The NHS Test and Trace Service COVID-19

UNISON briefing on Data Privacy Rights

The NHS and Public Health England (PHE) Test and Trace Service is now live in England and there are variations in Wales[1], N. Ireland[2] and Scotland[3] who have set up similar services but using different digital and data systems.

The non - digital tracing part of the service will employ up to 25,000 contact tracers in the UK and the digital tracing service in England, once live, will use a digital app NHS COVID-19, developed by NHSX (the NHS digital and data sharing unit in charge of health and social care data integration and transformation).

The testing and tracing approach is likely to be pursued not just by central government and devolved parliaments but also by some individual employers in the workplace. UNISON supports the test and trace approach as part of the wider aim to limit the spread of the virus, help get people back to work and get the economy back on track.

However access and implementing the testing must be transparent, fair and equal for all workers and any personal data collected by employers or the government as part of that process must be responsible and proportionate and meet our data privacy rights.

This briefing sets out

- how the test and trace service is expected to work
- the implementation of test and trace in the workplace
- data and digital concerns
- drafting guidance for members/branches

The briefing is applicable to all devolved regions in principle but some concerns over data privacy are greater for England and Wales compared to Scotland and N. Ireland as they have adopted a more privacy friendly approach in their digital test and trace service.

[1] https://gov.wales/test-trace-protect-your-questions

[2] https://www.health-ni.gov.uk/sites/default/files/publications/health/Test-Trace-Protect-Support-Strategy.pdf

[3] https://www.gov.scot/binaries/content/documents/govscot/publications/advice-and-guidance/2020/05/coronavirus-covid-19-test-trace-isolate-support/documents/covid-19-test-trace-isolate-support-public-health-approach-maintaining-low-levels-community-transmission-covid-19-scotland/covid-19-test-trace-isolate-support-public-health-approach-maintaining-low-levels-community-transmission-covid-19-scotland/govscot%3Adocument/covid-19-test-trace-isolate-support-public-health-approach-maintaining-low-levels-community-transmission-covid-19-scotland.pdf

A Summary of how test and trace works

1. Any adult currently with coronavirus symptoms can apply for a test. There are priority groups, such as essential workers, those living with essential workers etc, who can be prioritised for testing. Find out more who is eligible for a test.[4]
2. Under the Test and Trace system people who have coronavirus symptoms are asked to take a test. Find out more how to take a test.[5]
3. Those that test positive for coronavirus will be asked to identify people (this is voluntary and not obligatory) who they have had recent contact with and who may also therefore be at risk of infection.
4. Those people are then contacted by the contact tracers and are then asked to provide details including their symptoms so advice on isolation can be given, and to share contact details of anyone else they may have come into close contact with, who will in turn be contacted to help isolate the spread of the virus.

The digital NHSX COVID -19 contact tracing app

The accompanying digital contact tracing app - NHSX COVID-19 app - isn't live yet and may not be fully in place until September 2020. Currently it has failed recent cyber security, clinical safety and performance tests.

The NHS digital app service works similarly in Scotland and N. Ireland, except that the services are run by different contracted digital companies and personal contact data collection is used and stored differently with more privacy protections.

The purpose of all digital contact-tracing apps are to try and track down people and alert them of the need to self-isolate faster than traditional methods.

How the NHSX app will work:

1. When the app is made available in England, it will be available to download from Apple or Google app stores
2. Users then need to enable it to use the Bluetooth feature on their smartphone
3. When setting up the app, users will be asked to enter the first half of their postcode. This is so the NHS can use the data to see where hotspots of infection are breaking out. Users are not asked for any more details until they want to report symptoms
4. The app will run in the background of the phone, periodically waking up when it senses another phone with the app coming into range. It will then use Bluetooth to measure how far away the other person is every 15 seconds. The

[4] https://www.gov.uk/guidance/coronavirus-covid-19-getting-tested

[5] https://www.nhs.uk/conditions/coronavirus-covid-19/testing-and-tracing/ask-for-a-test-to-check-if-you-have-coronavirus/

app will log the other phone for 28 days if the two devices came into close contact. This is known as a Bluetooth handshake.

5. Users who download the app to their phone can voluntarily opt-in to record and report the details of their symptoms when they start to feel unwell. They will be asked a series of clinical questions. This will be similar to other NHS reporting functions, such as the 111 services
6. The answers will then be analysed by the NHS's artificial intelligence (AI) programme. If the AI decides the symptoms meet a threshold for Covid-19, that person will be asked to take a test and self-isolate for 14 days
7. The AI will then analyse contacts the symptomatic persons phone has logged (via its Bluetooth handshake) in the app to decide the potential risk of infection for each person. People deemed to have had 'high risk' contact with someone reporting Covid-19 symptoms will then be sent a warning alert from a central data system advising that they self-isolate for 14 days as well
8. If the test is positive self-isolation advice remains in place for all alerted. A PHE contact-tracing team will follow up with the tested user and find other people they may have infected. If the test comes back negative, the app will send out a second alert to the contacted people telling that they can stop self-isolating.

Test and trace in the workplace

The NHS test and trace service does not change the existing guidance about working from home wherever possible. For essential workers, people non-home working and those already working in a workplace and people returning to the workplace test and trace will impact on co-workers in the workplace.

The Department of Health and Social Care has published guidance on the NHS test and trace service which explains how employers and workers can play their part in the service to slow the spread of the virus and keep the public safe.[6] This includes health and safety mitigations, support for those workers self-isolating and guidance on pay and leave.

Some employers may seek to introduce a workplace testing scheme. Whether they intend it to be obligatory or voluntary they should consult with trade unions and follow the data protection guidance provided by the Information Commission Officer (ICO).[7]

This would mean providing a Data Protection Impact Assessment to cover issues like the purpose of testing, the processing of data, specifically health care data which is a

[6] https://www.gov.uk/guidance/nhs-test-and-trace-workplace-guidance

[7] https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/data-protection-and-coronavirus/workplace-testing-guidance-for-employers/

‘special category’ and guidelines for those who have been tested but are awaiting results.

Concerns over data privacy in the test and tracing service

The main concerns all stem from the fact that the government and NHSX have tried to create a centralised data collection process that goes beyond just alerting people via contact tracing to coronavirus risk. In almost complete contrast to the rest of the world and against EU digital advice it has tried to use the tracing app to create a digital and data infrastructure that allows existing and future pathways into NHS data, beyond test and trace.

1. **Failure over upholding existing data rights**
    - Trade unions, MPs[8], 177 global digital and AI academics and digital and human rights lawyers[9] believe that digital apps must uphold our existing data privacy rights and some designs are better than other. The UK NHSX app is believed to breach our privacy and GDPR rights
    - Complaints to the ICO are based on the fact that the NHS and PHE failed to carry out a data protection impact assessment (DPIA) before forging ahead with the scheme, despite GDPR calling for one in high risk data processing scenarios
    - The Test and Trace privacy notice failed to differentiate between personal data and ‘special category data’ such as NHS data, and it is claimed there is lack of specificity with regards to anonymous data and pseudonymous data. Instead the notice uses the Americanised term “personally identifiable data” – something that has caused alarm to data privacy specialists because EU data protection law is much stronger than American law

2. **Big global tech companies will process our NHS data with little transparency**
    - Those who may see and process the data, will apparently be “those who have a specific and legitimate role in the response”. This vagueness of ‘the specific and legitimate role’ is a real concern, because the NHS has made clear they’re working on the app with third party companies like Google, Amazon, SERCO:
    - The privacy notice for the Test and Trace scheme says that the data will be processed by contact tracers recruited from PHE and the NHS, as well as public service outsourcers Serco and Sitel Group, and held in secure storage by Amazon Web Services
    - The digital app outsourcing contract involves a total of eight private overseas companies. Two major contracts have been awarded to two companies owned by multinationals: Pivotal (UK) Ltd is part of the US giant Dell

[8] https://committees.parliament.uk/committee/93/human-rights-joint-committee/news/146351/report-on-the-contact-tracing-app-published/

[9] https://tech.newstatesman.com/gdpr/open-rights-group-reports-nhs-test-and-trace-to-ico

Technologies group which have a huge range of commercial and military contracts and Zuhlke Technology Group AG based in Switzerland which has over 10,000 projects and employs well over 1000 people in eight countries

- Google and Apple are also now involved in the app on a so called 'shadow' project, its currently unclear as to how its work will link to the existing UK app development (by Piviotal and Zuhkle). Its rumoured that the Google /Amazon app with a de-centralised trace system is now going to be used to replace the current centralised trace system being currently designed.
- This is because the mounting legal challenges and complaints against the current centralised app, a design created by NHSX, (which has been rejected by all the EU member states), has put pressure on the government and NHSX to make it more privacy compliant. This will likely cause further delay in the role out of the app and the google de-centralised approach may be now being built in.

3. Third Party access of UK NHS data by US and global digital corporations

- It is not clear specifically how the personal and NHS data generated through the app will be harnessed into the Palantir/Faculty AI COVID-19 datastore
- It is also not clear therefore if these third parties (including those providing manual and app tracing services) will also have access to the mega Covid-19 data store managed by Palantir and Faculty AI and in what capacity
- The COVID-19 data store since March had been collecting COVID-19 data from over 80 UK data centres, from health and social care organisations in order to "provide a single source of truth" about the pandemic
- Currently we are allowed to see what is going into the data store but not what is coming out. Only Cobra can see this and nominated 'others' too
- The data store project contracts released by the UK government in early June have revealed that personal health information about millions of NHS patients was provided to private tech firms involved in the COVID-19 Palantir datastore project
- Details of these deals with Amazon, Microsoft, Google and Plantir and Faculty have been now been published
- They reveal that companies involved in the datastore project were originally granted intellectual property rights - shockingly also including their creation of databases with NHS data - and were allowed to train their models to profit from unprecedented access to NHS data
- The terms of the deal have now been changed after a Freedom of Information request exposed how the free use of NHS data were being used for commercial benefits[10]
- Faculty have now asked for its contract to be amended to make clear that it will derive no commercial benefit from any software, including trained

[10] https://publicnewsupdate.com/uks-covid-19-health-data-contracts-with-google-and-palantir-finally-emerge/

machine learning models, developed during the course of the project and that the use of the IP is under the sole control of the NHS

4. **Failure to be transparent on the future purpose of the data collected**
    - The commercial and research intentions of the scheme have been ill-defined so far creating even more uncertainty and lack of trust
    - The UK app has been designed to collect identifiable data, which Public Health England (PHE) plans to keep hold of for 20 years in the instance of Test and Trace. This will include full name, date of birth, sex, NHS number, address, phone number, email address, and everything about symptoms, being kept on file for at least two decades, for no transparent or understandable reason
    - Concerns over 'mission creep' are also raised – for example - the possibility that intelligence agencies could someday get their hands on the tracing app's data was stoked by the revelation that the National Cyber Security Centre (NCC), a division of GCHQ is also involved in the app. Sharing the app data for immigration tracing purposes for example would be a mission creep
    - A solid legal foundation for the tracing app is needed. NHXS claims that the contact data collected is pseudonymised and that third parties won't be granted access to it. However we have already seen that later iterations of the app are intended to request increasingly personal information, like location data.
    - And although the data is pseudonymised, the NHS has the means to link it to an identifiable person. The project's Data Protection Impact Assessment (DPIA) expressly states that de-anonymised versions of the data might be used for research at a later date
    - There are concerns that the data could be linked to a UK future 'immunity passport' system. Facial recognition has already been added as a way of logging in to an NHS app that lets people order prescriptions, book appointments and find healthcare data. Initially, it will allow faster access to the services on the app, which is separate from the contact-tracing one. However its developers say it could also be used for Covid-19 "immunity passports"
    - The immunity passports, allow people to carry documented proof they have immunity because of a past infection and Health Secretary Matt Hancock has previously hinted at the possible use of a "system of certification" for those with antibodies for coronavirus. Limiting people's rights with passports or health certificates is extremely worrying[11]
    - The requirement for developing future pathways has also been a concern as part of the contracts require the design of a longterm digital roadmap for future features that can be built on to the app later

[11] https://www.wired.co.uk/article/uk-immunity-passports-coronavirus

5. Operation, discrimination, fraud and access issues

- It is estimated that a 60% take up is required for the app to be successful and as yet it is not clear how this app will work when people go abroad, in hubs of lots of people – airports, tower blocks, train stations etc
- People without smart phones or Bluetooth technology will be excluded access to the app and an impact assessment providing mitigation measures is needed
- The manual service has also raised security concerns, specifically around how fraudsters might seek to use it as a guise to trick victims into handing over sensitive personal data
- The threat of data misuse is also especially acute for populations that tend to bear the brunt of intrusive surveillance and policing powers. Religious communities, black and ethnic minority communities, poor communities, and immigrant communities are most at risk. The Home Office has already been found to exploit NHS data and data from schools in order to persecute immigrants in the UK. The app should not offer another avenue to do so

6. Legal Bill required to protect Privacy, GDPR, Equality and Human rights

- There needs to be accompanying legislation to protect employees and citizens which would guarantee:

  - Sanctions will not be applied for not joining the app voluntarily
  - Its not a mandatory requirement to download the app that employers can demand in the workplace, unless its compliant with the ICO guidelines on data protection law[12] and obligations in employment law, the contract with employees, health and safety requirements and equalities issues are taken into consideration.
  - No repurposing of the app, with legal framework to prevent function and mission creep with personal data
- The Joint Committee on Human Rights (MPs and Peers) has recommended[13] against rolling out the app nationally without a number of guarantees, which include the following:
  - Privacy protections enshrined in primary legislation
  - Oversight by an independent body
  - Transparency over what data is collected and its use
  - The committee believes the legislation should prohibit data sharing with employers

[12] https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/coronavirus-recovery-data-protection-advice-for-organisations/testing/

[13] https://committees.parliament.uk/committee/93/human-rights-joint-committee/news/146351/report-on-the-contact-tracing-app-published/

- It has also produced a draft bill[14] that would prevent the government from using the information gathered for any other purpose than fighting Covid-19 and require it to delete all the data after the pandemic ends

Guidance for members/branches

- Branches should hold a meeting with employers on any proposals for monitoring, surveillance and testing of employers for COVID-19:

    - Employers should be prevented from having access to data gleaned from any voluntary state-run app
    - Existing privacy rules, including those embedded in the General Data Protection Regulation (GDPR), must be respected
    - NHS data protection, employment, health and safety, employment contract obligations, equality regulations must all be compliant
    - Contact-tracing apps should only be used in the workplace if specific requirements are met and set out in a Data Protection Impact Assessment (DPIA)
    - Employers should clearly explain the purpose of the app, the type of data that will be collected, and how long the data will be kept
    - Workers must give their consent and trade unions should have a legal right to be consulted before an employer starts to collect data and make data-driven decisions in the workplace

- A Data Protection Impact Assessment (DPIA) must be completed and trade unions should be consulted on it. Best practice examples of a DPIA should be used and a checklist for what it should cover

- The ICO sets out specific guidance on data privacy compliance and specifically on health data which is viewed as a special data category. The employers ICO guidance contains[15]:
    - Guidance for employers and organisations that are planning on asking people if they have experienced COVID-19 symptoms or are planning to introduce testing
    - guidance for employers and organisations that are planning on using CCTV, thermal cameras or other surveillance methods as part of testing or ongoing monitoring of staff
    - guidance on compliance on people's rights in relation to their personal data

[14] https://www.parliament.uk/business/committees/committees-a-z/joint-select/human-rights-committee/news-parliament-2017/covid-contact-tracing-app-draft-bill-19-21/

[15] https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/coronavirus-recovery-data-protection-advice-for-organisations/