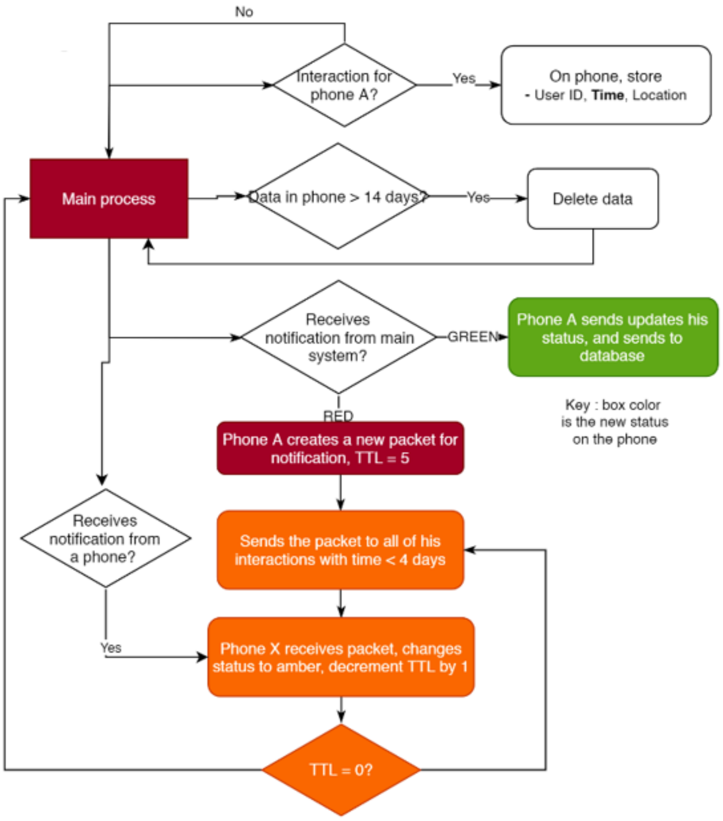
## Overview of the system


No
Interaction for phone A?
Yes
On phone, store
- User ID, Time, Location
Main process
Data in phone > 14 days?
Yes
Delete data
Receives notification from main system?
GREEN
Phone A sends updates his status, and sends to database
Key : box color is the new status on the phone
RED
Phone A creates a new packet for notification, TTL = 5
Receives notification from a phone?
Sends the packet to all of his interactions with time < 4 days
Yes
Phone X receives packet, changes status to amber, decrement TTL by 1
TTL = 0?

1. Interaction tracking. When users are in range, packets of data are sent through Bluetooth and stored on the phone. This data is backed up to the cloud.
2. Updating user status. When a status is changed, all user's statuses who have been in contact are updated using a TTL feature which decrements on every transmission, effectively mirroring the transmission cone.
3. Allowing medical professionals to confirm positive tests and send these to the user. This is done through an NHS integrated software which allows automatic updating of status.
4. Notify users that they have been in contact with an infected user. A set of high-speed servers send notifications once a user has a confirmed case and when a user has had an interaction with an infected or potentially infected user.
5. Feed infection statistics to the UK dashboard. These statistics are fed through specific locational databases and sent through the REST API.  This allows an efficient system - local databases can be mapped to the regions specified by the UK dashboard.

## Meeting Difficult NFRs

**Availability and Reliability:** 99.99% successful delivery rate is achieved by increasing the reliability of the system through backing up data on both local storage and central database, and each phone having a cloud backup. In the central storage, each level in the 3-tier database backs up each other. Secondly, there is buffering for any communication between server and user application to prevent loss of data/notification in absence of Internet.

**Scale:** Central server is a scalable unit so that the server can process various reports and interaction data and propagate the notification over 5 hops within 1 hour. In the 3-tier database, data storage is split up by locations. Level 1 stores local, level 2 regional, and level 3 national data; this prevents overloading of the database from request congestion and allows the system to handle the large user base.

**Privacy and Security:** Interaction data is stored on user devices and only sent to central server when there is a change in the status. All interaction data older than 14 days is deleted to ensure the privacy of users. User IDs are changed every 4 to 5 days for further protection. Various firewalls are in place to avoid data breaches and if a request to harm the database is detected, the system can stop the request through several security servers which are in place. Only the most recent four days are backed up to the cloud to minimise data retention and for the purpose of allowing users to get back on track if they lose or damage their phones.