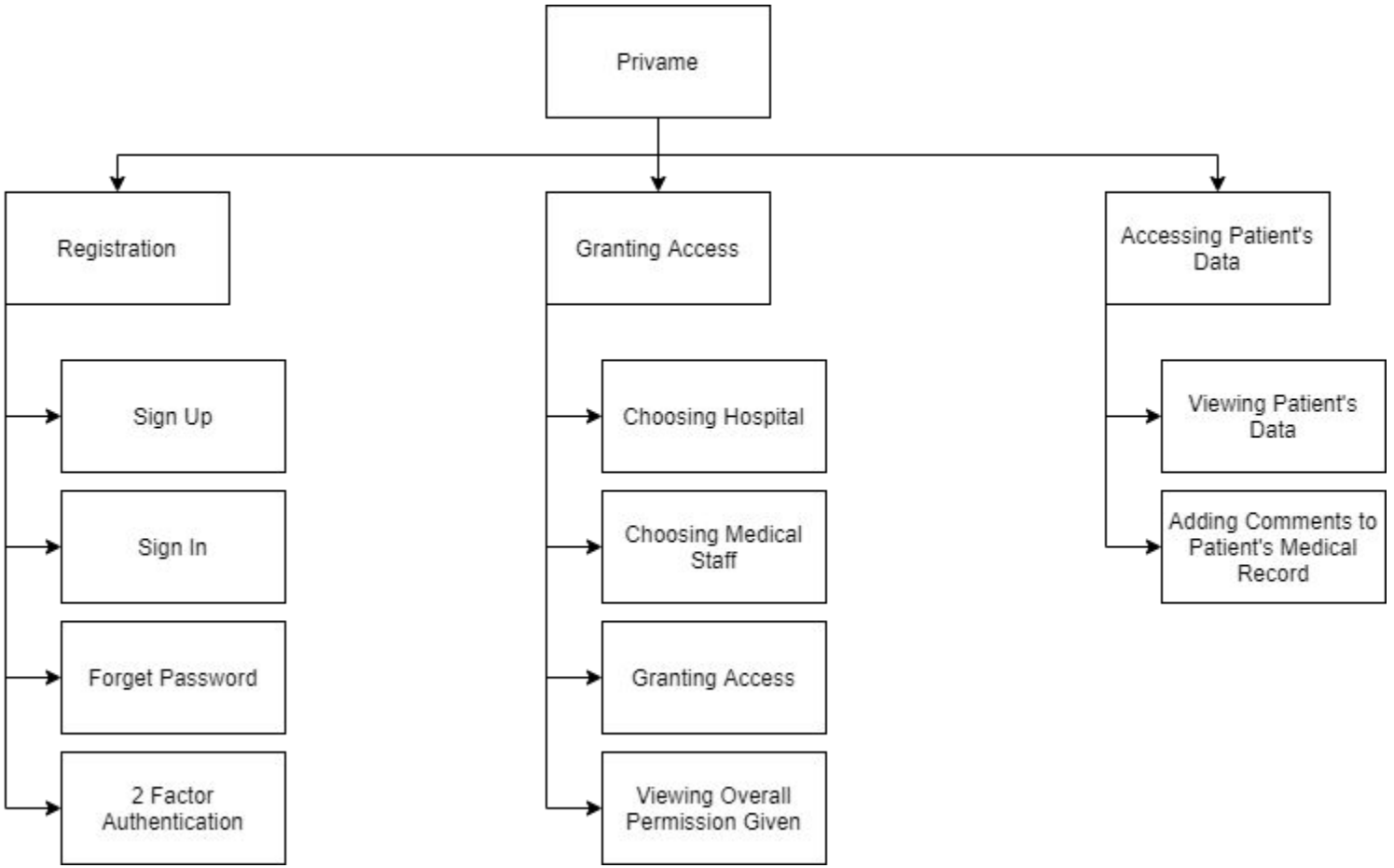
04

System Design & Implementation

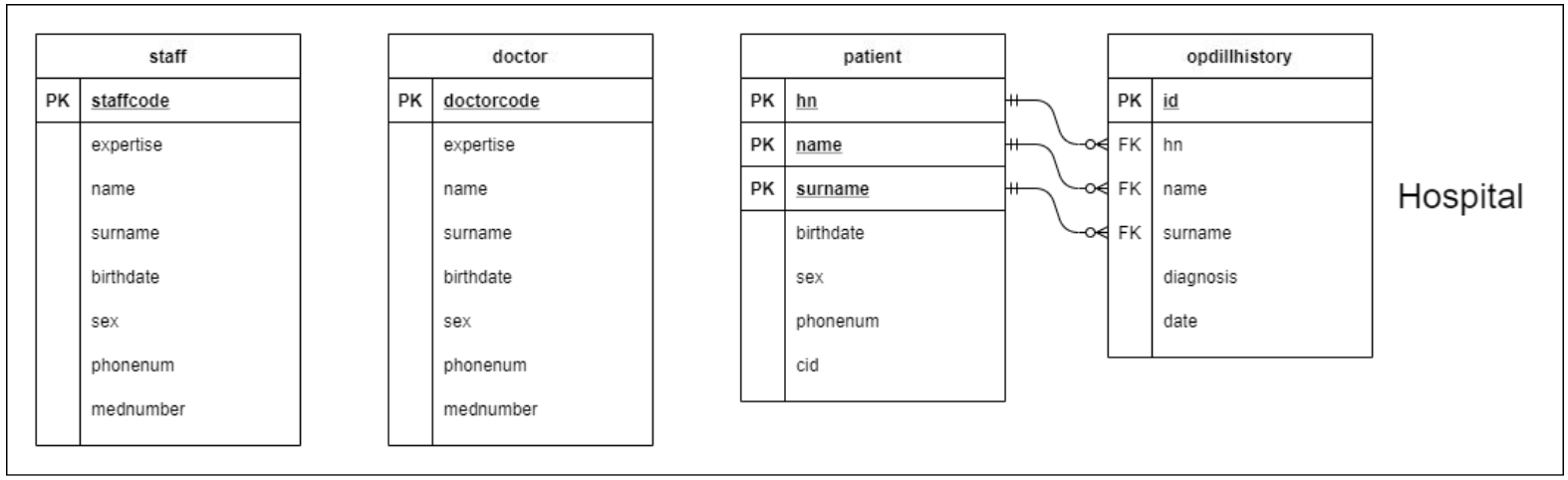
System Architecture Overview

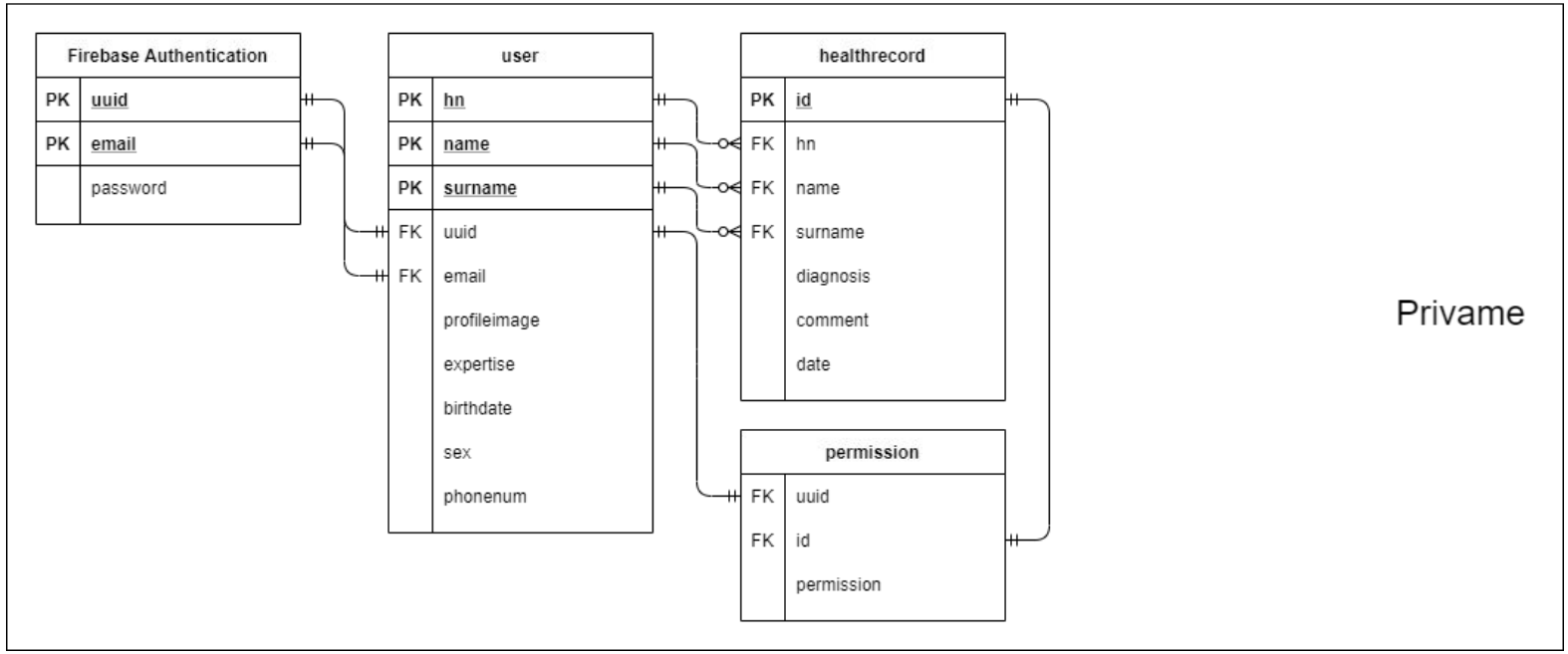


System Structure Chart

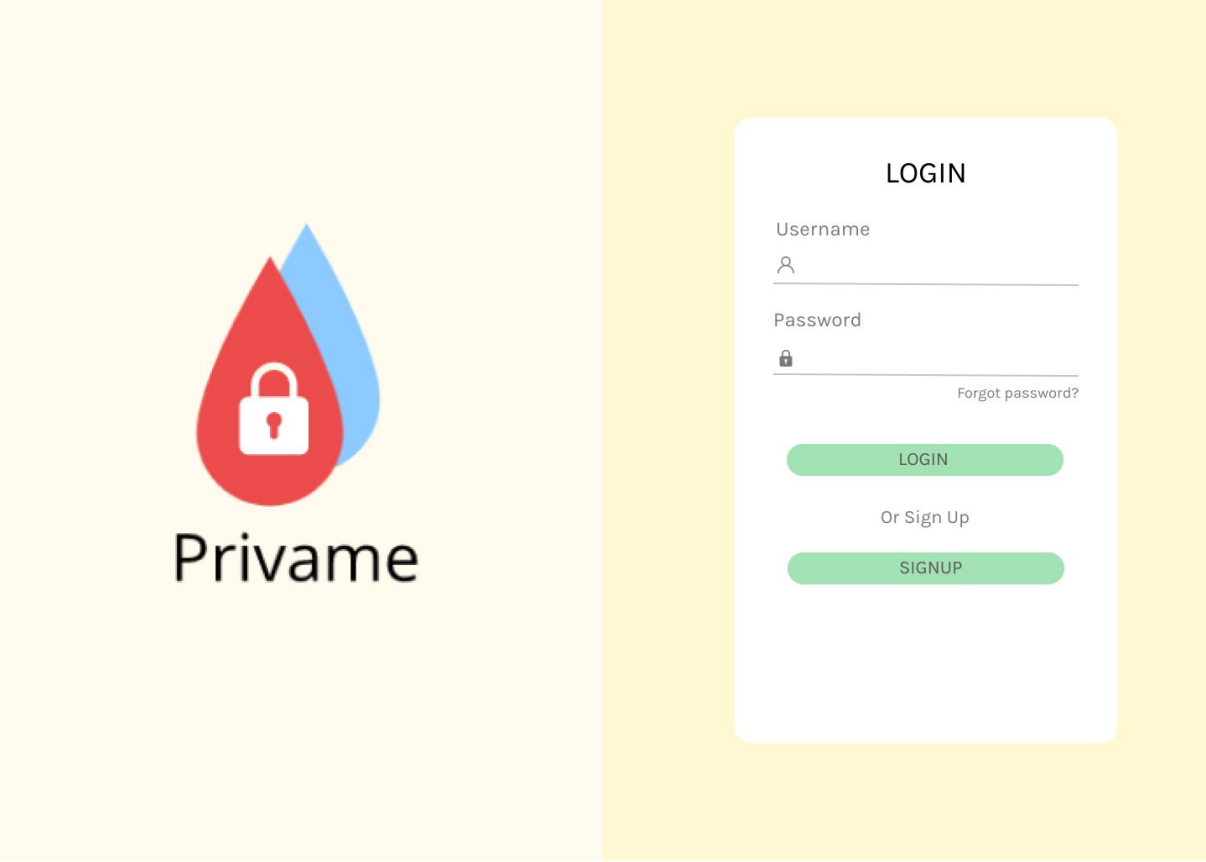


ER Diagram


staff
PK staffcode
expertise
name
surname
birthdate
sex
phonenum
mednumber
doctor
PK doctorcode
expertise
name
surname
birthdate
sex
phonenum
mednumber
patient
PK hn
PK name
PK surname
birthdate
sex
phonenum
cid
opdillhistory
PK id
FK hn
FK name
FK surname
diagnosis
date
Hospital

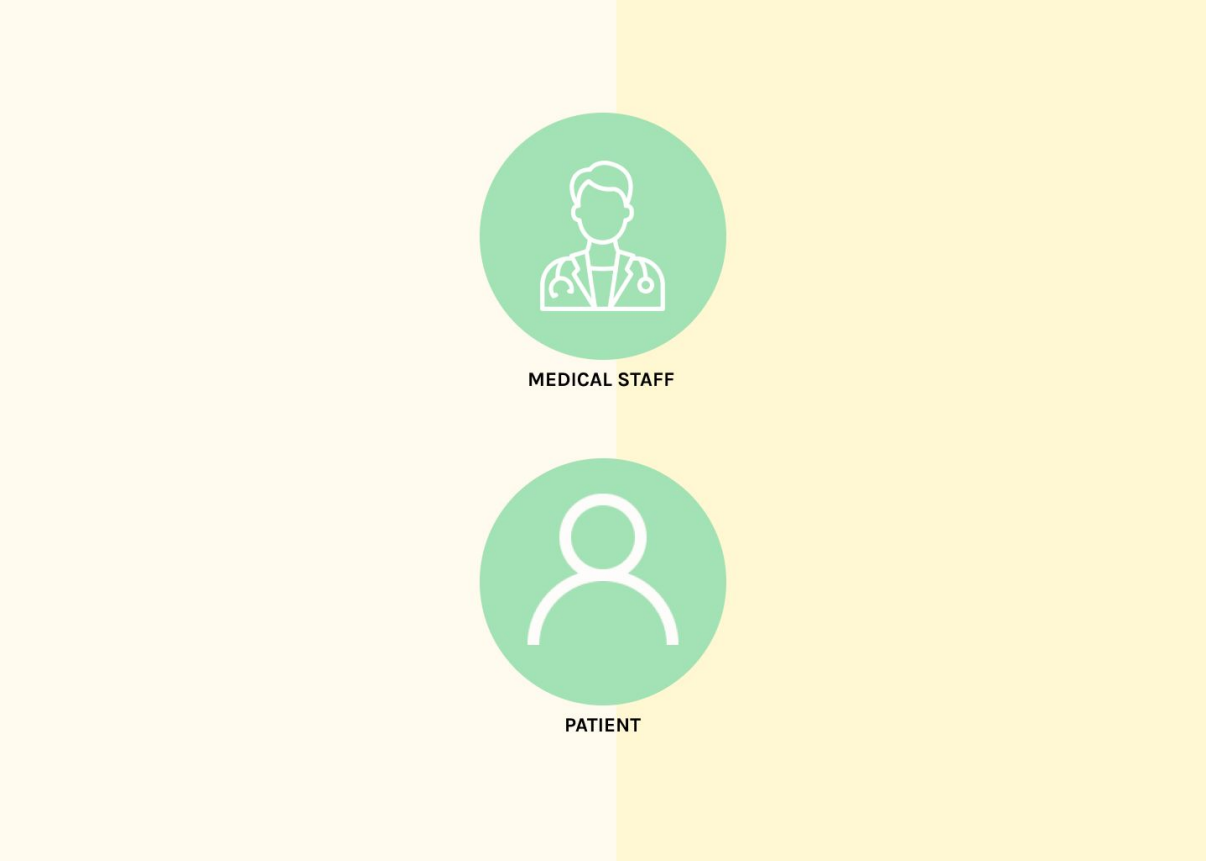

Firebase Authentication
PK uuid
PK email
password
user
PK hn
PK name
PK surname
FK uuid
FK email
profileimage
expertise
birthdate
sex
phonenum
healthrecord
PK id
FK hn
FK name
FK surname
diagnosis
comment
date
permission
FK uuid
FK id
permission
Privame

Prototype



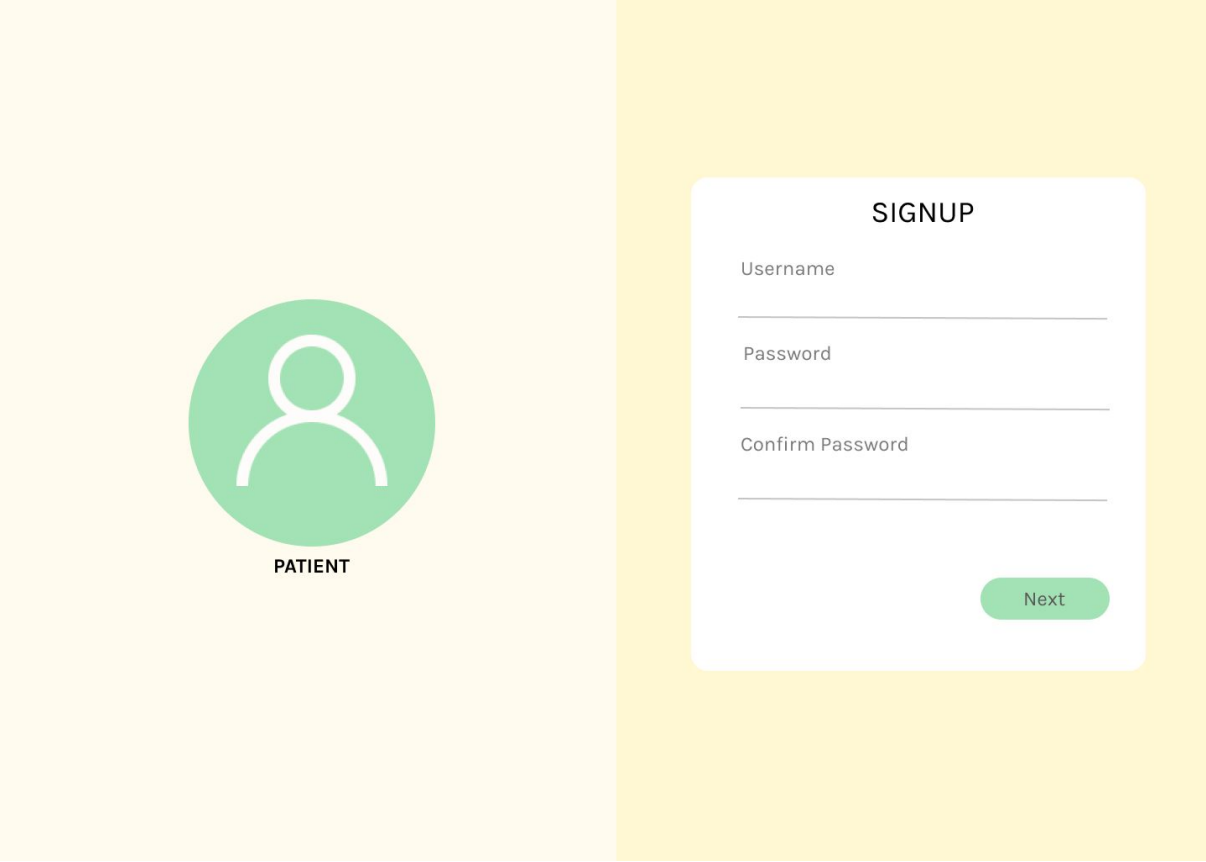
Login Page

Prototype



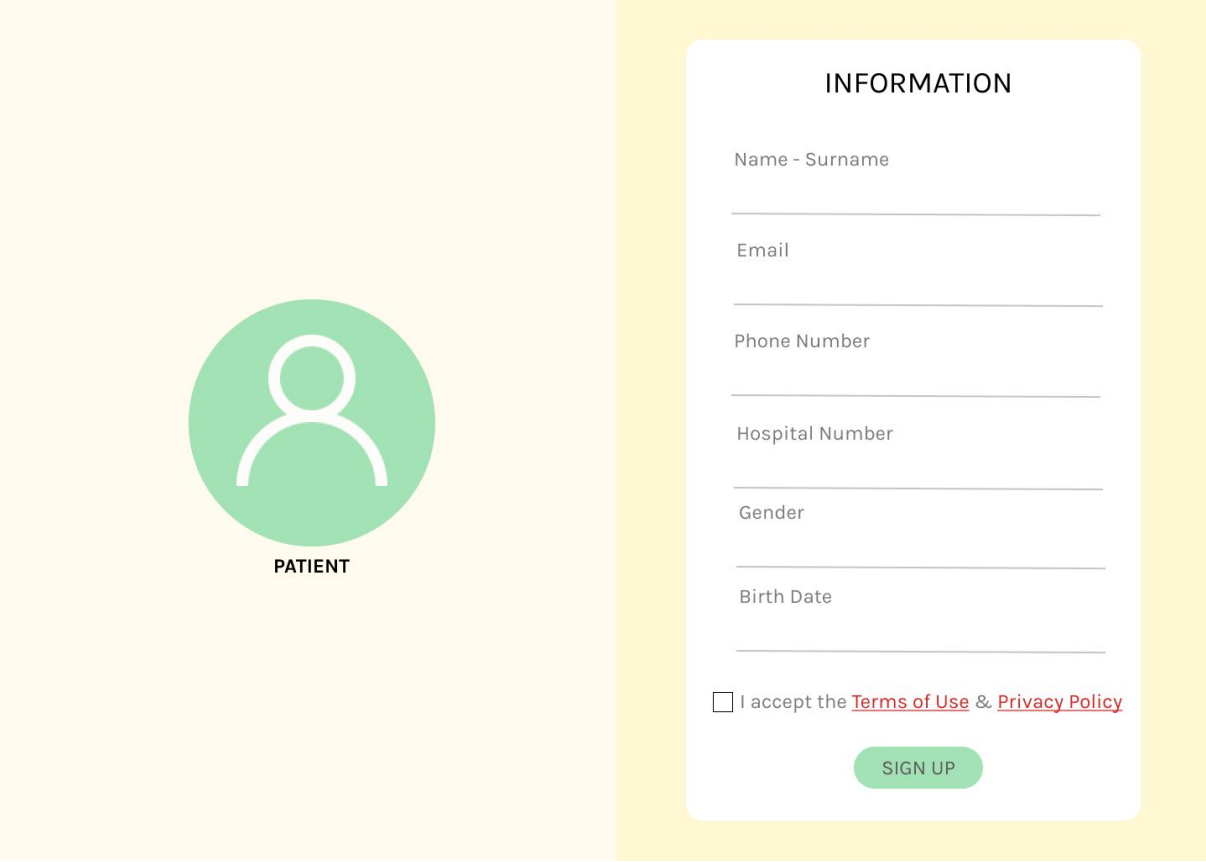
Choosing Role

Prototype



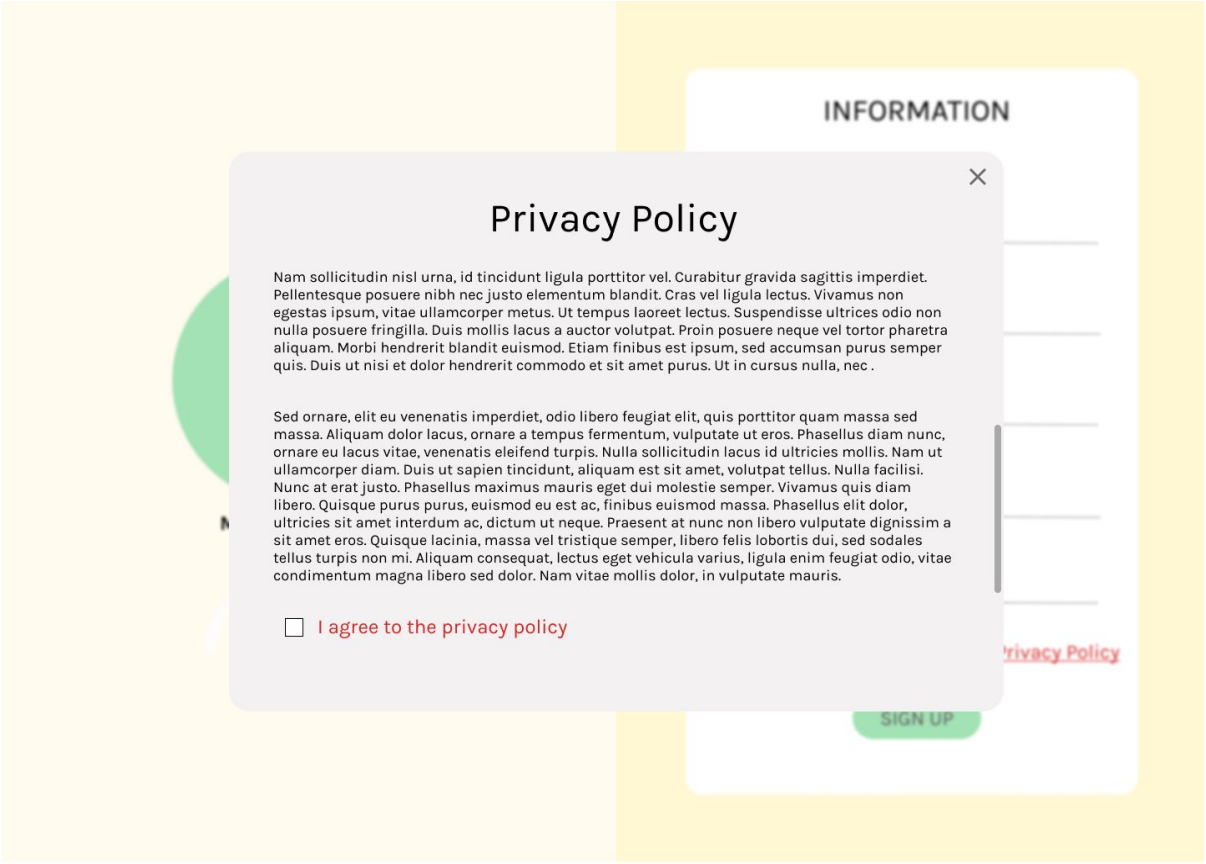
Sign Up

Prototype



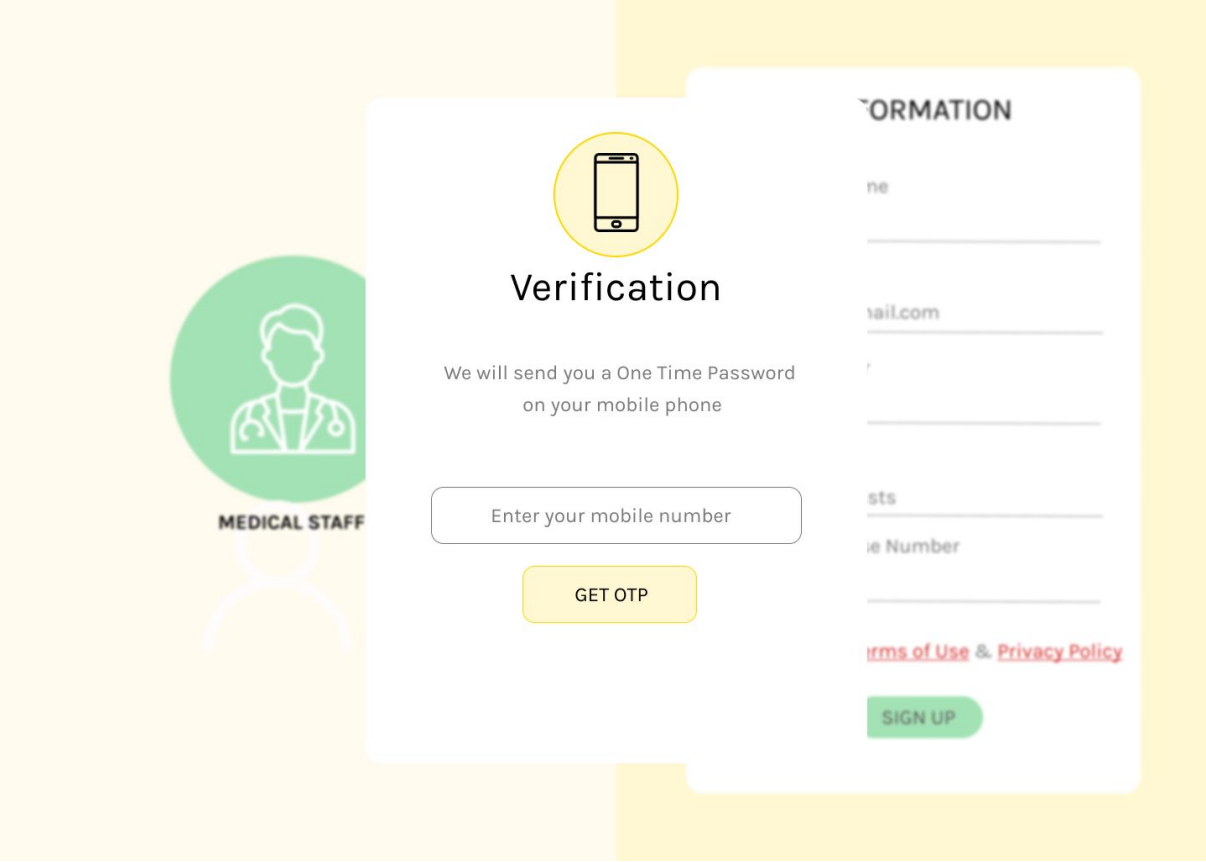
Add Information for Sign Up

Prototype



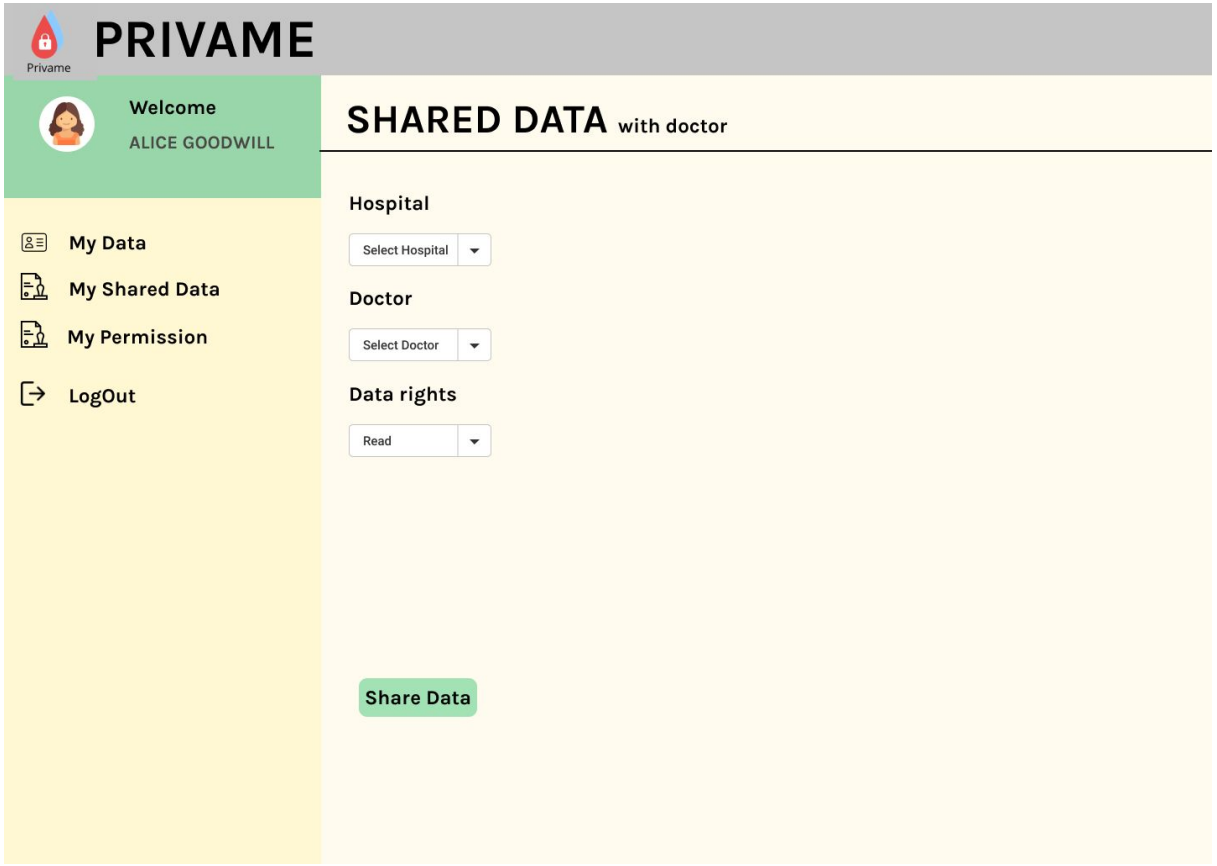
Privacy Policy

Prototype



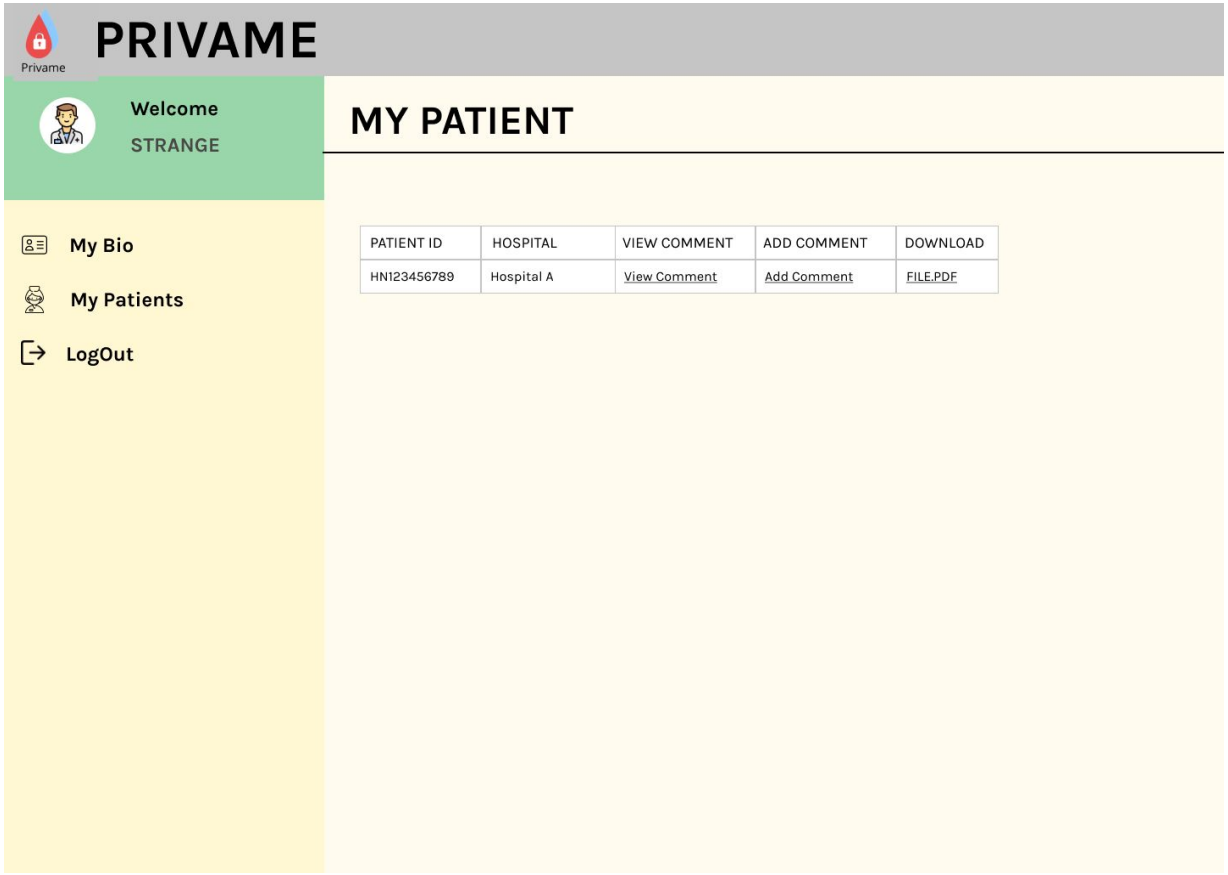
SMS Verification

Prototype (Patient)



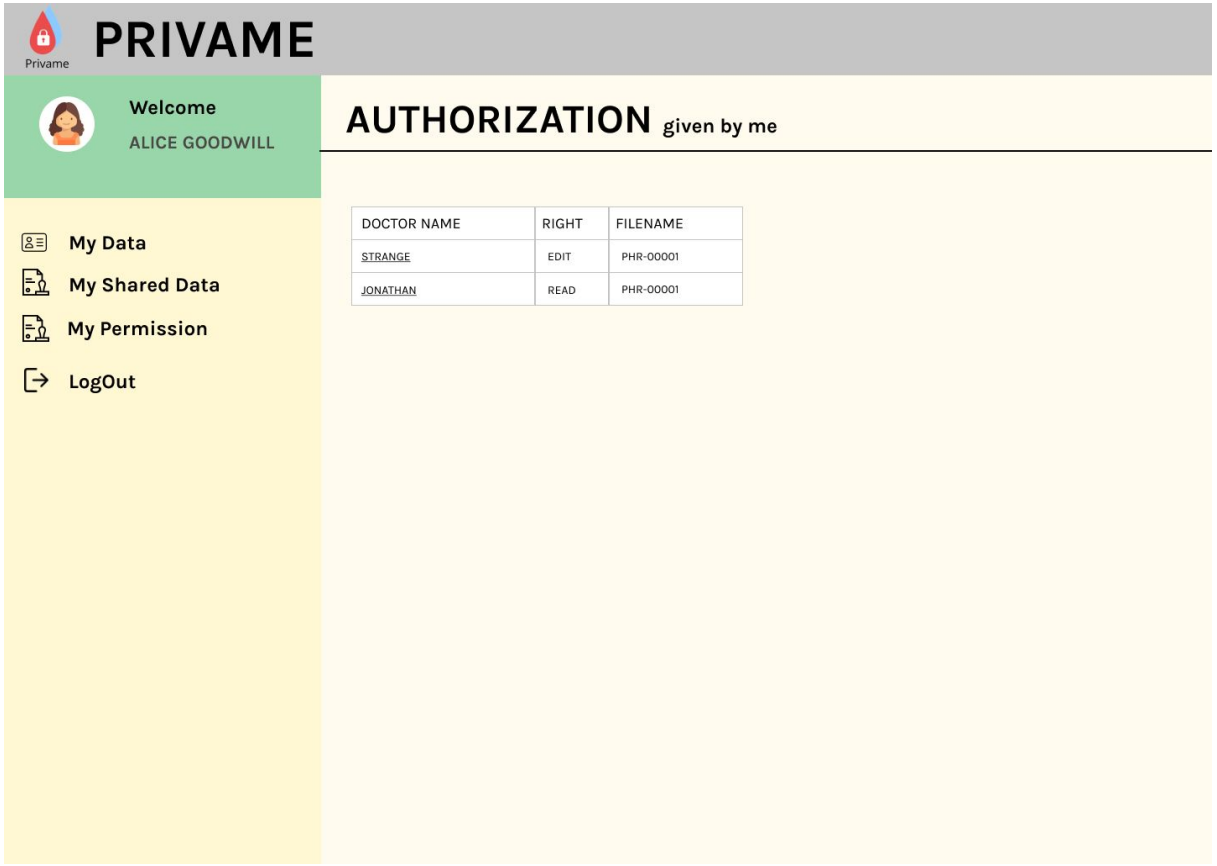
Access Granting Page

Prototype (Medical Staff)



Permission Received from the Patient

Prototype (Patient)



Permission Summary

05

Limitation

Limitations

1) The application only shows the hospital that collaborate with our project
2) The medical records in this project only cover basic health information
3) This application only supports the hospital that keep the medical record in form of SQL.

References

https://www.scb.co.th/th/personal-banking/stories/tips-for-you/pdpa-about-us.html

https://nodejs.org/en/knowledge/HTTP/servers/how-to-create-a-HTTPS-server/

https://severalnines.com/database-blog/scaling-postgresql-large-amounts-data

https://www.imperva.com/learn/data-security/anonymization

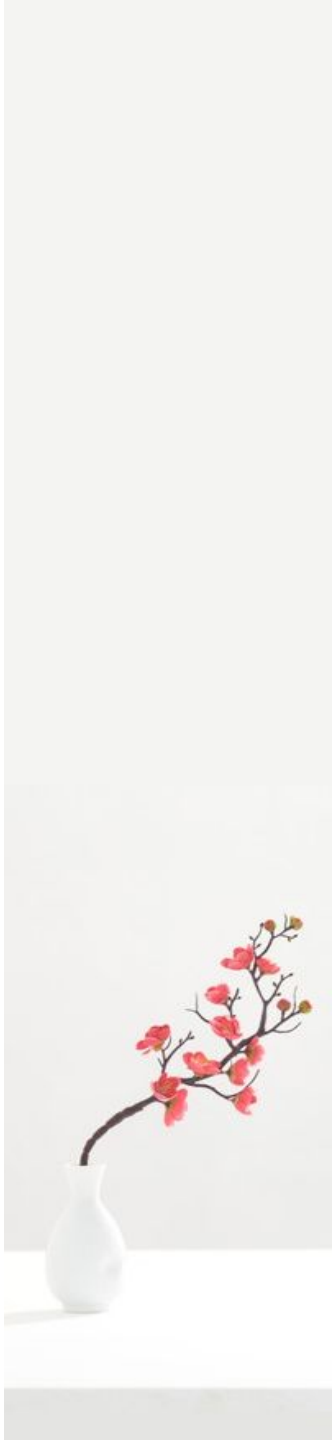
https://github.com/fireship-io/multifactor-auth-firebase

https://www.npmjs.com/package/data-anonymizer

https://firebase.google.com/support/privacy

https://owasp.org/www-project-api-security

https://www.gov.uk/data-protection



Thank You

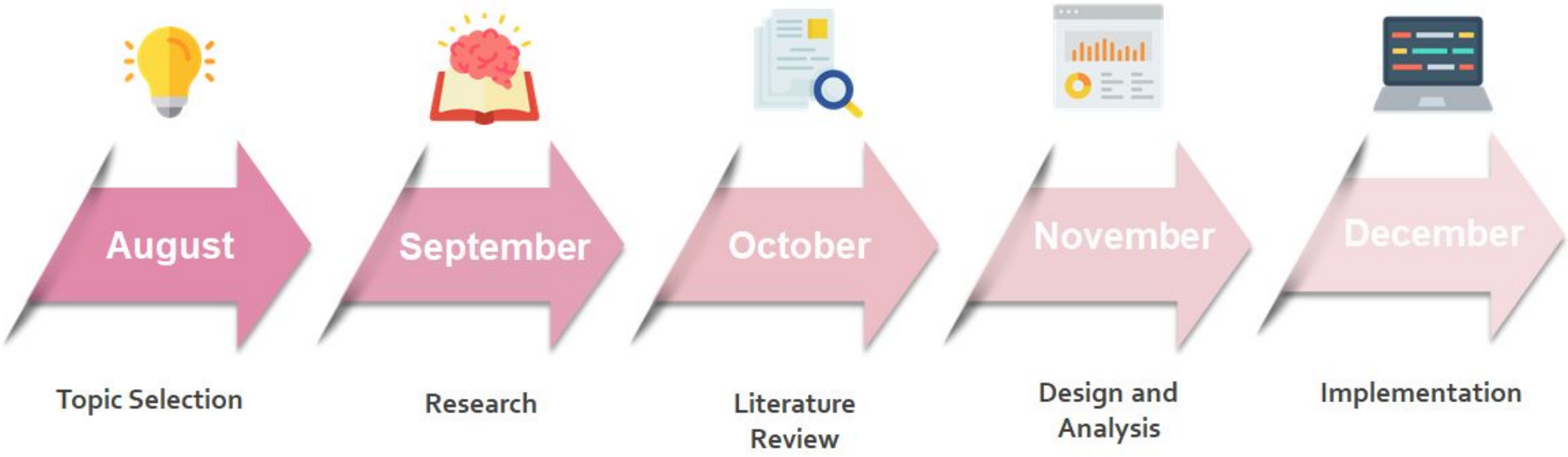
Q & A

Additional Resources

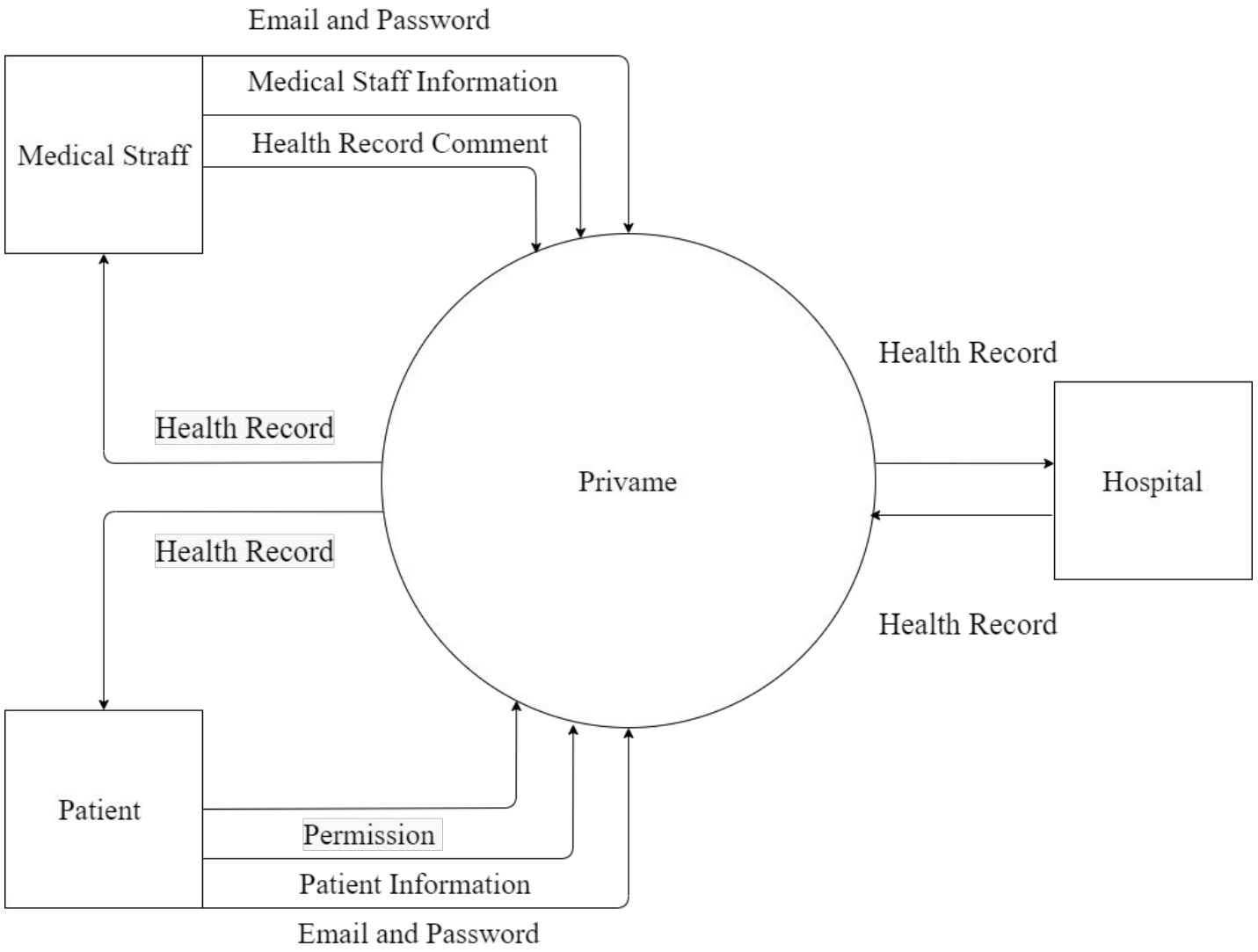
Protocols

	OpenID Connect	OAuth 2.0	SAML 2.0
Purpose	Authentication	Authorization	Authentication, Authorization, and SSO
Sending Format	JSON	JSON	XML

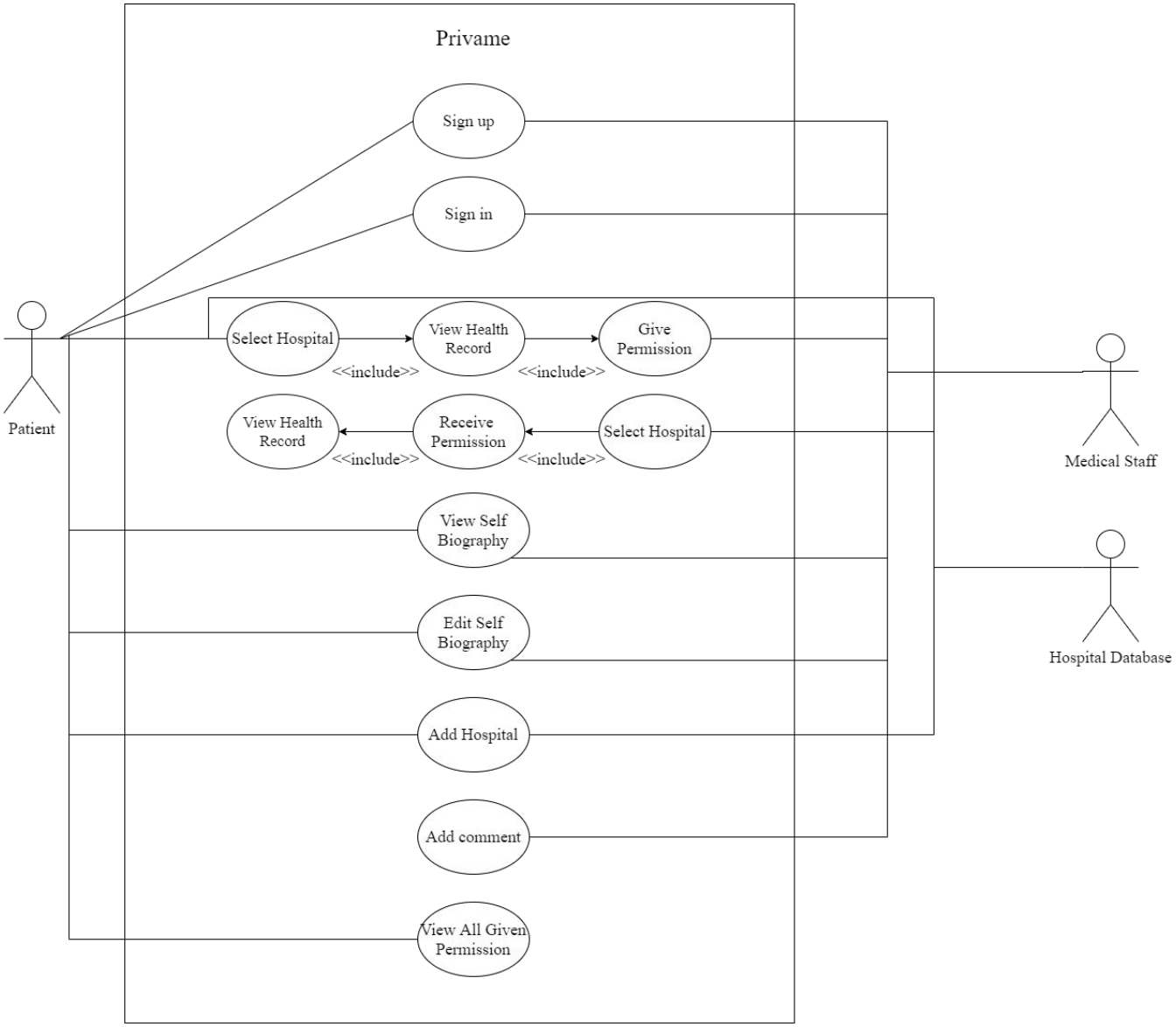
Timeline


August
Topic Selection
September
Research
October
Literature Review
November
Design and Analysis
December
Implementation

Data Flow Diagram

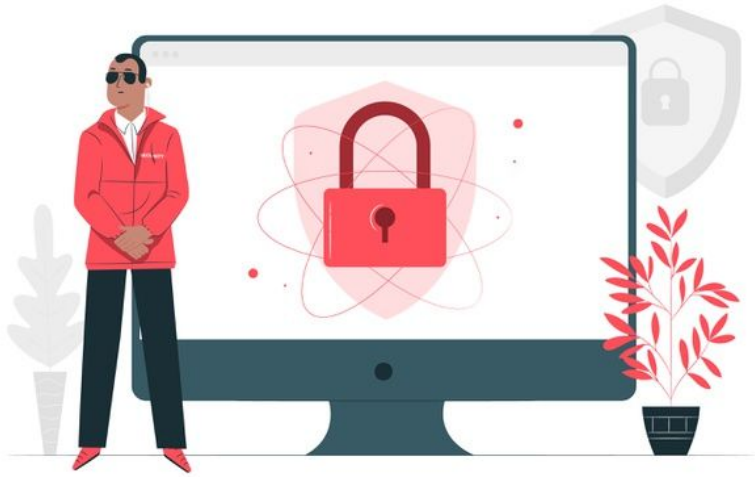


Use Cases Diagram



Personal Data Protection Act (PDPA)

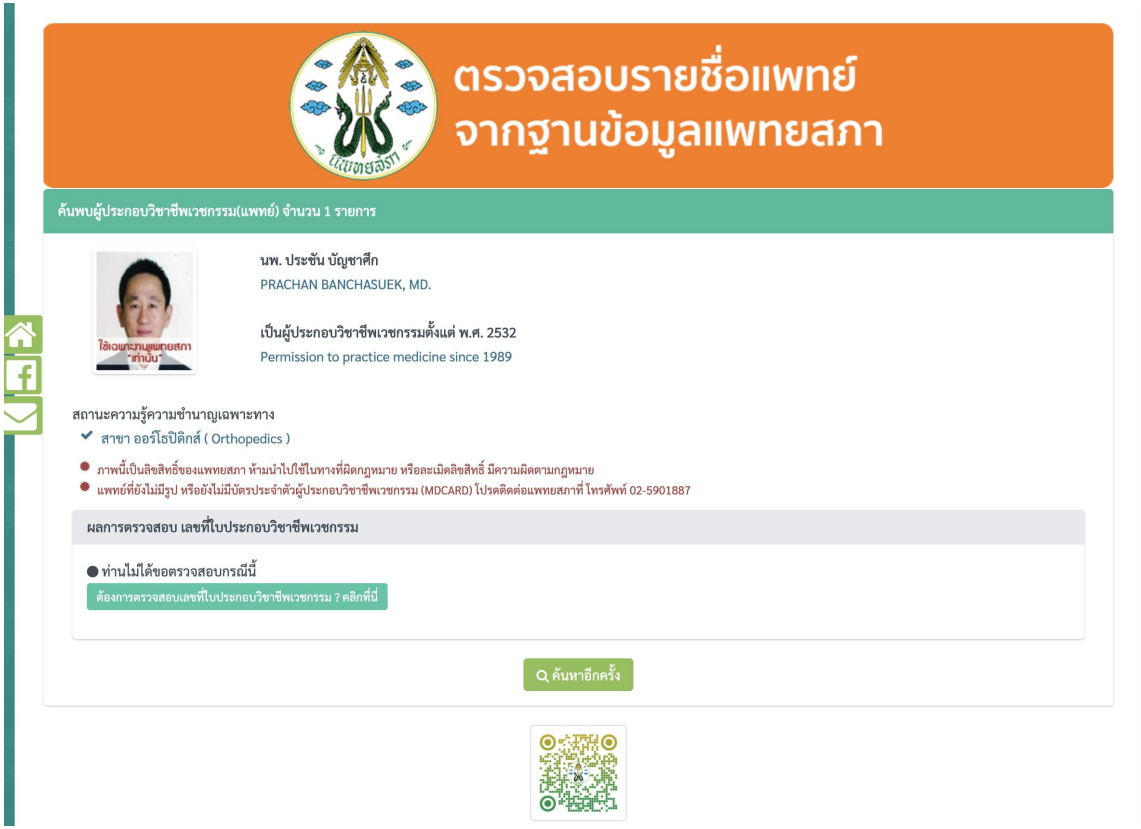
1. Right to be Informed
2. Right to Access
3. Right to Data Portability
4. Right to Object
5. Right to Erasure (Right to be Forgotten)
6. Right to Restrict Processing
7. Right to Rectification



General Data Protection Regulation (GDPR)

1. Be informed about how your data is being used
2. Access personal data
3. Have incorrect data updated
4. Gave data erased
5. Stop or restrict the processing of your data
6. Data portability (allowing you to get and reuse your data for different services)
7. Object to how your data is processed in certain circumstances

Personal Information References



Is Firebase Secure ?

Data protection

Firebase support for GDPR and CCPA

On May 25th, 2018, the EU General Data Protection Regulation (GDPR) replaced the 1995 EU Data Protection Directive. On January 1, 2020, the California Consumer Privacy Act (CCPA) took effect. Google is committed to helping our customers succeed under these privacy regulations, whether they are large software companies or independent developers.

The GDPR imposes obligations on data controllers and data processors, and the CCPA imposes obligations on businesses and their service providers. Firebase customers typically act as the "data controller" (GDPR) or "business" (CCPA) for any personal data or information about their end-users they provide to Google in connection with their use of Firebase, and Google generally operates as a "data processor" (GDPR) or "service provider" (CCPA).

This means that data is under the customer's control. Customers are responsible for obligations like fulfilling an individual's rights with respect to their personal data or information.

ISO and SOC compliance

All Firebase services (aside from App Distribution and Crashlytics) have successfully completed the ISO 27001 and SOC 1, SOC 2, and SOC 3 evaluation process, and some have also completed the ISO 27017 and ISO 27018 certification process:

Service name	ISO 27001	ISO 27017	ISO 27018	SOC 1	SOC 2	SOC 3
Cloud Firestore	✓	✓	✓	✓	✓	✓
Cloud Functions for Firebase	✓	✓	✓	✓	✓	✓
Cloud Storage for Firebase	✓	✓	✓	✓	✓	✓
Firebase A/B Testing	✓			✓	✓	✓
Firebase App Distribution					✓	
Firebase Authentication	✓	✓	✓	✓	✓	✓
Firebase Cloud Messaging	✓			✓	✓	✓
Firebase Crashlytics					✓	
Firebase Dynamic Links	✓			✓	✓	✓
Firebase Hosting	✓			✓	✓	✓

Scalability of Firebase Authentication

Account creation and deletion limits

Operation	Limit
New account creation	100 accounts/IP address/hour
Account deletion	10 accounts/second

★ **Note:** You can schedule a temporary increase to the account creation limit in the Firebase console

Accounts per project

Account type	Limit
Anonymous user accounts	100 million
Registered user accounts	Unlimited

Two-Factor Authentication

README.md

Multifactor Auth with Firebase

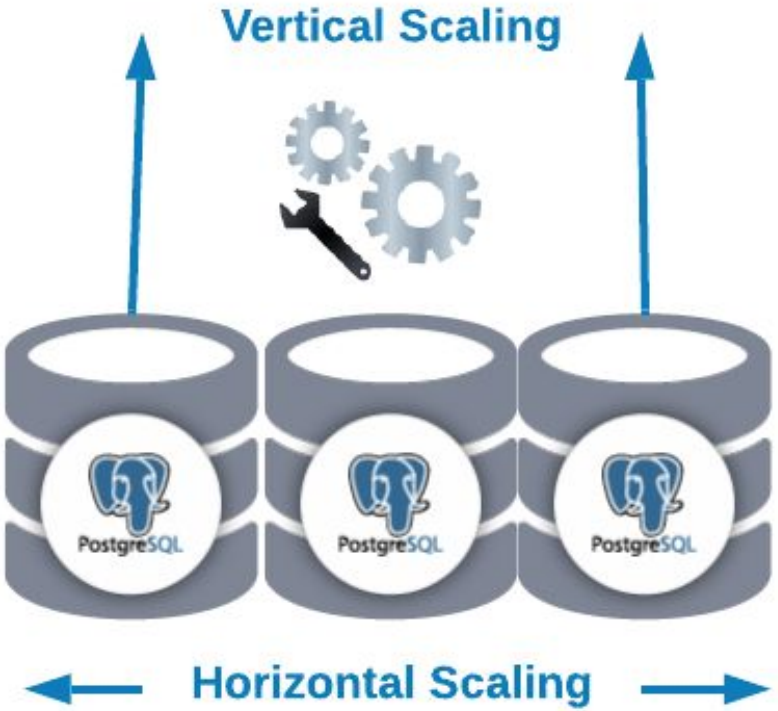
Watch the full Firebase 2FA Tutorial on Fireship.

Usage

Clone this repo. Update your Firebase config in `main.js`. Enable Identity Platform via the GCP console.

```
npm install
npm start
```

Scalability of Web Application



PostgreSQL

Why Is PostgreSQL So Popular?

PostgreSQL's popularity is still growing. Just look at the 2019 Stack Overflow Survey – one of the most important technology rankings in the world. Stack Overflow's surveyors collect the votes of actual programmers and developers. Among systems used by profession
MongoDB,
on the list (

Security

PostgreSQL ใช้ SSL ในการเชื่อมต่อกับ client/server นอกจากนั้นยังมีการเพิ่มประสิทธิภาพความปลอดภัยในตัวเรียกว่า SE-PostgreSQL ซึ่งเป็นการควบคุมการเข้าถึงตามหลักการความปลอดภัยของ SELinux (อันนี้ไม่รู้จัก ไปอ่านต่อได้ที่ ที่นี่)

MySQL ใช้ Access Control Lists (ACLs) สำหรับการเชื่อมต่อ และ ตอนนี้ MySQL ก็รองรับการเชื่อมต่อแบบ SSL แล้ว

PostgreSQL

PostgreSQL is a popular SQL database. It has been in active developn
years and is considered to be one of the most advanced relational dat
PostgreSQL is also easy to learn and setup compared to other relatior
available. Because of its free and open source nature, this is a popula
startups.

PostgreSQL is a cross-platfo
configuration and access/dat
though.

In this article, we'll will be u
includes PostgreSQL by def
different operating system.

Postgres Advantages over MySQL

Postgres is an object-relational database, while MySQL is a purely relational database. This means that Postgres includes features like table inheritance and function overloading, which can be important to certain applications. Postgres also adheres more closely to SQL standards.

Postgres handles concurrency better than MySQL for multiple reasons:

Postgres implements Multiversion Concurrency Control (MVCC) without read locks Postgres supports parallel query plans that can use multiple CPUs/cores Postgres can create indexes in a non-blocking way (through the `CREATE INDEX CONCURRENTLY` syntax), and it can create partial indexes (for example, if you have a model with soft deletes, you can create an index that ignores records marked as deleted) Postgres is known for protecting data integrity at the transaction level. This makes it less vulnerable to data corruption.

Why Postgres? Because it's the best. It really is *"The World's Most Advanced Open Source Relational Database"*. And it will really help you solve your challenges, and make your application *just work*.

How Do We Secure the Medical Record ?

Person	First name	Account type	Subscription date	Tickets submitted
1	Luke	Pro	13 May 2017	2
2	John	Enterprise	25 Feb 2016	3
3	Nathan	Free	17 Sep 2014	5
4	Aaron	Free	2 May 2018	2
5	Daniel	Pro	13 Aug 2018	1
6	Michael	Pro	13 Dec 2018	0

Person	First name	Account type	Subscription date	Tickets submitted
1	Daniel	Free	13 Dec 2018	1
2	Nathan	Pro	2 May 2018	0
3	Michael	Free	25 Feb 2016	2
4	Luke	Pro	17 Sep 2014	3
5	Aaron	Pro	13 May 2017	5
6	John	Enterprise	13 Aug 2018	2

How to create an https server?

How to create an https server?

2011-08-26

If you're using Nodejitsu, we handle HTTPS for you. Free SSL on jit.su and nodejitsu.com subdomains, and SSL on custom domains for business customers. *It's never necessary to create an HTTPS server yourself.*

To create an HTTPS server, you need two things: an SSL certificate, and built-in `https` Node.js module.

We need to start out with a word about SSL certificates. Speaking generally, there are two kinds of certificates: those signed by a 'Certificate Authority', or CA, and 'self-signed certificates'. A Certificate Authority is a trusted source for an SSL certificate, and using a certificate from a CA allows your users to be trust the identity of your website. In most cases, you would want to use a CA-signed certificate in a production environment - for testing purposes, however, a self-signed certicate will do just fine.

To generate a self-signed certificate, run the following in your shell:

```
openssl genrsa -out key.pem
openssl req -new -key key.pem -out csr.pem
openssl x509 -req -days 9999 -in csr.pem -signkey key.pem -out cert.pem
rm csr.pem
```

This should leave you with two files, `cert.pem` (the certificate) and `key.pem` (the private key). Put these files in the same directory as your Node.js server file. This is all you need for a SSL connection. So now you set up a quick hello world example (the biggest difference between https and http is the `options` parameter):

Development Guidelines

1. OWASP Top 10 Application Security Risks (2017)
2. OWASP API Security Top 10 (2019)

Testing and Evaluation

Vulnerability Assessment and Penetration Testing

Health Insurance Portability and Accountability Act (HIPAA)

It was created primarily to modernize the flow of healthcare information, stipulate how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance coverage.

Health Insurance Portability and Accountability Act (HIPAA)

The HIPAA Security Rule – Focuses on securing the creation, use, receipt, and maintenance of electronic personal health information by HIPAA-covered organizations. The Security Rule sets guidelines and standards for administrative, physical, and technical handling of personal health information.

The HIPAA Privacy Rule – Requires safeguards to protect the privacy of personal health information including medical records, insurance information, and other private details. The Privacy Rule limits what information may be used (and in what manner) and disclosed to third parties without prior patient authorization.

Health Insurance Portability and Accountability Act (HIPAA)

The act consists of five titles.

Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.

Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

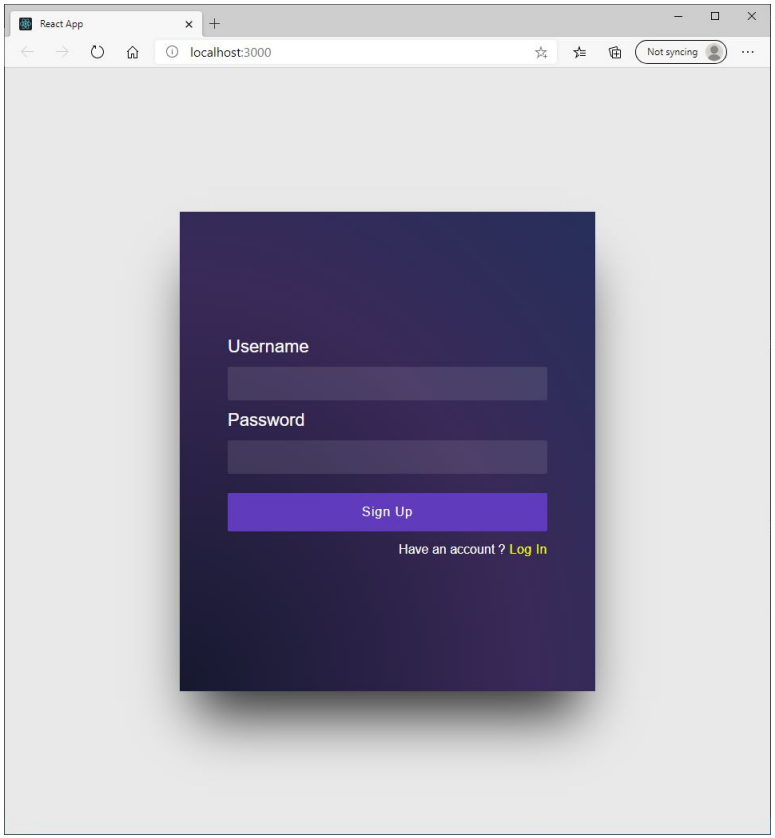
Title III sets guidelines for pre-tax medical spending accounts.

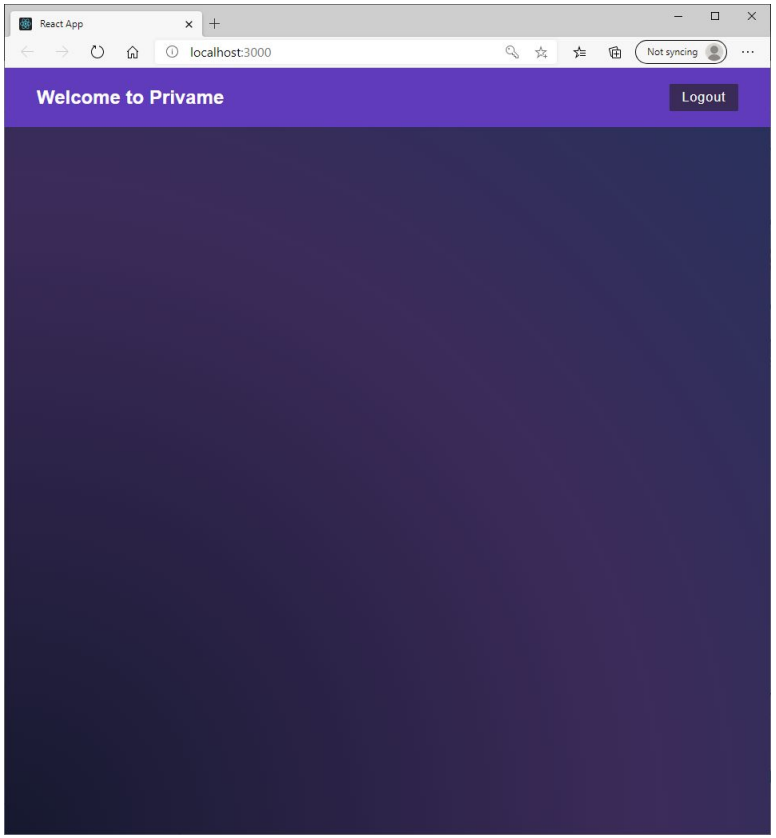
Title IV sets guidelines for group health plans.

Title V governs company-owned life insurance policies.

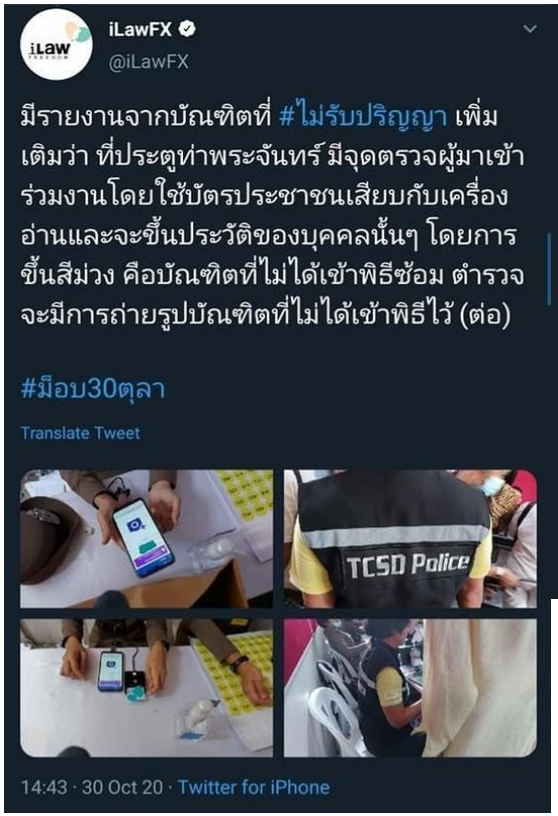
มหาวิทยาลัยมหิดล
คณะเทคโนโลยีสารสนเทศ
และการสื่อสาร

Current Progress





Example



ขณะที่ศูนย์ทนายเพื่อสิทธิมนุษยชนเผยแพร่ข้อความจากโซเชียลมีเดียของผู้ใช้รายหนึ่งระบุว่าถูกตรวจสอบประวัติการรักษาโรคจิตเวชที่ทางเข้าบริเวณประตูท่าพระอาทิตย์ ก่อนเข้ามหาวิทยาลัย โดยระบุว่า “ถ้าตรวจแล้วมันขึ้นประวัติว่าเรารักษาตัวที่ไหนก็จะโดนแยกตัวไปอีกโต๊ะหนึ่ง แล้วก็โดนซักประวัติว่าเป็นโรคอะไรรักษามานานกี่ปีแล้ว” ข้อความดังกล่าวระบุ “เขาบอกกลัวเข้างานแล้วควบคุมตัวเองไม่ได้”