**Security**

Security has been a fundamental part of the JustHealth project and it is something that we have taken seriously throughout development and it is now something that we are able to pride our project on. We have considered the security of the application holistically and have used a combination of security techniques in order to ensure the security of the application and confidentiality of user data.

Firstly, we have implemented strong password security that has been used throughout the application to ensure that no plaintext passwords are stored within the JustHealth database or the mobile application. This has been done through the use of standard python encryption and hashing methods.

As well as this, we also recognised the importance of using SSL/TLS in order to protect the confidentiality of data when it is being transmitted. Due to the fact that we are running our own web server on raptor, we were unable to used signed certificates and android would throw exceptions upon the use of self-signed. Therefore, the decision was made not to implement although, in the technical documentation evidence can be found which shows that we would be able to implement this had the application been hosted on our own server and not raptor.

HTTP Basic security was also used on the JustHealth API ensuring that not any one would be able to query the API. This was implemented on all publically accessible methods except those that can be accessed without needing to be logged in, for example, registration. All other methods therefore require the username and encrypted password of a registered user to be sent with any request to an API method.

Additionally, we apply further checks in order to ensure that the user that is querying the API is only able to query the API with regards to themselves or if they are a carer, themselves or certain information for their connected patients.

JustHealth have also utilised an Object Relational Mapper (Peewee) and therefore, do not use any SQL. This mitigates the risk of SQL injection completely. If data is sent to the database in the wrong format, it will simply be rejected by the ORM.