

## Part 2: Getting Digital Health Passports Right? Legal, Ethical and Equality Considerations

Dr Irene Pietropaoli

---

*This is a two-part blog series. In [Part 1](#) Prof. Lilian Edwards discusses if there is a case for vaccine passports at all. In Part 2, Dr. Irene Pietropaoli discusses the legal and practical detail of such schemes if it is decided to proceed.*

The UK Government has just closed a public consultation on a '[COVID-Status certification scheme](#)' (CSCS). We submitted our [response](#) where we make the following arguments.

***The Government should consider before commissioning new technologies whether existing legal safeguards are adequate and if not what new laws or steps might be appropriate to protect fundamental rights and freedom, as well as preserve public trust.***

The government must clarify what the legal bases for different uses of vaccine passports are, whether the Coronavirus-specific powers, or other regulations. The former are time-limited, and thus if that is the basis it must be clarified for exactly how long a CSCS scheme will be used and what the cut-off point will be: when a certain percentage of the population has been vaccinated, or herd immunity has been reached in the UK? We recommend that it be enshrined in primary law that any state CSCS scheme is terminated at the end of the emergency as defined in the Coronavirus legislation and a majority vote in both Houses of Parliament be required to continue it. Any CSCS scheme should explicitly be created as an interim, emergency solution, to guard against scope creep and mission creep.

Any scheme must meet legal standards around, inter alia, equality and non-discrimination, labour rights and privacy and data protection. The Government should not derogate from these by use of the emergency delegated legislation procedures, which have been used to impose lockdowns and quarantine during COVID, to the detriment of parliamentary debate and democratic accountability: instead it should, as the [Bingham Centre has set out](#) in the context of lockdown regulations, use primary legislation to ensure a process that better serves the rule of law. If we are to be back to [normal life by the end of June](#), then the same must be true of the law. No technologies should be trialled before appropriate Data Protection Impact Assessments and Equalities Impact Assessments are prepared.

The Government [is planning](#) to make CSCS available both 'to vaccinated people and to unvaccinated people who have been tested'. Theoretically, this means that vaccines are not mandatory. But in practice it may become so as a negative test is valid only for a short time (72 hours). If people would need a CSCS to access employment and public venues it may not be practical for them to take a test - even a rapid test - every time they enter a service. In reality, even if the CSCS is available for non-vaccinated people, in most settings this would still amount to, at least indirectly, forcing people to be vaccinated, which raises ethical concerns. It is important that the CSCS is not used as a tool for introducing compulsory vaccination, without a clear explanation of its necessity in all settings. This, as the Ada Lovelace Institute [finds](#) may increase mistrust by marginalised groups who may have higher rates of vaccine hesitancy.

Any requirement to use a vaccine passport to access public sector services must be necessary, proportionate and transparent, and there should be easy and free access to ways to challenge unreasonable restrictions.

Private sector workplaces are a key issue of debate. It seems possible that private employers are going to impose some kind of requirement to show a vaccine or health passport, independently from whether the Government adopts a CSCS. For example, a large London plumbing company [said](#) in January it was planning to rewrite all of its workers' contracts to require them to be vaccinated. A [global survey](#) by a recruitment agency, published in March found that 25% employers are already planning to start mandating vaccination for at least some roles. Private employers can argue that it is part of their health and safety legal duties. It is clear, however, from both the Court of Justice of the European Union and the European Court of Human Rights' jurisprudence that workers have rights of privacy at work as well as, at least currently, the right to refuse medical treatment.

We recommend that a workplace requiring a vaccination certificate for access should be conditional on having assessed whether it is necessary, whether alternatives are available (e.g. conventional safety measures, proof of negative test) and that potential impacts on workers' rights have been assessed and mitigated. As the Ada Lovelace Institute [found in February](#), it may be possible to update existing mechanisms already in place to protect workers, such as the Green Book on immunisation, which require vaccination in high-risk environments, or existing 'fit and proper person' requirements.

Facial recognition [has been suggested](#) as one means of verification at some venues, which raises further ethical concerns. We suggest that legislation should make it clear that any digital health certificate scheme presumptively should not incorporate biometric surveillance which has severe issues for human rights as well as accuracy and discrimination.

***The Government should carefully consider the risk that a CSCS may be used for different or expanded purposes than originally planned, and data stored in the CSCS may be used more broadly than intended.***

A major difference between previous vaccination requirements (e.g. the International Certificate of Vaccination or Prophylaxis, known as the 'yellow card', which the Centre for Disease Control and Prevention still urge people to take on relevant travels) and the CSCS is its digital component, which raises additional concerns around privacy and data protection.

The WHO [recommends](#) that, along with the digital implementation of 'smart vaccination certificates', the COVID-19 vaccination status should still be recorded through the paper-based International Certificate for Vaccination. Similarly, the [EU Digital Green Certificate](#) is meant to be available in both digital and paper format. It is not clear whether the CSCS will be available also in paper format. The Government should do so, providing a paper format with a QR code.

The Government should carefully consider the risk that a CSCS may be used for different or expanded purposes than originally planned, and data stored in the CSCS may be used more broadly than intended. Once personal data is collected it may, even unintentionally, be shared with third parties, and may be repurposed. Data protection and privacy are required under the [General Data Protection Regulation](#) so a centralised database would not be allowed. As also [pointed out](#) by Open Rights Group, the Government should not repeat the mistakes done last year while building a 'centralised and privacy-invasive' digital contact tracing system.

To address privacy concerns, companies developing COVID-status apps and other commercial [initiatives](#) suggest they can ensure there is no connection between the source of a person's data and the entity requesting it - linking people 'securely with their smartphones using biometrics and some form of government-issued identity document'. Even if privacy-preserving technology can be developed, however, it is [to be expected](#) that data will be viewed by different actors - e.g. employers, police, private companies, health care staff, etc. -, who may have different levels of experience and responsibility in handling personal data. Both private actors and public authorities have not proved to be always trustworthy at keeping personal data private and not sharing it, especially for commercial interests. The Government needs to consider the implications of the linkage of people's COVID-status credentials to the various means of identification or verification, especially when this is done via digital means - e.g. linked with the NHS app.

The Government needs to ensure that data stored in GPs' records are not going to be in any way copied or shared and that every use of data is consensual, safe and transparent. The Government also needs to guarantee that once the CSCS infrastructure is put in place to 'confirm' people's COVID-status, other health data is not added to it - e.g. HIV status. In the UK, there is a long-standing common law duty of confidentiality in relation to personal medical information - information provided in confidence should be treated as such and not divulged to third parties.

***The Government needs to consider and explain the longevity of the CSCS and set up a Parliamentary sunset clause.***

Further, the Government needs to consider and explain the longevity of the CSCS, as the risk is that once such requirements and related infrastructure are put in place, they will last longer than the COVID-19 public health emergency. The risk, as Ada Lovelace [finds](#), is that a response to a time-bounded crisis may result in 'normalising health status surveillance by creating long-term infrastructure'. Privacy organisations [fear](#) that 'vaccine passports mean the future we are being offered bears more control, not more freedom'.

It is crucial that a Parliamentary sunset clause be placed on any digital health certificate scheme. As COVID-19 is likely to become endemic, the Government should not use it as an excuse to extend emergency powers behind the time when most people have received a vaccine and the public health emergency is over.

***Any award of a contract related to a CSCS to the private sector must be accompanied with a full procurement process, full transparency and a data protection and equality impact process.***

The Government has already funded or otherwise supported the development of multiple commercial vaccine passports and COVID-status apps and other initiatives. It was [reported in March](#) that the Government has given at least £450,000 in grants to

companies to develop such initiatives. For example, Verifiable Credentials, which has received government funding to develop vaccine passports, [is testing an app](#) to verify vaccine status and COVID-19 test results with dummy data at a cinema and with real data at a hospital, where it has replaced existing paper-based methods.

[Public procurement of apps needs to be justified and accountable](#), given the ethical duty to manage public finances wisely. For example, it is hard to evidence the benefits of recent NHS spending on contact tracing apps, albeit this may have seemed rational at the time. Any award of a contract in this area to the private sector must be accompanied with a full procurement process, full transparency and a data protection and equality impact process. We are no longer in an unforeseen emergency and there is no reason to exempt procurement safeguards.

***A proportionality, transparency and legitimacy test should be applied where any private or public operator seeks to impose the requirement to show a digital health certificate to access services or goods, and oversight of this should be attainable by an appropriate tribunal or regulator.***

The proliferation of private sector 'passporting' systems in relation to labour and international travel also needs attention. There is severe danger here of infringement of rights by private actors not subject to FOI or judicial review oversight. We suggest as in the [Coronavirus Safeguards Bill](#) that a proportionality, transparency and legitimacy test be applied, and oversight be attainable by an appropriate tribunal or regulator.

There are ethical and business and human rights concerns in relation to the lack of regulation of commercial use of vaccine passports and other COVID-status initiatives. The Government should require companies developing to conduct proper human rights due diligence during the design and development, as required by the [UN Guiding Principles on business and human rights](#).

***In developing CSCS requirements, the Government should make reasonable exemptions for people who cannot be vaccinated.***

A CSCS may risk exacerbating social inequalities and discrimination in the UK. The UK Equality and Human Rights Commission [said](#) in February that vaccine certificates could lead to 'unlawful discrimination'. As minority communities have a lower rate of vaccination and testing, a CSCS may restrict access to employment and public spaces to people who are already affected by social inequality. In addition, [as reported](#) by Ada Lovelace, people have unequal access to technology, digital literacy and forms of identification, and the CSCS may reinforce such existing inequalities.

In developing CSCS requirements, the Government should make reasonable exemptions for people who cannot be vaccinated - e.g. pregnant women, people with disabilities or other medical conditions that prevent them from accessing or getting a vaccine, as well as people who are too young to get it offered yet. Under the [Equality Act 2010](#) a policy indirectly discriminating against people with protected characteristics (such as race, sex, disability, and age) must show to 'be a proportionate means of achieving a legitimate aim'. As such, CSCS requirements need to clearly explain their legitimate aim and their proportionality if they result in discrimination against those groups.

The Government [clarifies](#) that the CSCS 'would be available both to vaccinated people and to unvaccinated people who have been tested' and that it refers to 'the use of testing or vaccination data to confirm in different settings that 'individuals have a lower risk of getting sick with or transmitting COVID-19 to others'. If those are the justifications - lower risks of getting sick and lower risk of transmission- then the CSCS should reasonably also include people who have contracted COVID-19 and recently recovered from it - as they would have antibodies for a period afterwards. The [Digital Green Certificate](#) proposed by the European Commission aims to prove that a person has either been vaccinated against COVID-19, received a negative test result or recovered.

The Government should explain for how long the CSCS is valid for - and the difference between duration of a CSC showing vaccination, a negative test or, possibly, a test showing antibodies. The Ada Lovelace [recommends](#) that 'the duration of validity of the passport will remain dynamic in response to developing scientific understanding rather than a fixed date of issue'. Additionally, [as outlined](#) by the Royal Society, any vaccine passport should include a way of accommodating 'changes in vaccine efficacy against emerging variants'.

The Government should also consider how the CSCS will link with other similar schemes, such as the [IATA Travel Pass](#) and the EU [Digital Green Certificate](#). For example, would an EU citizen holding a Digital Green Certificate have the same rights in the UK of a CSCS-holder?

***Continuing public engagement is required to help guide the government as to the acceptability of using CSCS systems under different circumstances, as threat levels change.***

Without a public mandate, a national scale system with inherent privacy risks can easily fail, due to non-adherence or misuse. More public engagement is required to help guide the government as to the acceptability of using CSCS systems under different

circumstances, for how long for, and so on. It will also help members of parliament to better understand the fair and appropriate boundaries of legislative powers. Ultimately the utility of such technologies has much to do with trust - that they are safe, proportionate, secure, free of bias, respect people's rights and - in the case of a pandemic, appropriately temporary. Open conversations with the public and the different communities likely to be most affected by these measures will be needed on an ongoing basis, as threat levels change (e.g. with new variants), the effects of the current vaccination programme are felt and the nature of the 'new normal' becomes evident.

Correspondence to [lilian.edwards@ncl.ac.uk](mailto:lilian.edwards@ncl.ac.uk) and [I.Pietropaoli@biicl.org](mailto:I.Pietropaoli@biicl.org) or leave a reply below.

**Author:** [Dr. Irene Pietropaoli](#), BIICL's Research Fellow in Business and Human Rights and co-investigator in the AHRC research project '[The Role of Good Governance and the Rule of Law in Building Public Trust in Data-Driven Responses to Public Health Emergencies](#)' responds to the UK Government's [COVID-Status Certification Scheme consultation](#) - with contributions from fellow co-investigators, Prof. Lilian Edwards (Newcastle University), Dr Claudia Pagliari (University of Edinburgh), Dr. Anjali Mazumder (Alan Turing Institute), and Dr. Jan van Zyl Smit (Bingham Centre for the Rule of Law).

URL: <https://www.biicl.org/blog/23/part-2-getting-digital-health-passports-right-legal-ethical-and-equality-considerations>