



---

## Rapid evidence review explainer

For technology providers and developers

---

# Exit through the App Store?

## A rapid review of evidence on the technical considerations and societal implications of using technology to transition from the COVID-19 crisis

Governments around the world are beginning to look to data-driven technologies as tools to support the transition from emergency lockdown measures in response to COVID-19. There are three interlocking technical interventions being considered in the UK, as well as in other countries: **digital contact tracing applications, symptom tracking applications and digital immunity certificates**. It is suggested that these technologies can inform research into the disease, prevent further infections, and support the restoration of system capacity and the opening up of the economy.

### Digital contact tracing

Digital contact tracing applications are used to determine when a person has come into contact with people who are infected with COVID-19. When that happens, the app notifies the person, and in some circumstances the public health authority, and provides guidance or instructions. A digital contact tracing app is currently being developed by the NHS.

Based on the current evidence reviewed, there are significant technical limitations, and deep social risks, to implementing digital contact tracing. These include:

### Technical limitations

- Imprecision in detecting 'contact';
- Imprecision in detecting distance between people;
- Vulnerability to fraud and abuse.

### Barriers to effective deployment

- Establishing its effectiveness as part of a wider pandemic response strategy;
- Reliance on high levels of accuracy in data about infection rates, and on widespread uptake of the application by the population;
- Gaining and maintaining public trust and confidence;
- Potentially harmful behavioural impacts.

### Social considerations to be built in

- Potential exclusion of vulnerable groups;
- Societal and financial implications;
- Criminality and scams.

On the current evidence, these concerns outweigh the value that digital contact tracing offers to the crisis response.

To overcome these limitations and risks, digital contact tracing applications should ensure privacy-by-design, and include privacy-preserving protocols to underscore technical measures. We recommend that Government advances primary legislation that imposes strict purpose, access and time limitations on digital contact tracing applications.

### Key takeaways from the rapid review for technology providers and developers

The rushed deployment of technical solutions without credible supporting evidence and independent oversight may undermine public trust, and impede the technologies' effectiveness in supporting the crisis response.

Effective technical solutions must be built on accurate health data. Technology providers and developers should work closely with health and public health experts throughout design and implementation.

Designs, research and source code for technical implementations, as well as data about their effectiveness in reducing the spread of the virus, should be made public to enable scrutiny.

Technical design choices should factor in privacy-by-design and accessibility features, and be buttressed by non-technical measures to account for digital exclusion. Technical measures might include protection of individual privacy through decentralised privacy-preserving digital contact tracing, and be underscored by privacy-preserving protocols.

## Symptom tracking

Symptom tracking services take the form of apps and websites that encourage citizens to share information about themselves (such as their age, gender and medical history), and report their symptoms of COVID-19 – usually on a regular basis, such as once a day.

Symptom tracking apps may be useful in expanding understanding of the disease and tracking its spread. However, they suffer from limitations including the low quality of data obtained through self-reporting of symptoms, imbalances in the representativeness of the data collected, and false reporting risks. These limitations translate into both health risks and data risks:

### Health risks

- Data limitations confuse the evidence base;
- Health inequalities may be exacerbated.

### Data risks

- Data may be shared more widely than originally intended and platforms may be repurposed;
- Symptom tracking databases centralise large amounts of personal data;
- The organisation collecting the symptom data might attempt to monetise the data and the inferences it draws about participants.

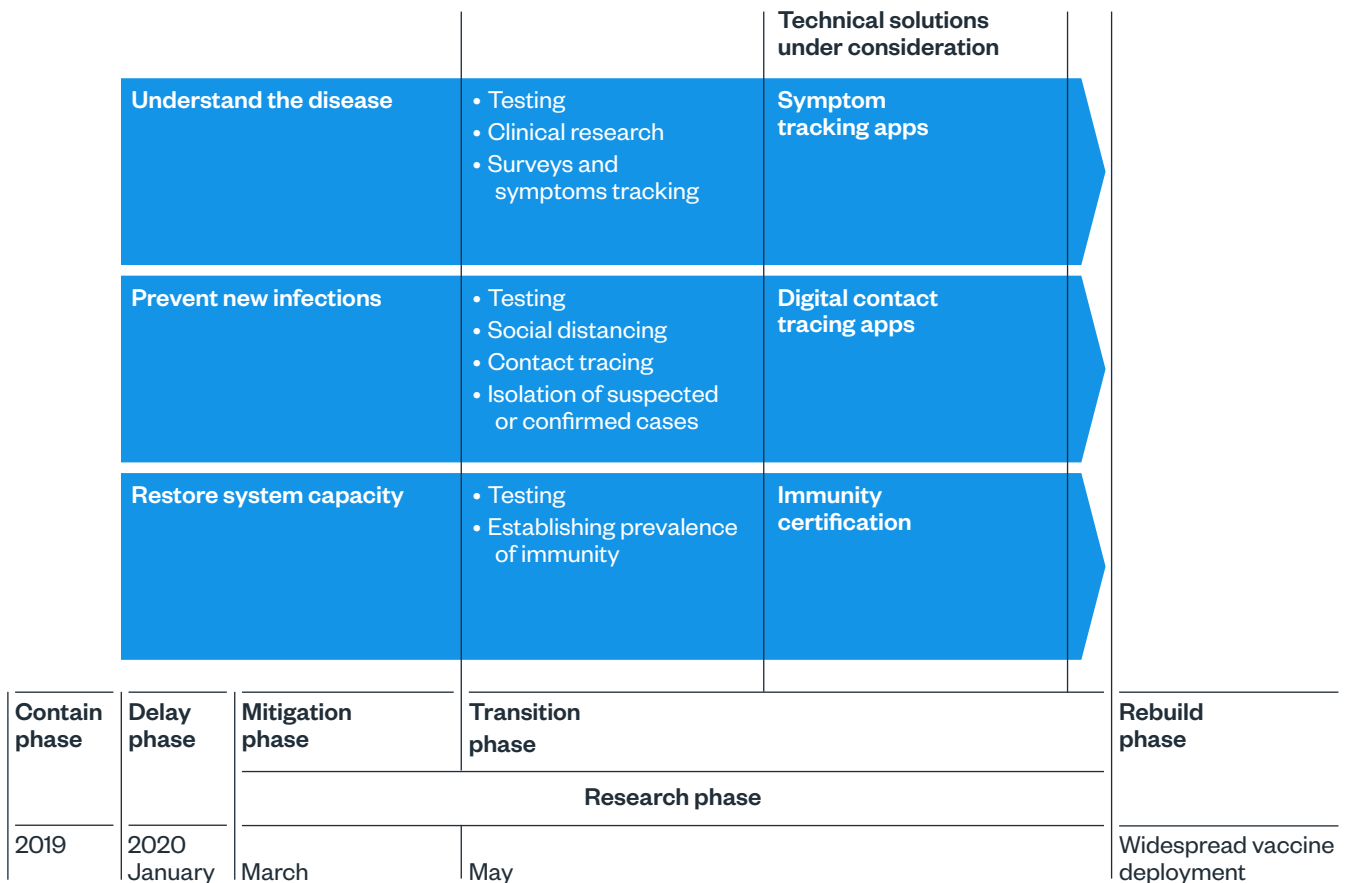
Mitigating these risks requires Government to advance, and Parliament to adopt, primary legislation to limit both the purposes for which data collected in symptom tracking apps is processed, and the period during which this data may be processed before being deleted.

## Immunity certification

There is broad agreement that widespread testing is the only route through which the UK can exit the coronavirus crisis. Immunity testing is likely to be a key part of this strategy. However, there does not yet seem to be a robust scientific means of testing immunity. There is therefore no credible basis for establishing a comprehensive regime of immunity certification at this time.

This rapid evidence review establishes four sequential questions that should be answered in order to guide policy formulation around immunity certification:

1. Is the science on immunity sufficiently robust to warrant a policy approach centred on immunity certification?
2. How would immunity testing be delivered?
3. How would immunity testing be certified?
4. How would immunity certification be integrated into policies and processes?



Overview of the uses of technology to transition from the COVID-19 crisis

The establishment of a regime for immunity certification will have deep societal implications, including:

- The infringement of individual rights, particularly privacy;
- Stigmatisation and discrimination;
- Establishing a two-tiered society;
- Fraud and abuse;
- Creating perverse incentives.

Government should establish an independent Group of Advisors on Technology in Emergencies (GATE) to oversee the development and testing of any prospective digital immunity certification system.

If this Group is established, technology providers and developers should follow its stipulations on the inclusion of privacy-preserving measures, and adopt measures to ensure that vulnerable groups are not excluded from the operation of the system.

**Exit through the App Store?**

Read the full rapid evidence review: [adalovelaceinstitute.org/covid-19-exit-through-the-app-store/](https://adalovelaceinstitute.org/covid-19-exit-through-the-app-store/)