

# 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 Pungsart



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



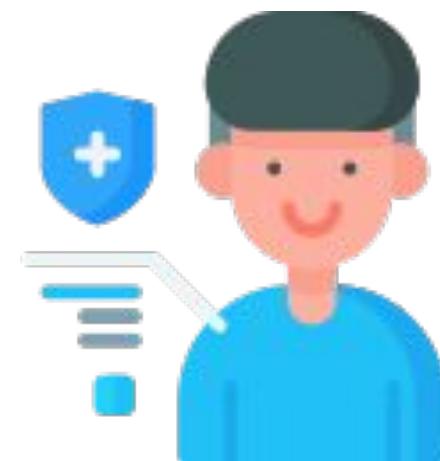
# HOSPITAL B



# 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

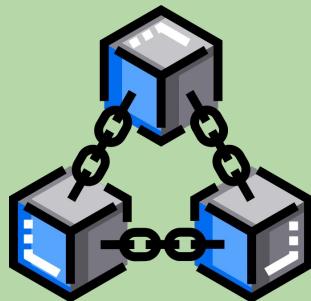
# Backgrounds



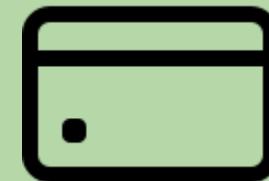


# Literature Review

## “Privacy and Security”



BLOCKCHAIN



SMART CARD



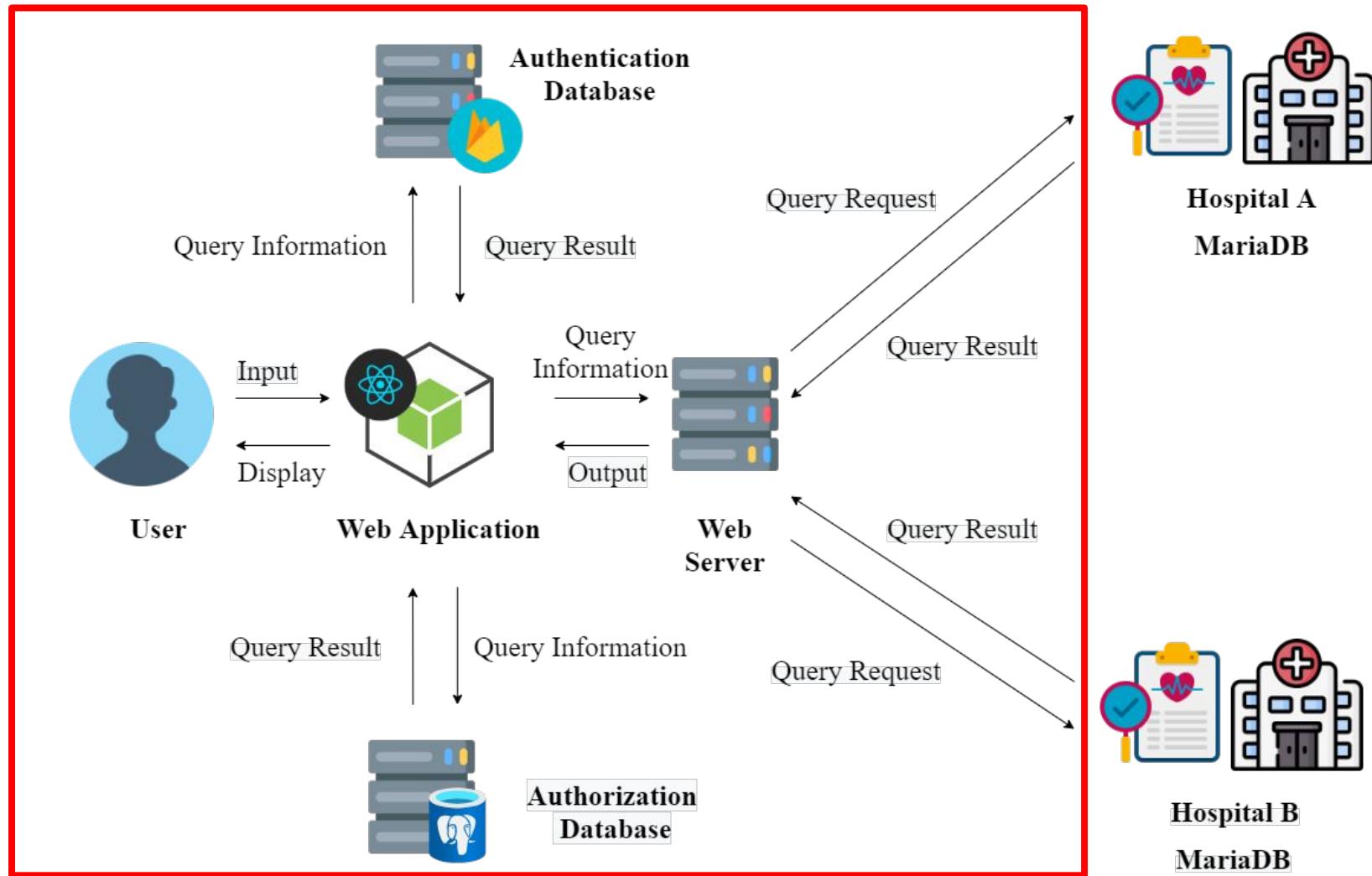
# 04

# System Design & Implementation



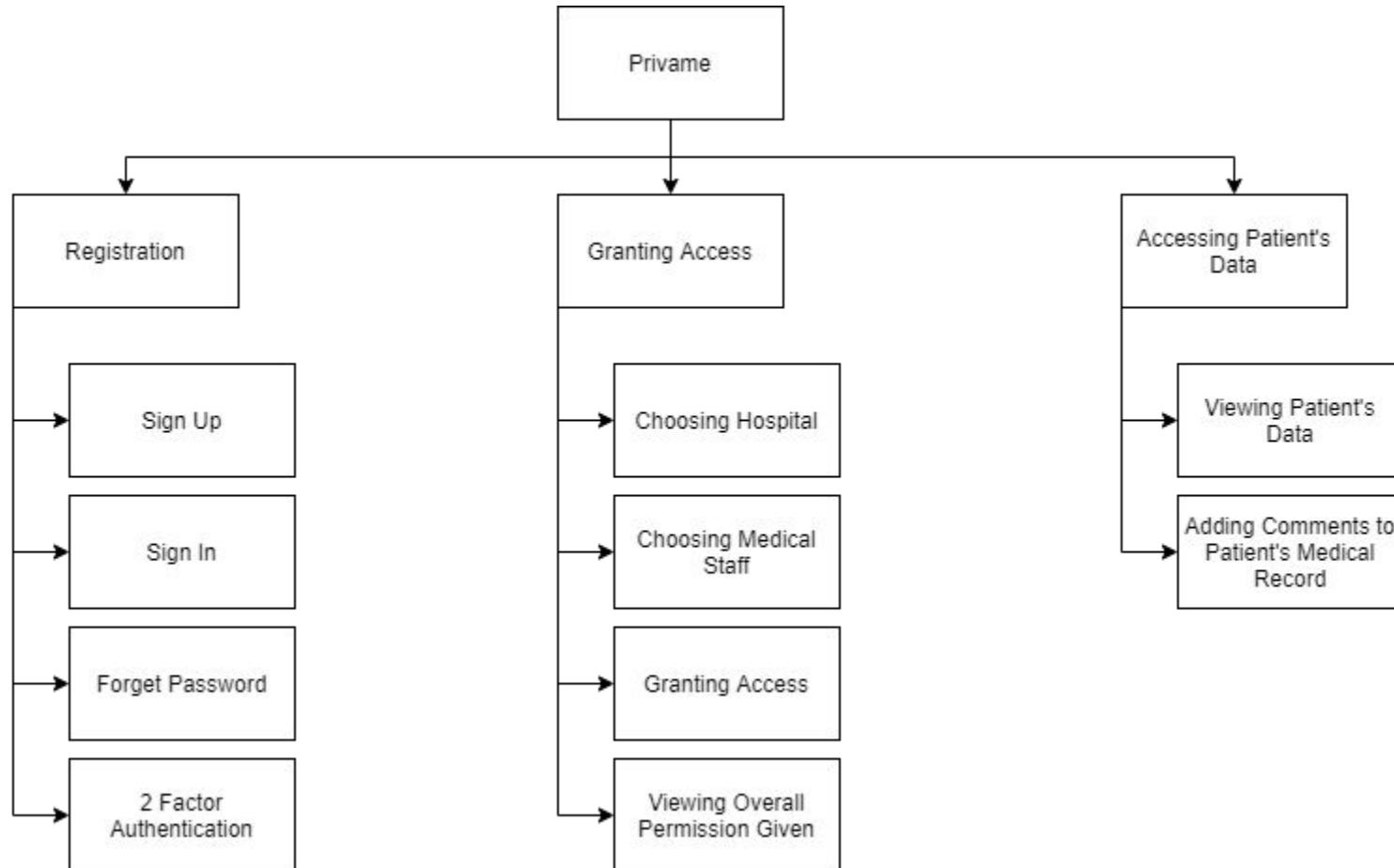


# System Architecture Overview





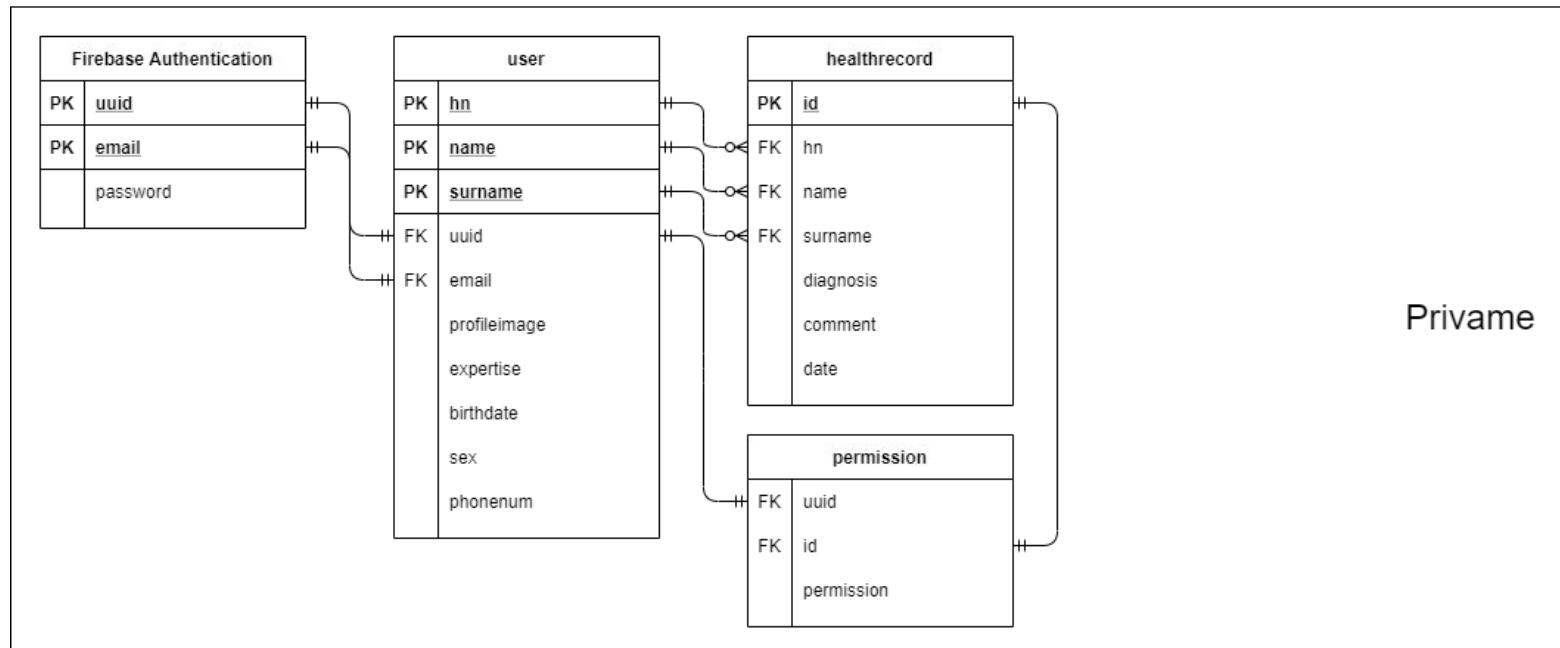
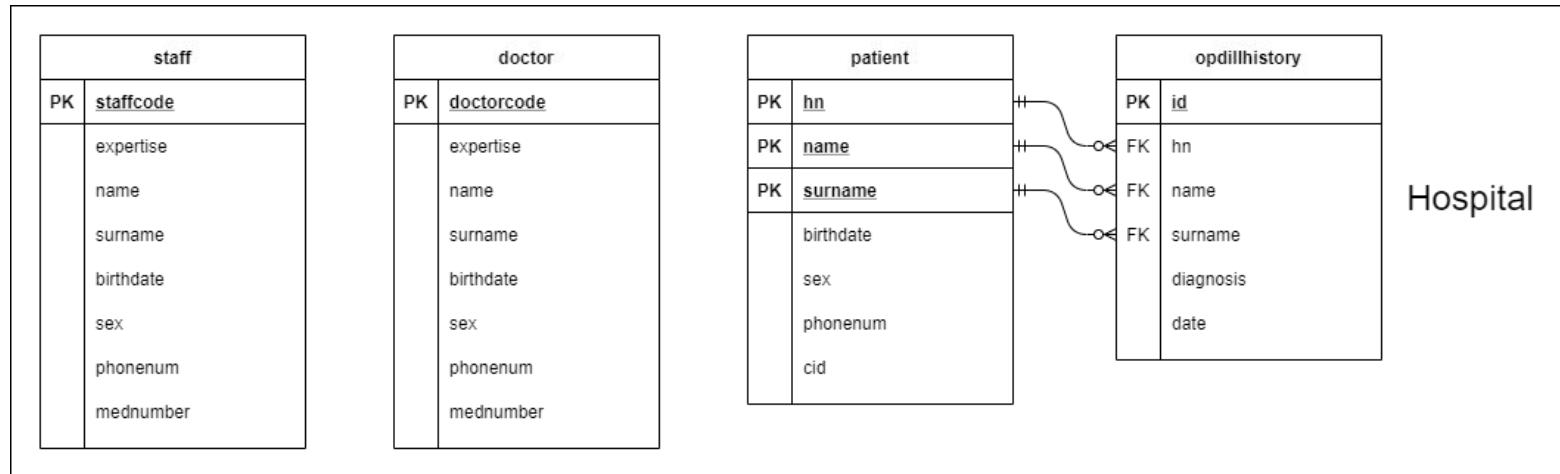
# System Structure Chart



# ER Diagram

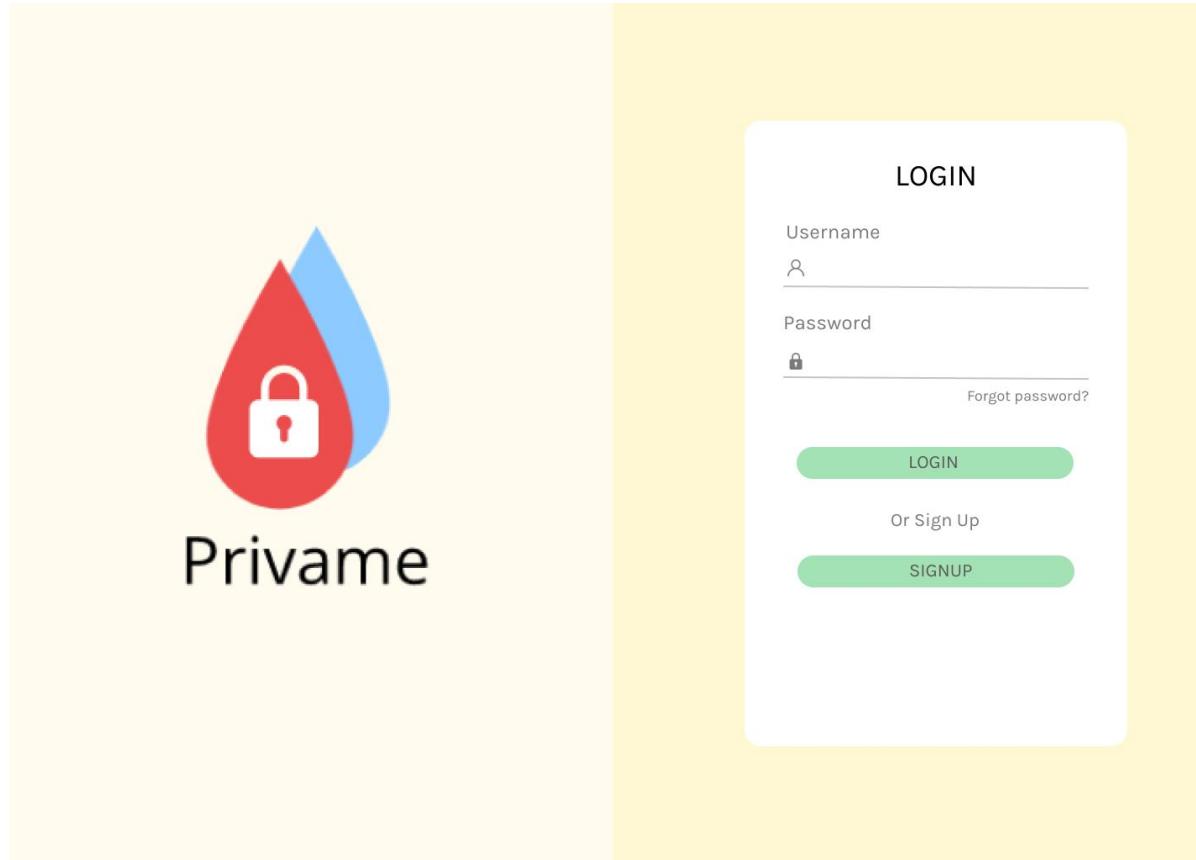


มหาวิทยาลัยมหิดล  
ถนนเทอดปุ่นโลยสารสนเทศ  
และการสื่อสาร





# Prototype



The image shows a prototype of a login page for a service called "Privame". The page is divided into two main sections: a left panel and a right panel.

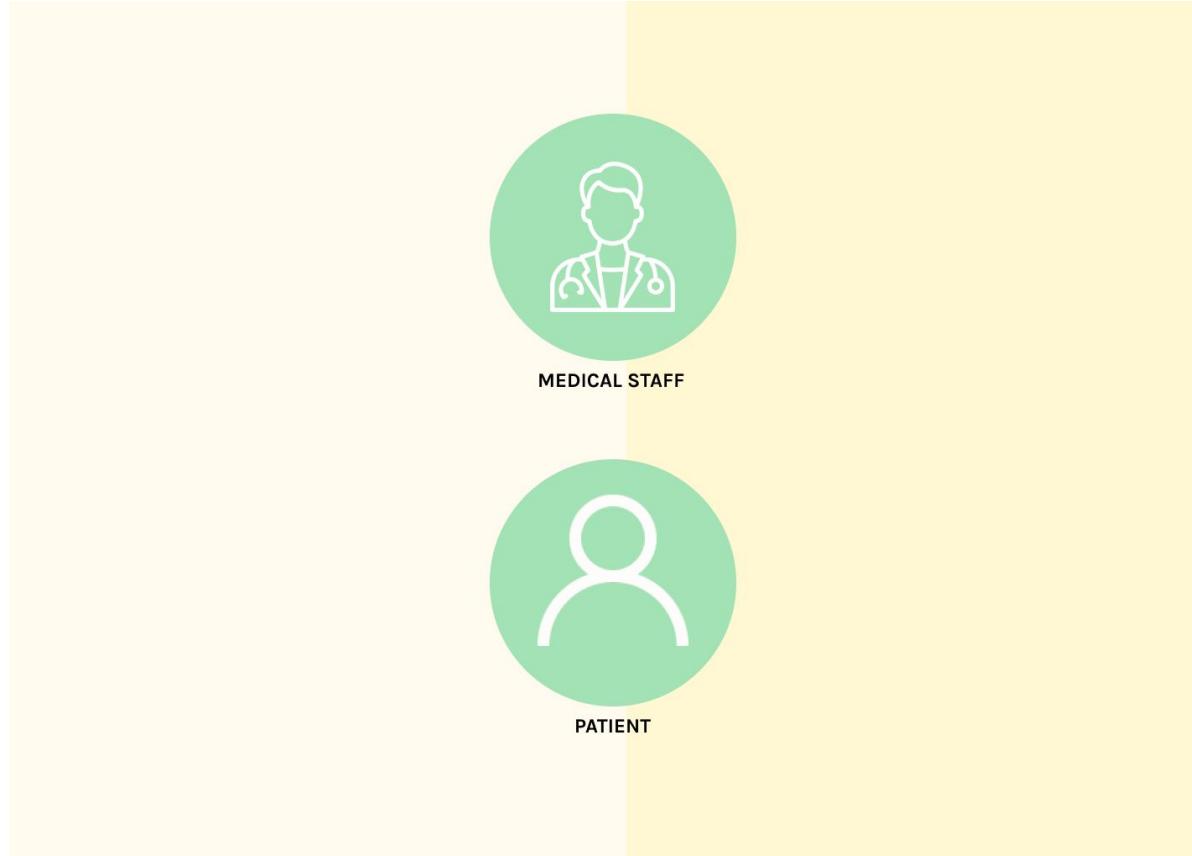
**Left Panel:** This panel features a large, stylized logo consisting of two overlapping teardrop shapes, one red and one blue, containing a white padlock icon. Below the logo, the word "Privame" is written in a bold, sans-serif font.

**Right Panel:** This panel contains a white rectangular form with rounded corners. At the top, the word "LOGIN" is centered in a bold, black font. Below it is a "Username" field with a placeholder icon of a person and a text input field. Next is a "Password" field with a placeholder icon of a lock and a text input field. To the right of the password field is a link "Forgot password?". Below these fields are two green, rounded rectangular buttons: a larger one labeled "LOGIN" and a smaller one labeled "SIGNUP". Between the two buttons is the text "Or Sign Up".

Login Page



# Prototype



Choosing Role



# Prototype



PATIENT

SIGNUP

Username

---

Password

---

Confirm Password

---

[Next](#)

Sign Up



# Prototype



PATIENT

### INFORMATION

Name - Surname

---

Email

---

Phone Number

---

Hospital Number

---

Gender

---

Birth Date

---

I accept the [Terms of Use](#) & [Privacy Policy](#)

**SIGN UP**

Add Information for Sign Up



# Prototype

**INFORMATION**

×

## Privacy Policy

Nam sollicitudin nisl urna, id tincidunt ligula porttitor vel. Curabitur gravida sagittis imperdiet. Pellentesque posuere nibh nec justo elementum blandit. Cras vel ligula lectus. Vivamus non egestas ipsum, vitae ullamcorper metus. Ut tempus laoreet lectus. Suspendisse ultrices odio non nulla posuere fringilla. Duis mollis lacus auctor volutpat. Proin posuere neque vel tortor pharetra aliquam. Morbi hendrerit blandit euismod. Etiam finibus est ipsum, sed accumsan purus semper quis. Duis ut nisi et dolor hendrerit commodo et sit amet purus. Ut in cursus nulla, nec.

Sed ornare, elit eu venenatis imperdiet, odio libero feugiat elit, quis porttitor quam massa sed massa. Aliquam dolor lacus, ornare a tempus fermentum, vulputate ut eros. Phasellus diam nunc, ornare eu lacus vitae, venenatis eleifend turpis. Nulla sollicitudin lacus id ultricies mauris. Nam ut ullamcorper diam. Duis ut sapien tincidunt, aliquam est sit amet, volutpat tellus. Nulla facilisi. Nunc at erat justo. Phasellus maximus mauris eget dui molestie semper. Vivamus quis diam libero. Quisque purus purus, euismod eu est ac, finibus euismod massa. Phasellus elit dolor, ultricies sit amet interdum ac, dictum ut neque. Praesent at nunc non libero vulputate dignissim a sit amet eros. Quisque lacinia, massa vel tristique semper, libero felis lobortis dui, sed sodales tellus turpis non mi. Aliquam consequat, lectus eget vehicula varius, ligula enim feugiat odio, vitae condimentum magna libero sed dolor. Nam vitae mollis dolor, in vulputate mauris.

I agree to the privacy policy

[Privacy Policy](#)

**SIGN UP**

## Privacy Policy



# Prototype

The screenshot shows a mobile application interface for medical staff verification. On the left, there is a green circular icon containing a white silhouette of a doctor wearing a stethoscope, labeled "MEDICAL STAFF". The main area has a yellow header with the word "Verification". Below it is a yellow circle containing a white smartphone icon. A text message reads: "We will send you a One Time Password on your mobile phone". Below this is a text input field with the placeholder "Enter your mobile number". To the right of the input field is a yellow button labeled "GET OTP". To the right of the input field is a large white form with fields for "Name" (placeholder "Name"), "Email" (placeholder "mail.com"), "Phone Number" (placeholder "Phone Number"), and "OTP" (placeholder "OTP"). At the bottom of the form are links for "Terms of Use & Privacy Policy" and a green "SIGN UP" button.

SMS Verification



# Prototype (Patient)

PRIVAME

Welcome ALICE GOODWILL

My Data

My Shared Data

My Permission

Logout

SHARED DATA with doctor

Hospital

Select Hospital

Doctor

Select Doctor

Data rights

Read

Share Data

Access Granting Page



# Prototype (Medical Staff)

The screenshot shows the 'MY PATIENT' screen of the PRIVAME app. At the top, there's a header bar with the 'PRIVAME' logo and a blood drop icon. Below the header, on the left, is a sidebar with a user profile picture and the text 'Welcome STRANGE'. The main content area is titled 'MY PATIENT' and contains a table with patient information. The table has columns for 'PATIENT ID', 'HOSPITAL', 'VIEW COMMENT', 'ADD COMMENT', and 'DOWNLOAD'. One row is visible, showing 'HN123456789' under 'PATIENT ID', 'Hospital A' under 'HOSPITAL', and two buttons under 'COMMENT': 'View Comment' and 'Add Comment'. A 'FILE.PDF' link is also present under 'DOWNLOAD'. On the far left of the sidebar, there are three menu items: 'My Bio', 'My Patients', and 'LogOut', each with an associated icon.

PATIENT ID	HOSPITAL	VIEW COMMENT	ADD COMMENT	DOWNLOAD
HN123456789	Hospital A	<a href="#">View Comment</a>	<a href="#">Add Comment</a>	<a href="#">FILE.PDF</a>

Permission Received from the Patient



# Prototype (Patient)

The screenshot shows the PRIVAME patient portal. The top navigation bar has a lock icon and the text "PRIVAME". The left sidebar, titled "Welcome ALICE GOODWILL", includes links for "My Data", "My Shared Data", "My Permission", and "LogOut". The main content area is titled "AUTHORIZATION given by me" and displays a table of permissions:

DOCTOR NAME	RIGHT	FILENAME
STRANGE	EDIT	PHR-00001
JONATHAN	READ	PHR-00001

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.

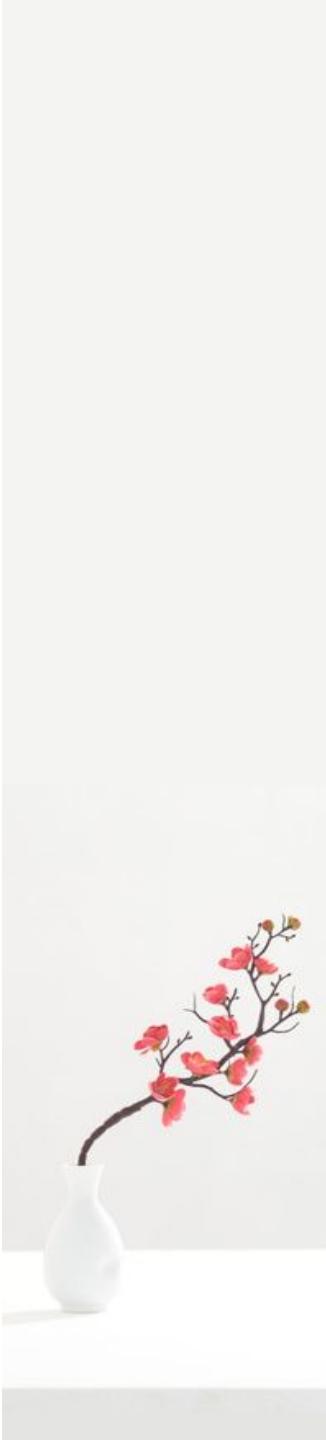




# References

- <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



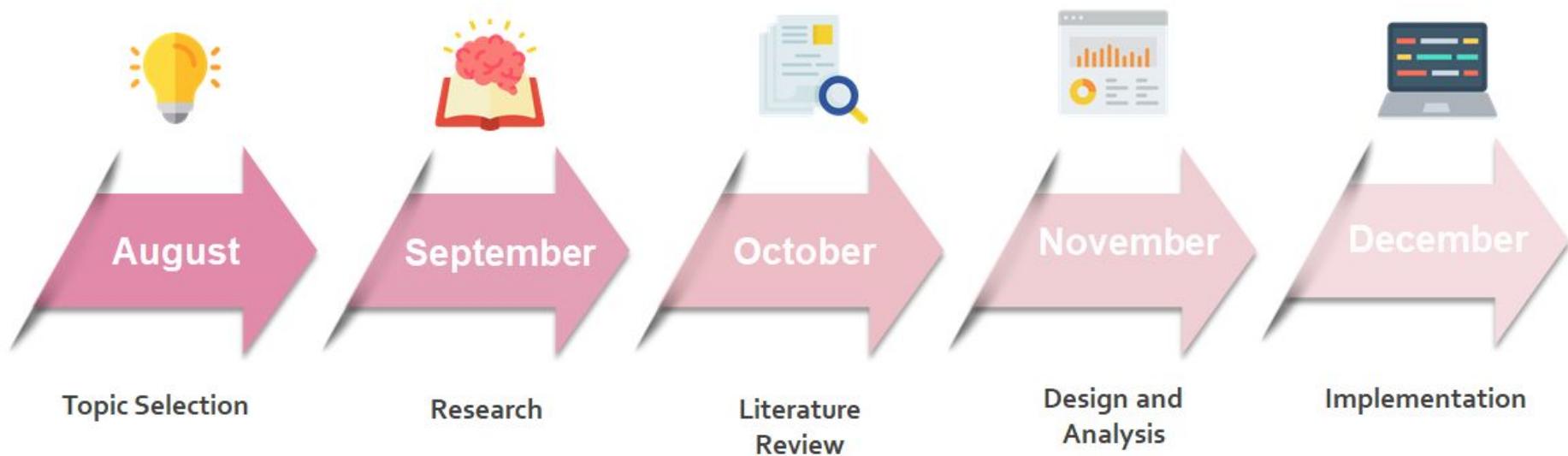


# Protocols

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



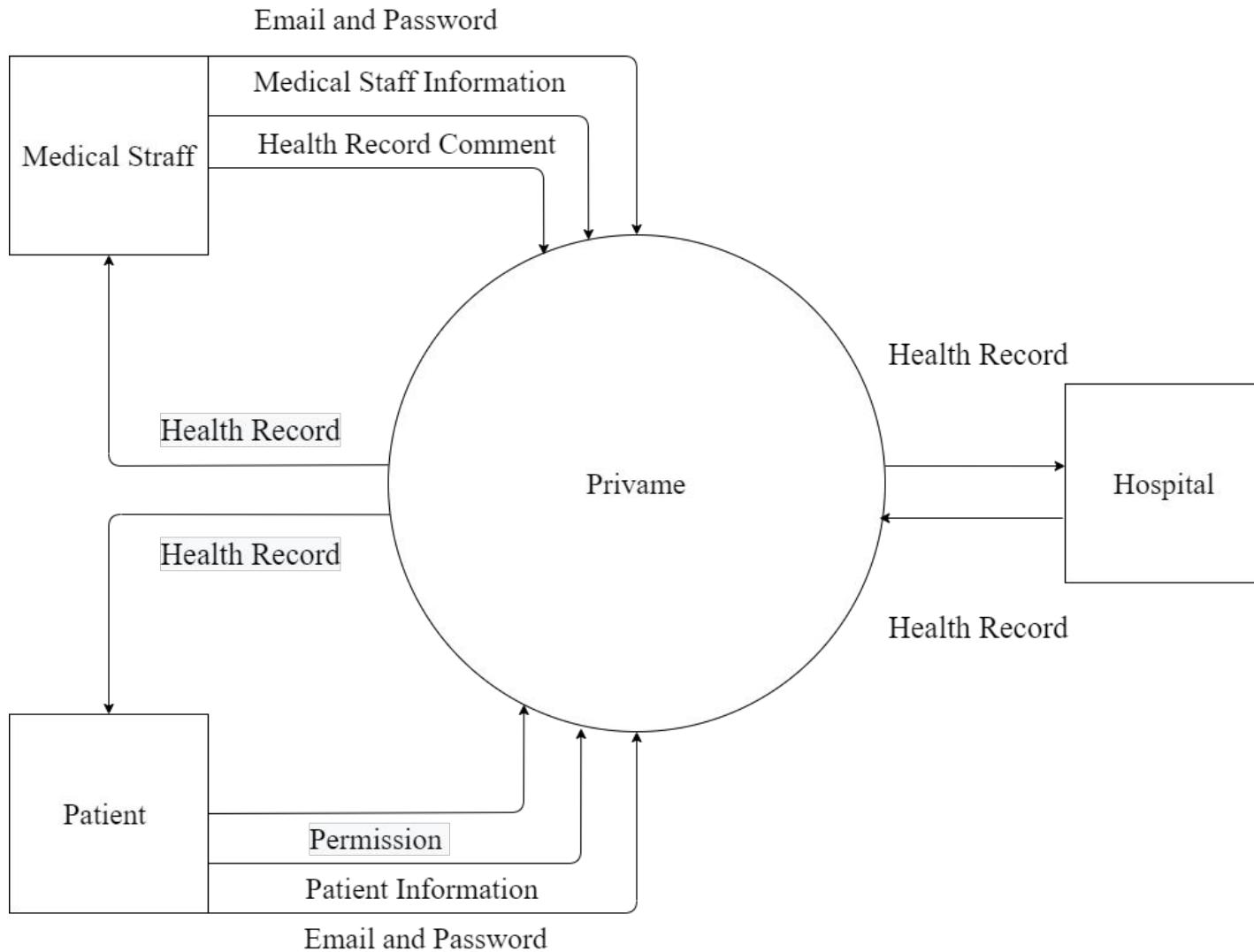
# Timeline



# Data Flow Diagram



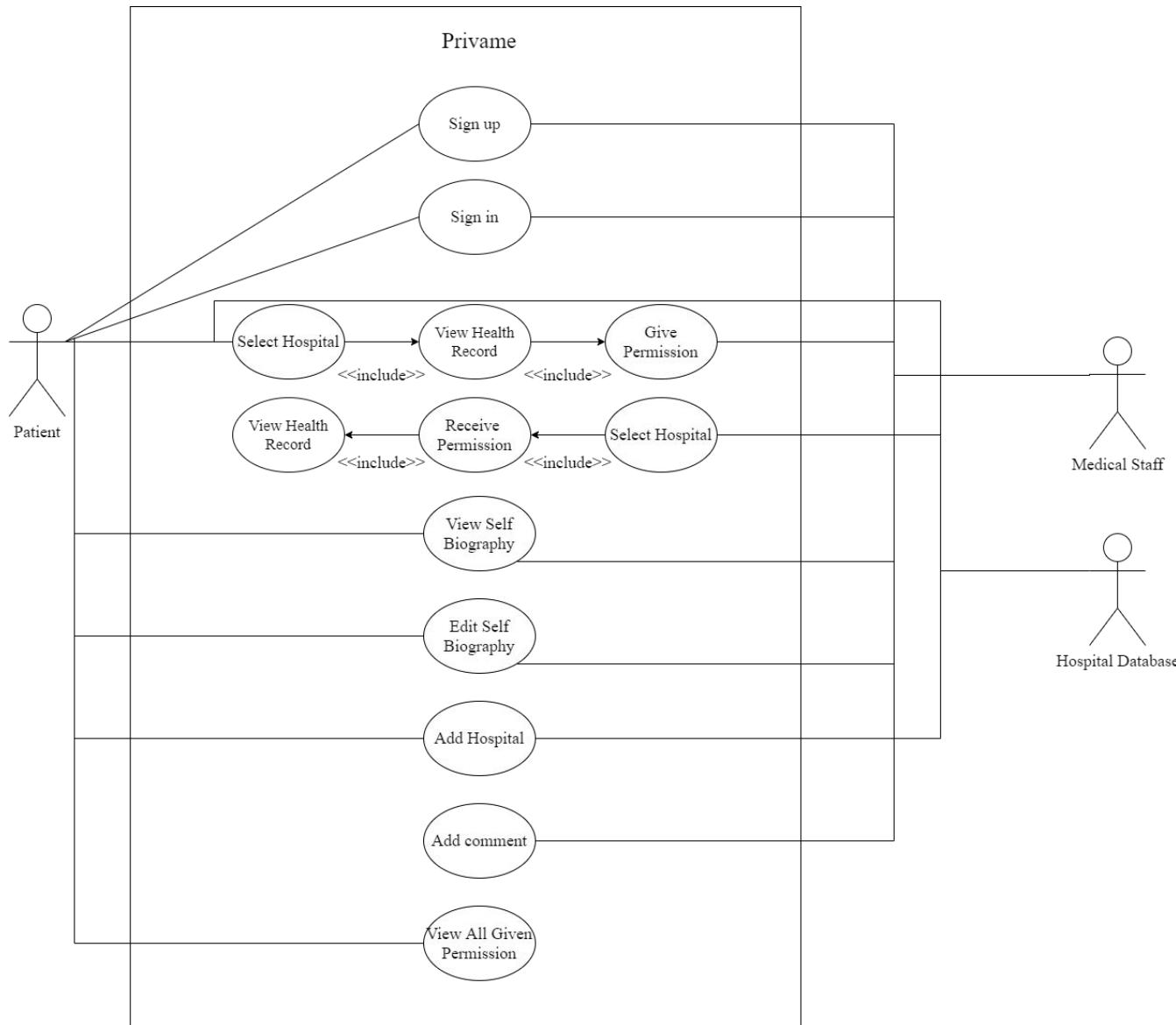
มหาวิทยาลัยมหิดล  
คณะเทคโนโลยีสารสนเทศ  
และการสื่อสาร



# Use Cases Diagram



มหาวิทยาลัยมหิดล  
คณะเทคโนโลยีสารสนเทศ  
และการสื่อสาร





# 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



## ตรวจสอบรายชื่อแพทย์ จากฐานข้อมูลแพทยสภา

ค้นพบผู้ประกอบวิชาชีพเวชกรรม(แพทย์) จำนวน 1 รายการ



นพ. ประชัน บัญชาศักดิ์  
PRACHAN BANCHASUEK, MD.

เป็นผู้ประกอบวิชาชีพเวชกรรมตั้งแต่ พ.ศ. 2532  
Permission to practice medicine since 1989

สถานะความรู้ความชำนาญเฉพาะทาง

- ✓ สาขา ออร์โธปิดิกส์ ( Orthopedics )
- แพทย์ที่มีใบอนุญาตประกอบวิชาชีพเวชกรรม ห้ามนำเข้าไปในโรงพยาบาลที่มีศักยภาพน้อย หรือของมีผลลัพธ์ที่มีความก่อความเสียหาย
- แพทย์ที่ยังไม่มีรูป หรือยังไม่มีบัตรประจำตัวผู้ประกอบวิชาชีพเวชกรรม (MDCARD) โปรดติดต่อแพทยสภาที่ โทรสาร 02-5901887

ผลการตรวจสอบ เลขที่ใบประกอบวิชาชีพเวชกรรม

- ท่านไม่ได้ขอตรวจสอบเมื่อ

ต้องการตรวจสอบเลขที่ใบประกอบวิชาชีพเวชกรรม ? คลิกที่นี่

ค้นหาอีกครั้ง



### ข้อมูลของฉัน / Virtual ID



มหาวิทยาลัยมหิดล  
คณะแพทยศาสตร์โรงพยาบาลรามาธิบดี



HN [REDACTED]  
บ.ส. [REDACTED]  
วัน/เดือน/ปีเกิด [REDACTED]  
เพศ [REDACTED]  
เบอร์โทรศัพท์ [REDACTED]



มหาวิทยาลัยมหิดล  
คณะเทคโนโลยีสารสนเทศ  
และการสื่อสาร





# 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.

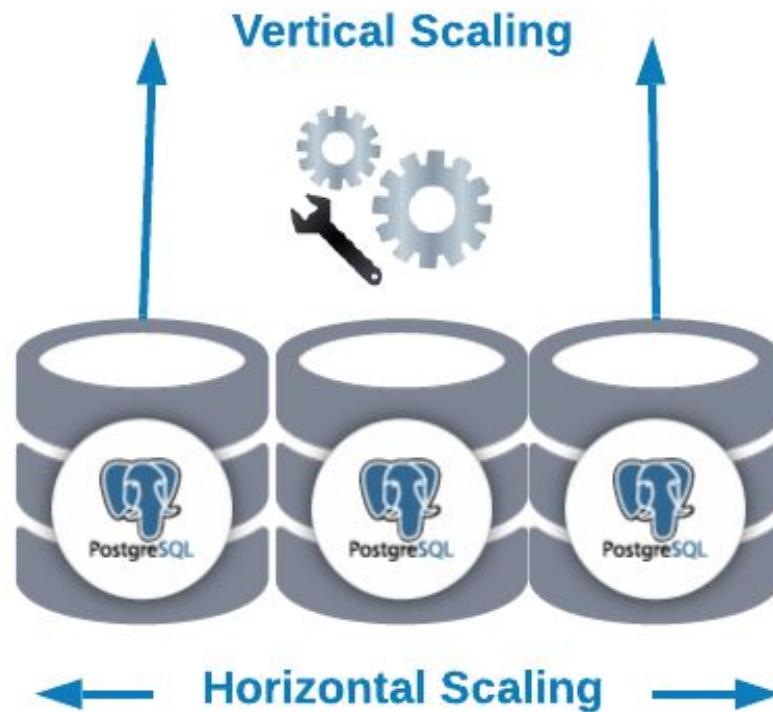
## Usage

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

## PostgreSQL

PostgreSQL is a popular SQL database. It has been in active development for years and is considered to be one of the most advanced relational databases.

PostgreSQL is also easy to learn and setup compared to other relational databases. Because of its free availability, it's becoming increasingly popular among startups.

PostgreSQL is a cross-platform database system, making it easy to install and configure on different operating systems. It also supports multiple programming languages and provides a wide range of features for managing data.

In this article, we'll will be using PostgreSQL as our primary database system. We'll cover how to install PostgreSQL on different operating systems, basic configuration, and access methods.

## 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 professionals:

### Security

MongoDB, PostgreSQL is SSL in client/server mode. PostgreSQL's security features include:

- SSL/TLS support for client-server communication.
- Role-based access control (RBAC) for managing user permissions.
- Row-level security (RLS) for controlling access to specific rows of data.
- File-based replication for disaster recovery and scaling.

PostgreSQL uses SSL for client-server communication. PostgreSQL's security features include:

- SSL/TLS support for client-server communication.
- Role-based access control (RBAC) for managing user permissions.
- Row-level security (RLS) for controlling access to specific rows of data.
- File-based replication for disaster recovery and scaling.

MySQL uses Access Control Lists (ACLs) for managing user permissions. MySQL's security features include:

- SSL/TLS support for client-server communication.
- Row-level security (RLS) for controlling access to specific rows of data.
- File-based replication for disaster recovery and scaling.

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



มหาวิทยาลัยมหิดล  
คณะเทคโนโลยีสารสนเทศ  
และการสื่อสาร



# Testing and Evaluation

Vulnerability Assessment and Penetration Testing



KALI LINUX

# 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  
คณะเภสัชศาสตร์  
และการสื่อสาร





# Current Progress

A screenshot of a web browser window titled "React App" showing a login form. The URL bar indicates "localhost:3000". The form consists of two input fields: "Username" and "Password", both of which have been redacted with a dark grey color. Below the password field is a purple rectangular button labeled "Sign Up". At the bottom of the form, there is a link that says "Have an account? [Log In](#)".

A screenshot of a web browser window titled "React App" showing a dashboard. The URL bar indicates "localhost:3000". The top navigation bar is purple and contains the text "Welcome to Privame" on the left and a "Logout" button on the right. The main content area below the header is completely blacked out, indicating a redacted or blank section.



# Example

iLawFX ✅ @iLawFX

มีรายงานจากบันทึกที่ติดที่ #ไม่รับปริญญา เพิ่มเติมว่า ที่ประชุมฯท่าพระจันทร์ มีจุดตรวจสอบผู้มาเข้าร่วมงานโดยใช้บัตรประชาชนเสียบกับเครื่องอ่านและจะขึ้นประวัติของบุคคลนั้นๆ โดยการขึ้นสีมองคือบันทึกที่ไม่ได้เข้าพิริช้อม ตำราจะมีการถ่ายรูปบันทึกที่ไม่ได้เข้าพิริช้อม (ต่อ)

#มีมอง30ตula

Translate Tweet

14:43 · 30 Oct 20 · Twitter for iPhone

iLawFX ✅ @iLawFX · 41m

หลังจากนี้แจ้งส่งไปอีกจุด เพื่อบันทึกข้อมูลของบันทึกที่ไม่ได้เข้าพิริช้อม และส่งไปจุดสุดท้ายเพื่อบันทึกข้อมูลอีกครั้งและถ่ายรูปบันทึกอีกครั้ง - กระบวนการทั้งหมดนี้บัตรประชาชนจะอยู่ที่ตัวร่วงตลอด ใช้เวลาประมาณ 5 นาที

#มีมอง30ตula

8 1,239 94

ขณะที่ศูนย์ทนายเพื่อสิทธิมนุษยชนเผยแพร่ข้อความจากโซเชียลมีเดียของผู้ใช้รายหนึ่งระบุว่าถูกตรวจสอบประวัติการรักษาโรคจิตเวชที่ทางเข้าบริเวณประตูท่าพระอาทิตย์ ก่อนเข้ามหาวิทยาลัย โดยระบุว่า “ถ้าตรวจแล้วมันขึ้นประวัติว่าเรา\_rักษาตัวที่ไหนก็จะโดนแยกตัวไปอีกโต๊ะหนึ่ง และก็โดนซักประวัติว่าเป็นโรคอะไรรักษานานนานก็ปีแล้ว” ข้อความดังกล่าวระบุ “เขานอกกล่าวเข้างานแล้วควบคุมตัวเองไม่ได้”