(IBM-ish client Brief)

- Version 1 : 2020-06-01–8:40
- Initial release

Context

NHSY is a unit that has a mandate to deliver technological solutions to challenges faced within the NHS and across general health-care in the UK. Our particular area of responsibility is in driving transformation of healthcare through the use of information technology and data, and also in managing the impact and potential concerns that might arise through the use of new technology.

Our in-house team has significant expertise on the development and delivery of automation and data-analysis technology within traditional healthcare contexts such as hospitalas and doctors surgeries. Where necessary we contract out to experts in other fields, particularly where we need rapid solutions in areas where there is less in-house expertise.

System Overview

NHSY is seeking proposals to develop an infection tracking and reporting system, which uses mobile phones to implement tracking and contact tracing for infectious diseases. In the future this may become a general system, but right now the clear and pressing demand is to monitor COVID19.

The core high-level requirements of this system are:

- R1 : Monitor close spatial interactions between members of the population using proximity of mobile phones.
- R2 : Allow individuals to self-report suspected infections using their own phone. The individual can then seek a medical test through a variety of providers to confirm whether or not they are infected.
- R3 : Allow medical professionals and certified testing services to associate confirmed positive tests with an individual's phone. A positive test confirms an individual's self-reported infection, while a negative test cancels an individuals self-report.
- R4 : Notify individuals when they have recently been in close proximity with confirmed infections. The notification should provide a green, amber, or red status for each individual:

  - Red : Individual is at high risk of infection due to direct or transitive contact with someone *known* to have been infected. Anyone with red status should self-isolate and immediately seek testing.
  - Amber : Individual is at risk of infection due to direct or transitive contact with someone who suspects (self-reports) they have been infected. Anyone with amber status should apply social distancing according to current national policy, and be watchful for symptoms.
  - Green : Currently there are no confirmed or self-reported cases which are likely to have been transmitted to the individual. A green status means people can follow the current default national guidelines.
- R5 : Feed anonymised infection statistics into the UK's Covid-19 data dashboard, aggregated daily in time and spatially to regions of approximately 10000 people.

The addition of low-cost/risk high-value features is welcomed. Extensibility points for future features is also of value. However, the bid will primarily be awarded based on the ability to deliver the core functionality on time.

Notification algorithm

Part of the reason for tendering out the design of the system is that NHSY currently has a lack of expertise in the design of large-scale distributed systems. We are expecting the bid to identify how the core requirements can be met, while also meeting the constraints discussed below. In particular, your bid should include a discussion of how your contact tracing system works at a high-level for non-technical executives. This is expected to be reflected in the designs and models that our technical team have asked for.

Our working assumption is that a person takes at least 72 hours (3 days) from the initial time of infection to become infectious. Current evidence suggests longer time-scales, but a precautionary approach is being taken. As a consequence, our operational model is that an infection can spread from a single individual at one "hop" every three days: if an individual `x` is infected on day 1, then they have a chance of infecting everyone they interact with on day 4 and on all following days. Anyone infected on day 4 then has a chance of infecting people they interact with on day 7, and so on.

Another way of putting this is that the infection can spread through the social interaction graph at one hop every 3 days. For any given individual `x` on day `d`, there is a "cone" of people they might have transmitted the infection to. The cone has size 1 on day `d` (it's just the person `x`), and grows over time. This cone first grows on day `d+3`, but may also increase on day `d+4` due to the people that individual `x` met on day `d+1`. On day `d+7` the cone starts growing faster due to any secondary infections from day `d+3`.

Over time the cone of exposed individuals grows larger and larger, but fortunately not every contact will result in infection. However, to manage the number of notifications, particularly if there is a second spike or other high intensity infection event, any given self-reported or confirmed case is limited in the time and number of social hops. While this may later be turned into a configurable parameter, for this initial release it will be fixed. So a 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 5 direct interactions (social hops) from the source.

The longest incubation time is assumed to be 7 days, so if an infection is reported or confirmed on day `d`, then the relevant notification cone is rooted at day `d-4` (assuming 3 days of non-infectious time at the start).)

Note that a given person may be within the cones defined by multiple self-reported or confirmed infections. Any secondary infections form the root of new cones, so it is quite likely that a person may end up both within the cone of the original infection, and also the cone of a secondary infection caused by the original. Different infections from separate sources are also likely to spread and overlap, particularly during local outbreaks. An individual's status should be red if they are within the cone of any confirmed infection, and orange if they are within the cone of any self-reported infection. The red status takes precedence over orange.

Your company has been invited to take part in this bid due to your reputation for expertise in computer science and mathematics, as the in-house design team mainly deals with traditional back-end development. So an aspect of the solution we are particularly interested in is *how* the contact tracing method will work, and how the various requirements and constraints will be balanced. We recognise that these ideas and approaches may be commercially sensitive, so details of the solution will be considered commercially confidential, and not shared with others outside of the bidding process.

Hardware and platforms

To balance rollout speed versus population coverage, the system is required to initially support just two mobile-phone eco-systems: iOS and Android.

An NHSY technical team is already negotiating with Apple, Google, and key smartphone providers to establish proximity APIs. The detailed design and operation of these APIs is not yet stabilised, though the following functionality has been agreed:

- Proximity detection will use blue-tooth.
- The detection service will be a kernel service, in order to minimise power consumption, and also manage privacy concerns around data leakage.

- Only signed applications approved and signed by the OS vendor will be able to access the kernel service.
- Applications register arbitrary data of up to 1024 bytes with the kernel service. This data will be exchanged with another phone when an interaction event occurs.
- The kernel service periodically advertises it's presence using a local bluetooth broadcast.
- The service also monitors for local broadcasts from other devices.
- When two devices detect they are in close proximity for more than a pre-set time-period, then an interaction is considered to have happened.
- During the interaction event, the two phones exchange the data currently associated with each phone, and the service records the time, location, and data exchanged.
- Two phones will only register each other at most once per 24 hours. Repeated proximity within the day will not lead to more reported interaction events.
- Applications are notified with batches of new interaction events on a minute-by-minute granularity. The information reported to the app is the raw time and location as captured from GPS and internal clock, and the interaction data received.

The thresholds for proximity in space and time that generate a notification are being set independently by a team of epidimiologists and medical professionals, and will be fixed within the kernel service.

It is up to the mobile-phone application to manage post-processing of data to minimise data-leakage to central servers. Applications should attempt to protect and hide user's identity as much as possible, and a stated data minimisation policy will be a condition of application approval and signing by phone vendors.

The Android and iOS applications will be developed by existing in-house teams with expertise in mobile development, user-interface design, and testing. These teams expect to be given an interface to be used to talk to the back-end systems outside the phone. This interface could either be a web API or a loadable code module, though a loadable module would also need to pass application approval. The app teams will also implement any required local computation and data storage, following requirements provided by the successful bidder once the contract is awarded.

The development, deployment, and management of all back-end systems and servers will be the responsibility of your proposed solution. Any reasonable technology stack can be used, with a preference for those which reduce execution risk and can scale to a national level.

The UK's COVID-19 data dashboard is an existing service which integrates data-feeds from nation-wide sources. Due to existing data-integrity and security policies, data can only be uploaded to the dashboard through a pre-defined REST API, and can only be accessed from nominated IP addresses using client-authenticated SSL keys. Further details of the REST API are available at XXXX (*ignored for the purposes of this assessment*).

Medical testing

Medical testing will be performed in a number of different ways at multiple venues, including:

- Hospitals
- Drive-through testing clinics
- Mail-order testing services
- Doctor's surgeries

Some of these testing venues will not be operated by NHS staff, nor will they occurr on NHS premises. Some testing services are manual, while others are highly automated. However, all staff and automated services performing tests will have valid login credentials for the national NHS user authentication system. Due to security concerns, none of your system's components can be located on existing NHS infrastructure or servers. However, OAuth access delegation to the NHS authentication servers is available over the internet from any location.

Note that some tests will be performed while the individual is present, while others will be performed hours later, or at a remote site from the individual. Because this notification system is based around the tested person's phone, there must be some way of associating the user's phone with the eventual test-result. Be aware that different testing systems will also use quite different mechanisms to inform *people* about test results, ranging from text, to email, to verbal confirmation; this is a seperate interaction to the testing centre's interaction with your system.

In the ideal case, positive medical confirmations can be submitted to the system without any action on the part of the person tested. This avoids the problem of positive tests being lost due to the tested person being unwilling or unable to perform an action on their phone.

Privacy and Security

Balancing privacy versus efficacy is an important tradeoff, and the core function of allowing contact tracing and notification must not be impeded. However, maximising privacy and minimising data-retention is important to ensure that the public has confidence in the system, and trusts that data will not be used for secondary purposes. While infections may last an unknown amount of time,

in order to limit data retention the system should not maintain interaction information longer than is necessary to process notifications. It should not be possible to identify which phones have reported infections (whether self-reported or medically) after 4 weeks.

The possibility of malicious actors who mis-report infections is also a concern, with reasons for mis-reporting ranging from casual maliciousness to concerted attempts to skew local statistics. Regardless of why they choose to mis-report, the system should attempt to be robust against attempts to over-report infections. The system should explicitly seperate self-reporting from medically confirmed reports, so that separate statistics can be maintained for confirmed versus suspected cases, and also so that notifications can be weighted according to confidence in the source.

NHSY is particularly interested in this privacy-functionality-security tradeof, and the welcome bids that take innovative approaches to balancing functionality versus privacy and security. Proposals that minimise or encrypt server-side data are welcomed. Proposals with a strong and credible privacy story that can be communicated to the public are also encouraged.

Scale

The system is intended to scale to penetration of 50%-80% of UK mobile-phone users, in all locations from rural areas to dense metropolitan areas.

Self-reporting

Self-reporting of possible infections is anticipated to be around 5,000 to 10,000 per day on average, regardless of the actual prevalance of COVID-19 in the population. The system should be able to scale to a peak of 500,000 self-reports per day, though this is an extreme case. During outbreaks the geographical distribution of self-reports is likely to vary significantly, with the number of correct self-diagnoses accompanied by many incorrect self-assessments due to the known outbreak.

Medical reporting

The number of medical tests is expected to reach a sustained average of 200,000 tests per day, with a peak of 500,000 tests per day. Lockdown policy will be adapted in order to target no more than 500 new confirmed cases per day. However, this rate will increase and decrease in response to societal, environmental, and other factors, with a worst-case peak anticipated at 50,000 confirmed cases per day.

Availability and Reliability

It is important that the system achieves high-levels of availability and reliability. The system should always be able to propagate warnings within 6 hours of the relevant self-report or confirmed report. Lower notification latency is preferred, with a target of 1 hour from report to all contacts being notified.

This initial system is expected to operate during the containment phase, with manual contact tracing taking precedence if the prevalance drops low enough to support an elimination scenario. As a consequence, a 99.99% successful delivery rate for medically confirmed notifications is acceptable.

The system must be able to track interactions in the temporary absence of internet connectivity. One scenario of particular concern is interactions that happen in enclosed areas with no connectivity, such as underground trains or buildings in wifi/mobile deadspots. Interactions in such areas are particularly important due to the density of people and lack of airflow, so interactions should still be tracked, then reported later once connectivity becomes available.

Timelines

The execution timeline is important, as the sooner the system can be rolled out, the greater the positive effect will be. Our goal would be to have the system rolled out nationwide **8 weeks** from the contract being awarded. This must include all development, verification, and testing work. Due to the short timeline, we expect proposals to consider:

- Technology, implementation, and execution risk: low-risk approaches are preferred.
- Testing and deployment: how will the system be piloted or debugged; how will it be rolled out?
- Scaling: how will any infrastructure be scaled up in this time-frame? What are the expected performance requirements/constraints of the system when operating at a nation level?

Deliverables

Due to the current lockdown NHSY has changed it's standard bid procedure to accomodate remote working. Rather than the standard in-person presentation, we will accept 10 minute recorded presentations - unfortunately this will not allow for the standard Q&A session. Along with the presentation, each bid will be expected to provide a set of technical work-products which describe their design and architecture.

The required bid deliverables are:

Non-technical audience: - `NT/NT1-Pitch.mp4`: at most 10 minute recorded pitch in mp4 format. - `NT/NT2-Prospectus.pdf`: 1 page pdf prospectus, highlighting the main features of the design and why it is good - `NT/NT3-Method.pdf` : 1 page pdf description of the **high-level** approach to tracking interactions and delivering notifications.

Technical audience: - `T/T1-SysCtxtDiag.pdf` : System-Context diagram - `T/T2-UseCaseSelf.pdf` : Use-case for self-reporting a suspected infection - `T/T3-UseCaseMedical.pdf` : Use-case for medically reporting of a confirmed infection - `T/T4-ArchOverDiag.pdf` : Architectural overview diagram - `T/T5-DataModel.pdf` : Data model - `T/T6-CompMod.pdf` : Component Model

Organisational - `O/O1-Principles.md` : Organisational principles and processes used by the team. - `O/O2-Log.csv` : High-level log of interactions, discussions, and work.

Organisational deliverables

The non-technical and technical deliverables are self-describing, and should follow industry or your own in-house standards as appropriate.

The two organisational documents are required in order to fulfill the NHSY committment to the Kinder Contracts initiative. We support the goal of ending Corporate Value X, and so require documentation to demonstrate compliance.

Principles

This document should briefly describe the up-front methods used to organise and perform the work. The required sections are:

1. Idea creation: Methods used for idea-creation and selection.
2. Work allocation: approach used to allocate work to each team member.
3. Tools: Technologies, tools, or processes used to manage shared documents and work products.
4. Communication: how communication amongst the team is managed, including medium and aproximate frequency.
5. Sign-off: Process used to ensure that final documents have been prepared, checked, and that everyone has signed off on them.

No more than 100 words is expected per section, though there is no penalty for writing more.

We expect most companies will already have this to hand in some form as part of their standard operating procedures. Given the importance of setting up decision procedures when implementing a complex project in a short time period, a team that does not know how it organises itself *before* starting work will be considered weaker candidates for selection.

Log

The document should describe *approximately* who did what at a rough granularity of an hour. This is to help NHSY understand where teams spent their time – however the success of a bid will not be based on this information, and is only dependent on tracking and supplying this information.

Meta-notes

(This is not realy part of the brief)

How good does it need to be?

There is no such thing as the perfect solution, and any solution is going to contain some un-anticipated holes or weaknesses. This is true of bids created by large teams of experts, particularly if the system requested has not been seen before.

The goal of architecture is to avoid the big problems where possible. Does a particular interface need to ingest 1 billion records per second? Does a large data-base need to support 1 million transactions per second? Does each phone need to maintain a data-base of 1 billion records? Does it take four hours to process 1 hour of interactions? Do you need 1 server per 100 phones? Details can be sorted out if and when the contract is signed, and can be deferred to the programmers, database admins, and operations people. You're getting paid more than them because you can think about things at a higher-level.

This doesn't fit with the current COVID19 data/model

Most of this was written in early-mid May, and is a best approximation to requirements that *might* come out. It is inevitably very simplified, with a real RFP being signficantly longer. Try to solve the problem being stated here by the client, rather than tracking the real problem.

Some of the requirements are contradictory

Probably. This is why it is a request for proposals on a new system, rather than a request for bids to deliver existing systems. The client is not completely sure what they want, or what can be delivered, which is why they are asking external people to look at it. They want you to solve problems or contradictions in a reasonable way.

Why does the client care about our organisation?

They don't. This is purely for assessment, so that there is some assessable evidence about how things were organised, and that you co-operated as a group. Being able to work in groups is one of the intended learning outcomes of the workshop.

In particular, note that the time log will not be used to try to increase or decrease marks, either for teams or individuals. The main question is whether it was tracked.

It is *expected* that most people will receive full or close to full marks for organisational principles, as long as they are completely and look credible.