Department of Health & Social Care

From the office of Lord Bethell
Parliamentary Under Secretary of State for Innovation (Lords)
39 Victoria Street
London
SW1H 0EU
Tel: 020 7210 4850

By email to: Alan Woodward, Mark Ryan, Eerke Boiten

07 May 2020

Dear Alan,

I would like to thank you and your colleagues for taking the time to meet and discuss the new NHS COVID-19 app. It was a welcome opportunity for me to be able to hear your views and share the plans for this new app, in these unprecedented times. In this letter I hope to address some of the areas that were raised in our conversation.

Development of the App

Throughout the development of this app, we have been focused on our aim of protecting the NHS and saving lives. We believe this app can help do so, as part of a wider strategy of testing and traditional contact tracing. We would have liked to have been more transparent, right from the start. But a degree of secrecy has been necessary to allow the team the space to focus on product development at a serious pace.

We also had to ensure that any communications about the app did not pre-empt or undermine Government decisions on its use or relevance as part of a wider response to COVID-19. With a clear message to stay at home in order to protect the NHS and save lives, we have carefully refrained from open discussion about what the app might enable as restrictions are eased until such time that we were sure that it could work and could support other strands of our approach to managing COVID-19 as we come out of lock down. However, now is the time to be open, to make sure we get this right and I welcome meeting with you to discuss the app as we move towards the next stage. Today we published the Data Protection Impact Assessment of the first version of the app which is being piloted in the Isle of Wight and the app's source code which can be found on NHSX's Github page https://github.com/nhsx.

There were some key points I shared in our meeting, in response to your concerns and I want to share them here again with you in full.

Centralised vs Decentralised

Ensuring the privacy of users and security of their personal data is a priority for the NHS and UK Government, and this has been at the core of the app's development. When someone downloads the app it will keep an anonymous record of when they've been close to other users. Any sharing of that record if symptoms develop is voluntary and will be held on a secure NHS system.

The NHS is adopting a centralised model over a decentralised model. This is because it better supports the epidemiological model used by the Government in managing the disease. This will ensure that we are able to react quickly to changes in scientific advice and let people know rapidly if they are at risk from contracting coronavirus.

Our priority has been to maximise the public health value of the app to save lives, while preserving privacy, in line with the law.

People will always have a choice of whether to provide this information and no individual can be identified through the central app system.

International Comparisons

We are working with other countries and organisations to exchange ideas and like the UK, many countries are working on solutions that best support their local systems while taking into account cultural and societal differences. The design of the NHS COVID-19 app best supports the needs of the clinicians managing the virus in the UK.

The UK's approach is similar to that followed by Australia, France, Norway and Singapore among others. These countries have made similar technology choices (Bluetooth Low Energy), have a proximity cascade solution and use a centralised system.

Our understanding of how the virus works and how the technology works is developing. And, as it develops, if we think there is a better way of doing what we need to do, we can change. We are interested only in one thing, which is what works best for the people in this country.

Data and Privacy

I would like to turn to our discussion around data and privacy. The NHS COVID-19 app won't hold any personal information about users. It cannot access anyone's personal identity or any other information from a person's phone. The app does not collect location data either. And so it cannot be used to track people's location.

We have drawn on expertise from across the UK government and industry to review our design and to help us test and improve the app. We've involved experts from the National Cyber Security Centre to ensure it is safe and secure to use and they have provided a full technical paper on the app here https://www.ncsc.gov.uk/report/nhs-covid-19-app-privacy-security-report.

The privacy and security design carefully balance supporting the epidemiological model and the needs of clinicians who are managing the virus in the UK, with the individual privacy needs of users. NHSX systems won't build a social graph in the traditional sense, although they do have pairwise proximity events for anonymous identities. Using anonymous contact graphs analysis can help score encounters as more or less risky.

Any connectivity external to the app systems will be through privacy preserving gateways. The app back end runs on infrastructure separate to other NHS systems.

In future releases of the NHS COVID-19 App, people may be able to choose to provide the NHS with extra information about themselves to help us identify hotspots and trends. No decision has been taken as to whether this is useful or necessary. However, if a change is made to allow people to choose to submit more data it will:

1) be done transparently

2) always be optional

3) be done in the most privacy preserving way.

Data that app users have chosen to share with the NHS may be retained for research in the public interest, or by the NHS for planning and delivering services. This will be done in line with the law

and on the basis of the necessary approvals required by law. The data will only ever be used for NHS care, management, evaluation and research. Users will always be able to delete the app and associated data whenever they want in line with the Data Protection Act.

Transparency

I further shared my views and commitment to transparency, echoing Matthew Gould's commitment made to the Science and Technology committee on 28 April. Today we published the Data Protection Impact Assessment of the first version of the app along with the source code to allow public scrutiny and further discussion.

The Government is committed to transparency on what data is gathered and why, as well as the app's code and underlying algorithms, this will all be available publicly to enable scrutiny.

If we make any changes to how the app works over time, we will explain in plain English in our Privacy Notice why those changes were made and what they mean for users. Technical experts will also be able to review the published Data Protection Impact Assessment, which will be a live, iterative document that ensures any changes to processing are fully considered and addressed.

While moving at speed, we are following the same rules for information governance that underpin our day-to-day work. GDPR principles will be followed. Data sharing will always be proportionate, data collected minimised and users' privacy preserved in line with data protection law.

We have been discussing our plans with the Information Commissioner and the Centre for Data Ethics and Innovation, as well as with representatives from Understanding Patient Data and volunteers who provided a patient and public perspective. We set up an ethics advisory board for the app which includes members of the National Data Guardian's Panel and is chaired by Professor Sir Jonathan Montgomery from University College London who previously headed the Nuffield Council on Bioethics.

Once the pandemic is over, the data collected by the app will either be destroyed or fully re-anonymised and used for research purposes. This decision and the mechanisms for performing either outcome will be made transparently.

Many thanks again for the discussion.

Kind Regards,

LORD BETHELL