Project Legal Statement

Introduction

Our client, Apian, is a medical drone start-up that partners with the NHS to connect the healthcare industry with the drone industry to improve patient health outcomes and staff well-being. Apian has asked us to work together with them and start a project which we call PorterBLE.

The PorterBLE system consists of a web app and an android application. The Android Application is for medical porters to use. The purpose of the application is for tracking their location within the hospital. Once a porter with their smartphone comes close to a beacon placed in the hospital, the app will send the MAC Address of that beacon to our web app's backend for us to display their live location. The web app is made for medical dispatchers for them to monitor the availability, location, and create a delivery request for porters who are available and closest to the pick-up location.

For such software applications, not only do we need to outline the functionality but also, we need to consider the legal implications of PorterBLE. We have outlined below the data privacy, licenses/intellectual property, and manufacturing processes.

Sustainability and Costing

The client will need to pay for deploying our solution, for that we utilized following paid services:

- Cloud Run: 34.4 USD per month
- Cloud SQL: 154.45 USD per month
- Twillio: 0.0420 USD per message to send, 0.0075 USD per message to receive

Licenses and Intellectual Property

Here are the dependencies used for this project:

- Spring Boot (Apache-2.0 license)
- Node.Js (MIT license)
- React (MIT license)
- Material-UI (MIT license)
- Twilio (Apache-2.0 license)
- Google Api Client (Apache-2.0 license)
- PostgreSQL (PostgreSQL License)

Data Privacy

As mentioned above, The PorterBLE system consists of an android app and a web app that works together. The system may not be publicly accessed, and it may only be accessed by our client and their partners. In this case, it would be the medical staff in the hospital. The app requires login details which ask for the porter's name and phone number which we store in our database. Once a porter is registered in our web app's backend with their name and phone number, we use this information to cross-check whether the user trying to log in through the app puts in the correct login details. If the user gives the correct login details, they will receive a one-time pin for authentication. We store all our user data in the google cloud service's database. For database security, the google cloud service has its form of encryption layer as stated on their website, "At Google, our comprehensive security strategy includes encryption at rest, which helps to protect customer content from attackers. We encrypt all Google customer content at rest, without any action required by you, using one or more encryption mechanisms" (Google Cloud, 2022).

To summarize, the only data we store is the medical porter's name, phone number, and location. We will not expose any of this data to the public and only the hospital admins can access this data.

Conclusion

We have outlined above the legal aspects as well as the sustainability/costing of this project. We carefully considered every social aspect of this project especially data privacy since medical staff will be using our software in the future. We also included the cost of the services we're using and also listed the dependencies, in order for future developers to iterate and improve on the software.