Making a Infection Tracking and Reporting System.

TO DO LIST:

Discuss how contact tracing system will work at a high level

Need to discuss how the testing centre has interacts with our system and how to link test results with the user’s phone.

Requirements:

Monitor close spatial interactions between members using proximity of mobile phones.

Allow users to self report for possible infections. This individual can then seek Medical tests for confirmation.

Allow Medical Professionals to associate positive tests with a user’s phone which either confirms or removes a self report.

Notify individuals if they have been in close proximity with confirmed infections.

Feed anonymised infections statistics to UK dashboard aggregated daily and spatially per 10000 people

Levels: Red-> High risk of infections as been in contact with someone who is confirmed

Amber -> Possible infections as been in contact with someone who is has self reported but not confirmed

Green -> No Confirmed or self reported cases which are likely to have been transmitted that have been in contact with the individual

ASSUMPTIONS:

Takes at least 3 days from initial time of infection to become infectious. Infection can spread from a single individual at 1 hop every 3 days. If person x is infected on day 1, they can infect others from day 4 onwards.

Person should only receive an amber or red status due to infections reported or confirmed within the last 14 days and if they are a maximum of five hops from the source. If an infection is reported or confirmed on day d, the relevant notification cone is from d – 4 . (Everyone in contact with the person after day d – 4 is given red or yellow if met with this person). An individual’s status should be red if they are in the cone of any confirmed cases and orange if they are within the cone of any self reported cases. ( red for red, orange for orange).

FR’s and NFR’s:

System needs to integrate with Apple and Android

Use Bluetooth

Use a kernel service

Only signed applications approved and signed by the vendor will be able to access the kernel service

Applications register 1024 bytes with the kernel service. This will be exchanged with another phone.

Periodically advertises it’s presence using local Bluetooth.

Also monitors local broadcasts.

If two devices, detect they are in close proximity for more than a pre-set time-period, an interaction is said to have happened.

During the event, the two phones exchange data currently, recording time location and data.

Two phones only register each other at most once per 24 hours.

Applications are notified with batches of new interactions on a minute by minute granularity. Information reported is location and raw time along with interaction data.

Another NFR, is that our system must integrate with the REST API.

System needs to be robust against users who misreport infections.

We do not need to worry about the thresholds for space and time that generate a notification.

We need to minimise data leakage to central servers, protecting users identity as much as possible, and a stated data minimisation policy will be a condition of app approval.

We are responsible for development, deployment and management of all back end systems and servers.