Requirements Specification for NHS Digital

NHS Identity App

Version 1.0

20 October 2020

Prepared By:

Group 11

Paridhi Agarwal (skcb42)

Mitchell Aaron Chandra (psrs87)

Soonhyun Chang (pcpx25)

Omar Mazhar (zsdd25)

Sonia Parmar (dkcp77)

Jia Xiu Sai (rpsh88)

Contents

1.1 Overview and Justification

Our project is to make an improved login system to the current NHS app. We aim to make the NHS login system more secure and convenient for NHS users to access their data, ergo making the app more user-friendly to help with the overall digitalisation of the NHS on a grand scale. This will not only save time for the users, as all their data can be viewed with just a few clicks as opposed to physically going to NHS centres (which is now impossible)/making many tedious calls to multiple numbers only to finally get through to a call centre, but also majorly reduce costs for NHS as they would require fewer people at call centres to answer customer questions regarding the navigation of the app, as the update we plan to implement for the app is expected to be very user-friendly.

The purpose of this system is to enable users to log in, more securely and conveniently than the previously existing system to maximise the total number of users. The reason why this is beneficial is that presently, many people do not utilise the app's functionality due to it being inconvenient and redundant.

The login system is quick and convenient is extremely important as it is the first thing people do when they download an app. Details like user confirmation and verification would be very quick and easy to follow through in the updated app with just a few clicks. The app will be extremely secure to abide by all data privacy requirements.

1.2 Project scope

The current population of the UK approximates to 67 million - all of which have access to the NHS. The NHS currently have an app where users are able to access their medical records, appointments and prescriptions. This can be accessed using a login system. Our goal is to not recreate the whole app but to only make a more efficient registration and login system that will allow NHS users to easily login and access their medical records.

The login function will use current and new methods to improve the user login experience. For example, the app currently allows the option of logging in using their fingerprint through biometric authentication which we will also implement in our login system since this one action is enough to uniquely identify each user. The user will also be given the option to add their fingerprint at registration. As an alternative, the user will be able to log in via an OTP or email ID & password. (i.e. the user does not have a fingerprint scanner)

The registration feature will include the user inputting personal details about themselves that will be enough to verify and uniquely identify their medical records. For example, their name, date of birth, email address, phone number and to physically identify themselves, users will send a photo of their ID (driver's licence, passport etc) along with a video recording of themselves to obtain verification from a member of staff from NHS Digital. This is to ensure that the correct records are retrieved for the user.

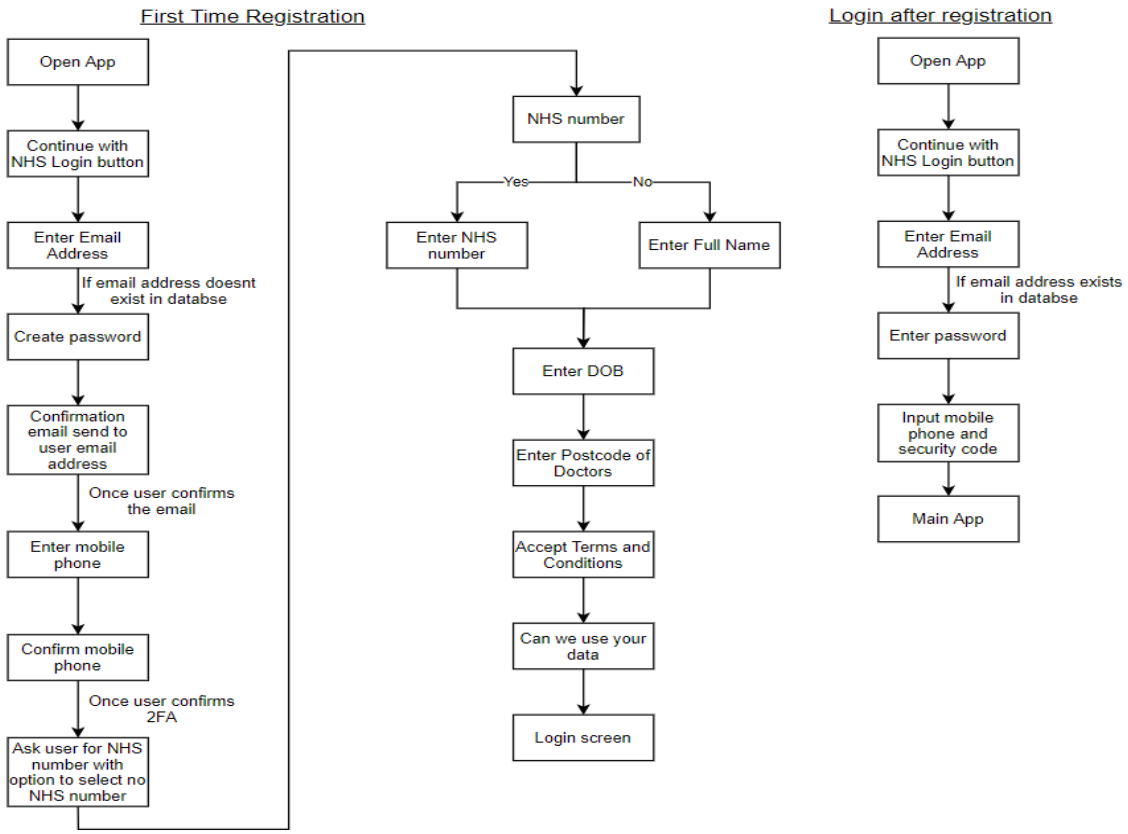
Users will also be able to login offline (via fingerprint/pin code) in the case of signal loss. These two methods are appropriate since their identification can be verified using the mobile phone. We intend to improve the "Forgot Password" function by giving users the option of choosing how they wish to authenticate themselves to reset their password. These options include email, phone number or security questions (more in section 2).

Features we could include in the future version of the login system are: creating a retina scan that will be uniquely identifiable to each user, using an automated system for face scan (via phone camera for android), and for iOS users, integrating the NHS app with the iOS healthcare app to allow users to access their medical records offline on their phone - this could also include authenticating using the devices' passcode as another form of verification. Another future implementation could include having family access to medical records - i.e all users in a family will be able to access each other's medical records. This would be useful if parents have to keep track of their child's prescriptions/ injections and ideal for elderly users who are not sure how to access their medical records.

1.3 System description

The new login system for the NHS app will be implemented on both Android and iOS. To maximise user experience and compatibility, the Android version will be written in Kotlin and the iOS version will be written in Swift.

The flowchart below describes the current registration and login system of the NHS App.



The user opens the app, selects continue and is prompted to enter an email address, and on a separate page enter a password twice (which will occur on the same page in the improvement)

The user will then receive an email asking them to verify their email address. Once the email is verified, the app asks for a mobile phone number to be inputted, which will allow them to verify using an OTP. After entering the OTP the user will be asked if they have an NHS number, where one of two things may happen.

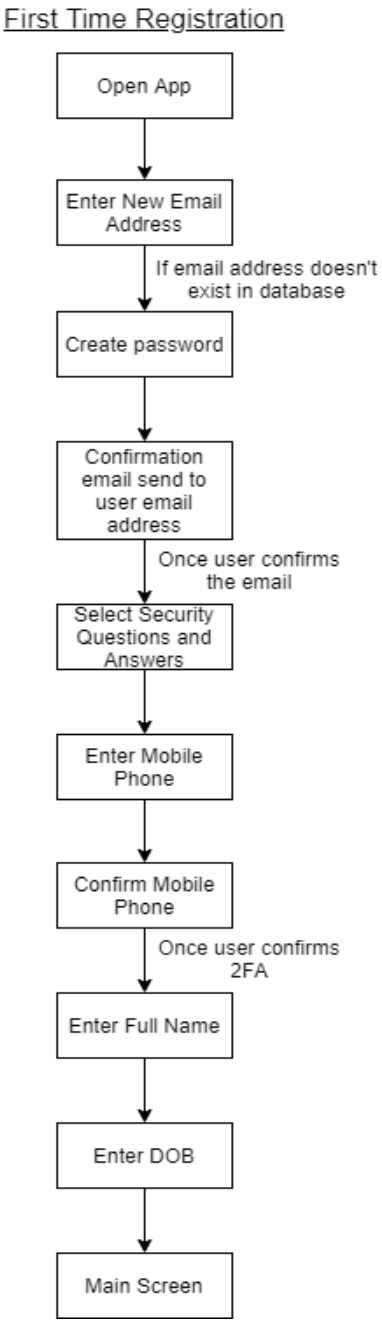
a. The user enters their NHS number and continues normally
b. The user enters their full names and continues normally

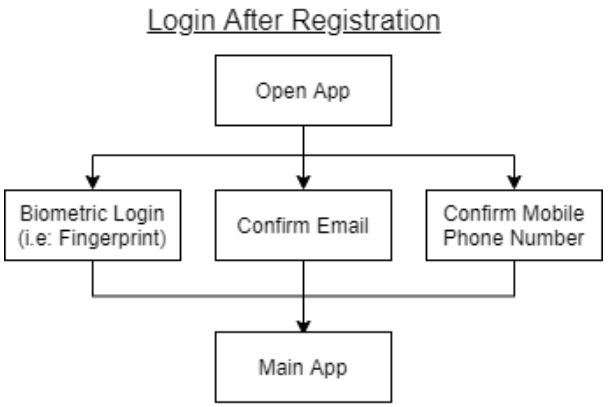
Once one or the other has been completed, the user will be asked for their date of birth (dd/mm/yyyy) then they will enter the postcode of their doctors.

Finally, the user accepts the terms of service and responds to whether or not they consent to share their data that will be used for research, and reach the Home Screen.

The Simple flowchart on the left below shows the registration system this project will be implementing for the app.

Once the user is registered, for future logins, the user will be able to log in and access the app via fingerprint or however the user would unlock their mobile device like the right flowchart below.





More information on the login system to be implemented is shown in 2.1

The first research was done by downloading the current NHS app and attempting to login to decide which features are inefficient and which are well implemented, to determine the features to include in the new login system. The current NHS app itself was used as the basis to understand what is effective and what must be changed in the new app.

As not every member of the team was confident with utilising Kotlin, for research, a few websites were visited and the URLs are below:

1. https://kotlinlang.org/docs/reference/
2. https://developer.android.com/kotlin
3. https://devdocs.io/kotlin/

Similar to Kotlin, a few members were not confident with Swift and so multiple Swift related websites were visited, as shown below:

1. https://developer.apple.com/swift/
2. https://swift.org/documentation/
3. https://swiftdoc.org/

Research on similar systems was also undertaken and are outlined below:

In many current bank apps (Lloyds, HSBC etc), the first time the user downloads the app to log in and register their device, the user enters their details and confirms their security code. After the device is registered, the user can log in by just scanning their fingerprint(or however they would unlock their mobile device) making it much easier to login in future attempts.

Lloyds has recently introduced ‘Strong Customer Authentication’ which is an EU regulation that provides customers with more protection when online banking and shopping. This benefits users as it makes it harder for fraudsters to target accounts.

A not useful feature of some bank apps is the requirement of the user to have a password on their phone without which they do not allow to open the app. Many people do not want a password on their phone and the app would be secure even if it required a password only to open the app.

The IOS Health App is also extremely successful as it is easily accessible and very user-friendly. Although currently nothing can be utilised in the NHS app from the Health App, in the future, there could be collaborations between both apps.

The EU-Exit App also has an extremely similar login system to the current NHS app login system, yet is much more successful which is due to the fact that they do not have many unnecessary pages but use 4 pages with all relevant information contained in each page. This was taken into account when deciding what to implement and what to exclude for the new implementation of the login system. In spite of its proper use regarding paging, the app, from a consumer perspective, asks too many questions and still takes too long to complete.

2.1 Functional requirements

As we are working on a login function, there will be two main functions, the first will apply for when a user is logging in for the first time and the second is when the user is logging in after they have completed the registration during the first time they registered.

If this is the first time the user opens the application, they will need to register to ensure their identity and allow for a smoother login the next time they decide to use the application. Due to this, the registration has more steps to ensure that all information needed is covered.

To minimise the number of clicks and redirection, we will implement the login/registration page such that the user can input their details in fewer pages. For example, they can log in with their email and password on one page instead of how the app currently operates where the user inputs their email, clicks on a button to then input their password and then login - this will increase the efficiency of the user's inputting their data and gaining access.

FR 2.1.1 Registration of a user

Users can input their details, take a picture of their ID, take a video of themselves to send to the NHS digital team to confirm their identity so they can access their login.

This is a high priority as without registering, the user can not use or log in to the app.

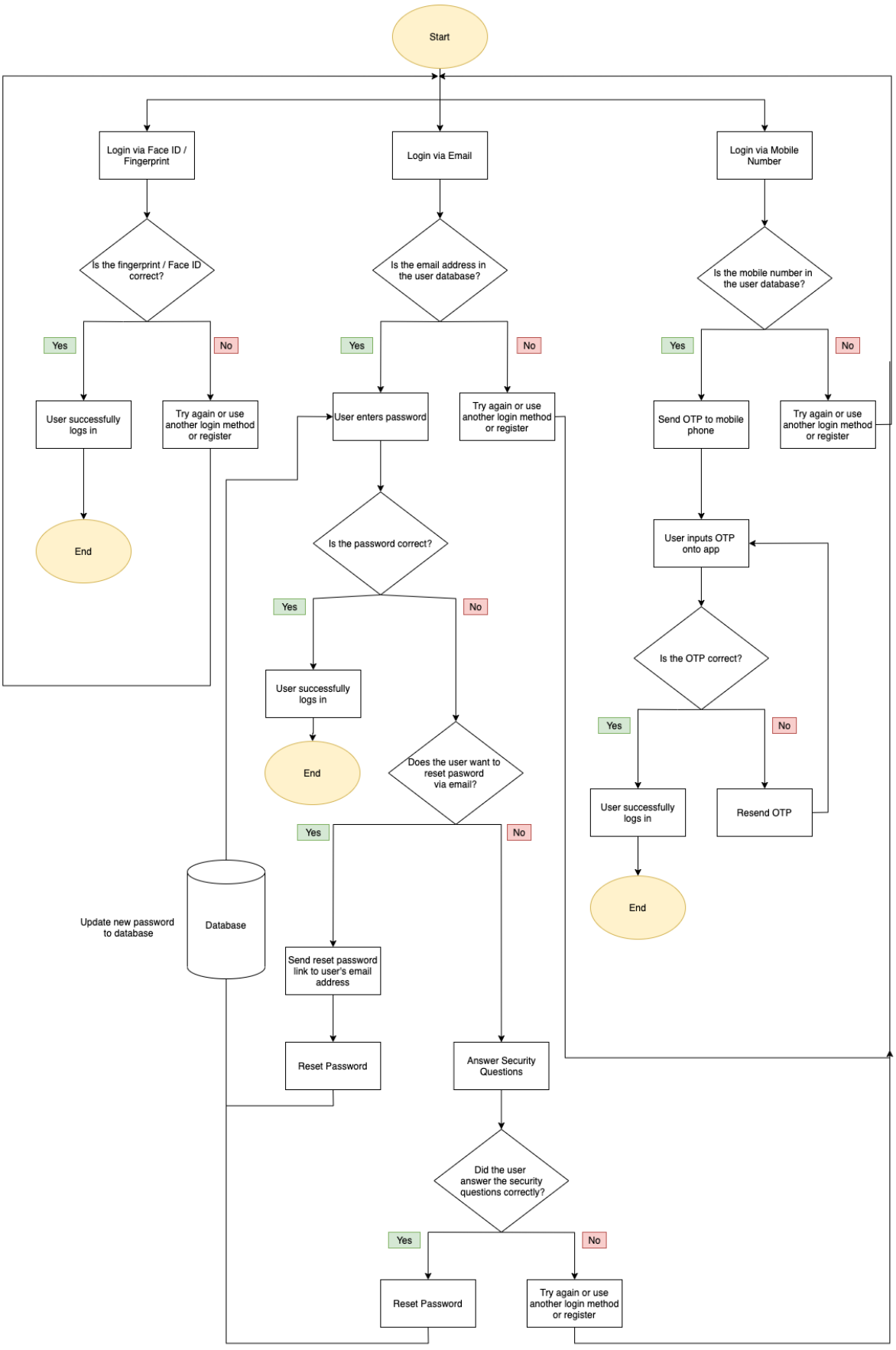
The app must have inputs for all the details required and the user must input all of their details as stated. The details must be accurate and correct. For example, the picture of the id must fully fit in the picture sent and the video must clearly show all of the user's face. The biometric authentication must meet the FIDO standard. For example, when the user sends their id and a video of themselves to NHS digital, someone from NHS digital will approve of the user, creating a key and later will attach this key to the user's biometric. Next time they log in the corresponding key will be selected, granting the user access to the app. The app should have validation of all inputs, informing the user in case they forget to input vital details. The registration feature could have integration with iOS devices, for example, to use on the health app which could record the user's BMI. this information could be updated in their medical records so doctors in the future could see their activity/weight changes.

The user registering does not depend on any other functional requirement. It is what the login will depend on.

If the user has correctly input their personal details and has sent a clear picture of their ID and a video to the NHS digital team, they should be able to proceed onwards from the login page. (i.e. a notification should appear, welcoming the user.)

Exception handling may include halting the program if the user misses out a text box to fill in. The user may take a picture of an invalid id, i.e. cut off parts of the id that is necessary for the verification on NHS digital side.

The login system for returning users has been described in the flowchart below:


Start
Login via Face ID / Fingerprint
Login via Email
Login via Mobile Number
Is the fingerprint / Face ID correct?
Is the email address in the user database?
Is the mobile number in the user database?
Yes
No
Yes
No
Yes
No
User successfully logs in
Try again or use another login method or register
User enters password
Try again or use another login method or register
Send OTP to mobile phone
Try again or use another login method or register
End
Is the password correct?
User inputs OTP onto app
Yes
No
Is the OTP correct?
User successfully logs in
End
Does the user want to reset pasword via email?
Yes
No
User successfully logs in
Resend OTP
End
Update new password to database
Database
Send reset password link to user's email address
Reset Password
Answer Security Questions
Did the user answer the security questions correctly?
Yes
No
Reset Password
Try again or use another login method or register

FR 2.1.2 Existing User Login - Fingerprint/ Face ID

Users can provide their fingerprint or Face ID to login and access data.

This is a medium priority as, if the user does not have the means to provide fingerprint/ face ID, they can log in using the Email ID or mobile number.

The app must have all the fingerprint/ FaceID data saved in its database. The details must be correct and complete to make it securely stores all data, only then can it check whether a user with those particular fingerprints exists. The details must be accurate to make sure that a user is linked to their fingerprint and not to that of other users in the database. The user should be able to log in via their fingerprint quickly and could add multiple fingerprints if they wish. Once the user has scanned their finger /face, the corresponding (public) key will be found and will grant the user access. After a successful scan, the app should leave login and go to the main part of the app.

The user registration (FR 1.1) is what the login will depend on. The main dependencies of this involve the user initially inputting the correct fingerprint/ face ID during registration and the system saving this information accurately so that the user will have a smoother login.

If the user has correctly logged in using their fingerprints, the app needs no further proof of identity and the user is successfully redirected to the main app.

Exception handling may include halting the program if the face ID/fingerprint recognition is incorrect multiple times. In that case, the user must be asked to log in using a different method.

FR 2.1.3 Existing User Login - Email

Users can enter Email ID and Password to login and access data.

This is a medium priority as, if the user does not remember their email ID or password, they can log in using fingerprint/faceID or mobile number.

The app must have all the Email ID and passwords data saved in its database correctly. The details must be correct and complete to make it securely stores all data, only then can it check whether that email ID has been registered along with the correctly linked password. The details must be accurate to make sure that an Email ID is stored in the database with the correct passwords and there is no overlapping between different users. The user should be able to login with the correct email and password, after this, the app should leave login and go to the main part of the app.

The user registration (FR 1.1) is what the login will depend on. The main dependencies of this involve the user initially inputting the correct email ID and password during registration and the system saving this information accurately so that the user will have a smoother login.

If the user has correctly logged in using their Email ID and password, the app needs no further proof of identity and the user is successfully redirected to the main app.

Exception handling may include halting the program if the password entered is incorrect. In that case, the user must be asked to reset their password either by sending a reset password link to their email ID or by asking security questions that the user set up during registration.

FR 2.1.4 Existing User Login - Mobile Number

Users can enter their mobile number (that they registered with) and an OTP sent to that number to log in and access data.

This is a medium priority as, if the user does not remember their mobile number, they can log in using fingerprint/faceID or email address.

The app must have all the mobile numbers data saved in its database during registration correctly. The details must be correct and complete to make it securely stores all data, only then can it check whether that mobile has been registered before. The details must be accurate to make sure that a mobile phone is associated with the correct user and that the OTP sent matches the OTP entered by the user. If the user has not received an OTP, the user should have the option to send another OTP to their mobile phone. If the user still is unable to receive the OTP via text, there could be an option to allow the user to receive a call, saying the code through the phone instead of via text.

The user registration (FR 1.1) is what the login will depend on. The main dependencies of this involve the user initially inputting the correct mobile number during registration and the system saving this information accurately so that the user will have a smoother login.

If the user has correctly logged in using their mobile number and entered the correct OTP, the app needs no further proof of identity and the user is successfully redirected to the main app.

Exception handling may include halting the program if OTP is entered incorrectly, The OTP can be requested again any number of times but with the waiting time increasing exponentially by each request (using the equation 2n where n is the number of attempts starting from n = 0).

2.2 Non-functional requirements

Type

The new login system that we will implement must have strong security for accessing patient information and an ethical requirement of ensuring that the user's registered and login details remain encrypted and protected from all other users and members of staff. GDPR is an important aspect of the NHS to ensure patient records are kept confidential, therefore it is essential we carry this through to the app.

The space requirement for the app currently (as said on the google play app store) is 130mb. As we are only making the login page, and most other functionality will remain the same, the login page should not exceed 130mb.

Metrics

The user should be able to fully input all their details to register correctly within 5-10 minutes. Moreover, videos have to be sent to the NHS digital team to verify the user's identity, the complete response time for registering a user should be within 2 hours (as previously stated on the app.)

The user should be able to correctly login to the app via email with a response time of < 1 second, 90% of the time.

The user should be able to correctly login to the app via mobile number with a response time of < 1 second, 90% of the time.

The user should be able to correctly login to the app via a fingerprint/face ID with a response time of < half a second, 90% of the time.

These fast response times are required to gain quick access to the main part of the app.

Security

The user who possesses the NHS account will be allowed to change their personal details (i.e the details they registered with). No one else will be allowed to change these details. However, upon verification of the user and request, the NHS digital tech support team should be able to change a user's details, if, for example, a user contacts the support team requesting to change their email address on the app. Overall, only the user will be allowed to change their personal details, and occasionally, if there is an issue for the user, the NHS Digital technical support team will also be allowed access.

Constraints

To remain consistent, we will implement the NHS app by selecting the same (lowest) operating system compatibility as the current NHS app has on the app stores. This will ensure that all other features we do not implement can be easily added if needed. This is a constraint if certain users have an older mobile and older mobile operating system than what we are using, for example, older than Android 5 lollipop.

Another constraint may be the number of users that can use the login system at a given time - the servers may overload if too many users log in at the same time which will result in a lag and a decrease in speed of the app.

Scalability

The app must be able to cater to a lot of users at a given time and integrate well with the mobile device‘s operating system, especially when using regularly the fingerprint and pin code stored used on the phone. As the number of users potentially increases, our app must work as efficiently without any additional introduced lag or change in functionality.

Usability

The app must be very user friendly so that users of all demographics are able to navigate through the app with minimal clicks and redirections. There will be a consistent design through the login/registration system using the NHS logo and traditional blue to highlight reliability and familiarity.

2.3 Risks and Issues

Category	1	2	3	4	5
Risk levels	Very low	Low	Medium	High	Very High

Covid-19 - **5**

With the current situation in the world, Covid-19 has certainly changed the way of life for everyone, including us. With this in mind, we put the risk at the highest category 5 as we have to take the precautions necessary and at the same time follow the guidelines given by the government. The impact of this is substantial as many things such as meetings cannot be conducted physically, for the time being, thus needing us to adapt and overcome the obstacles that could arise from online communication. The health and well-being of our team members are also priorities when discussing this as it will greatly impede our progress if there are members who require time off due to Covid-19 or any other severe illness.

Mental Health - **4**

With the current situation in the world, morality and mental state can also play quite a big factor when working on this project. We will do our best to keep the mental health of our team at a healthy level, making sure that everyone is coping and handling the changes well. We have placed mental health as a huge risk that could cause delays and issues in the progress of the development as traits such as demotivation and unproductiveness are common when a person is experiencing low mental health.

Technical barriers - **4**

Several technical barriers that could become a problem in the development stage of this project. One of the main barriers that we will face is creating the application so that it will work for both the Android and IOS platform. This is due to the fact only a few of us have experience with building mobile applications, thus we need to take more time and resources to make sure that the back-end coding is understandable, clear and manageable when it is handed over to the client. In regards with back-end code, there are many features in this application we would want to implement but might not be able to due to factors such as time complexity of the feature and prioritising the foundations of the application. The complex features range from retina scanning to syncing the finger sensor to the application if the user's mobile phone has it available.

Tight schedules - **3**

Our schedules can play a factor in the project not being finished on time, especially with other assignments and commitments our members might have. However we put this risk level as 3, which is a moderate risk level as even with the potential schedule clashes and unexpected events that might happen, we are focused and are highly confident in providing a solid foundation for the applications with a clean back-end code. This time constraint will cause more problems when we want to try to implement the more complex functions into the application after the foundation is completed.

Malicious activities - 3

There are several malicious activities that we need to take account of when building this application. Since there is a substantial amount of sensitive information involved in the application, we have to cover all the risk at each layer of the Mobile Security Stack. This includes:

- Infrastructure: This includes the interception of data over the air as mobile data has the same type of problems as laptops.
- Hardware: This concerns baseband layer attacks that could happen to the user's phone. Have to take account of memory corruption defects in the firmware used to root the device.
- OS: Taking account of jailbroken IOS or Android phones, as when a phone is jailbroken, it exploits the defects in the kernel code or vendor-supplied system code
- Application: Have to make sure that our application has minimal vulnerabilities and high protection from malicious code as our application will be accessing the device sensors. In essence, we have to make sure that our application cannot be abused for location tracking and personal data on the device.

With these points, we have to minimise as many vulnerabilities as possible so it is going to also be a high priority. However, even with all the testing, there will still be certain vulnerabilities that might have not been accounted for, thus this risk might hinder the development and is placed at moderate risk.

Poor communications - 2

Communication is always an important factor to have down in a team, members of the team should be dedicated and are in sync with all the tasks we individually need to do to contribute, thus this helps put the risk factor at a below moderate level. The times where communications could be an issue could be in several scenarios ranging from WiFi problems (As meetings have to be online) to members schedules could have sudden changes which can cause a clash in meeting times. Clear and precise communication between the client is also an extremely important factor that is vital to keep consistent and efficient progress on the application. Any misunderstanding can cause the application to head towards the wrong direction, leading to wasted time and effort from our team.

Budget changes - 1

Since the project is heavily reliant on our skills and expertise in mobile application development, there is not a glaring requirement to have a big budget to complete this project. However, if there are certain features the client would desire in the application that might increase the cost, then this is where the issue might arise if the budget is low.

End-user engagement- 1

This concerns the satisfaction of the users with the functions in the application or any of the future updates that are planned for it. This can be measured usually by the ratings on the app store, but methods such as tracking the monthly usage of the application and allowing the users to create constructive reports on glitches and improvements they want to see in the application. We have placed this risk as a relatively low one as there is only one NHS application that every person in the UK can use. Even with this, we still want to maximise the application's usage to ensure the safety and health of certain areas and allow users to stay up-to-date with the current status of the situation.

3.1 Development approach

For this project, the development approach chosen is Scrum. Scrum is a subset of the Agile software development methodologies. For more information, visit the official Scrum website: https://www.scrum.org/

3.1.1 Implementation

Scrum is based mainly on its iterations, which repeats until the product requirements have been implemented. Each iteration is called a “Sprint”. During the development, the team will meet before the start of a sprint, this is called “Sprint planning”. In this meeting, the client explains to the team the most valued requirements to be delivered to the customer at the end of the sprint. As already said, the client has the product vision and therefore he/she prioritizes the requirements by order of more business value for the customer. In the case where the client is not present, the internal meeting is held to discuss concerns and difficulties faced in the previous sprints.

3.1.2 Roles

Client

The client has the product vision, the knowledge about all the requirements and the business value of each one for the customer. The client has a very clear vision of the final product and how it should work. This knowledge should be pass onto the team to develop this vision

Team

The team, with 6 members, with the mission to build the product. It’s a self-organized team with all the skills and knowledge needed to develop the product. Each team member must be willing to learn any skills that the team isn't equipped with.

Scrum Master

Appointed member of the team with excellent knowledge of Scrum, his/her objective is to help and support the team and the product owner in applying Scrum. He/she will help answer any questions about the use of Scrum and encourage the team to stick to it. This will help the team stay on track of developing the project.

Communications Manager

Appointed member of the team who is a confident communicator and presenter, his/her objective is to help and support the team with external communications which includes partners and the client.

3.1.3 Benefits of scrum

Embrace of change

Scrum prioritizes delivering incremental business value to the customer. It's more flexible in requirements gathering and it allows us to start the development phase earlierAll the requirements must be well defined, but they all don't need to be defined at the start of the project.

Customer feedback

With iterations of the software present to clients, feedback can be received in between sprints. This feedback is crucial as it provides the development team with priorities of features to implement for the following sprints.

Reduces the risk

During each sprint planning, the team can solve any question about the requirements explained by the client. When the sprint is finished, a prototype must be delivered to the customer with new functionalities or changes introduced into the product. When building the product by increments, inspection and adaptation of the product by the customer are done at least once in each sprint, increasing the control of risks, as the development time can be broken down into shorter periods.

3.2 Project Schedule

The Current plan* is displayed below in the form of a table:

Date	Name	Details
12/11/20	Requirement specification	Present client with the requirement specification
13/11/20	Start of Sprint 1	First Sprint planning
13/12/20	Start of Sprint 2	Second Sprint planning
13/01/21	Start of Sprint 3	Third Sprint planning
28/01/21	Test plan report	Finalize test plan
13/02/21	Start of Sprint 4	Final Sprint planning
14/03/21	Product finalization	Ensure product ready to release
18/03/21	Final Product	Final product handover and presentation
07/05/21	Internal group reflection report	

*Note: Dates are to be finalized.