SICCAR®

Immunity is relative: an approach to COVID-19 transmission risk certification

Maarja-Liis Ferry, E-Health Lead, SICCAR
March 2021

siccar.net

About the author

Maarja-Liis Ferry is a final-year medical student with an interest in the application of technology to improve healthcare. She holds a BSc in International Health and has worked with organisations such as Students for Global Health, the Healthcare Leadership Academy, and the International Federation of Medical Student Associations. She is working with SICCAR to explore and contextualise the many applications of distributed ledger technology to health and social care.

In a world where data is simultaneously our most valuable and vulnerable asset, the UK must act swiftly to be a world leader in setting standards and providing solutions to the issue of COVID-19 'immunity passports'.

SICCAR proposes an open approach that relies not on a one-off, static proof of vaccination, but on a dynamic certification of transmission risk based on both vaccine and testing status.

The global recovery from COVID-19 presents an opportunity to empower individuals to access their own health data.

Adaptable and dynamic certification

The UK Government states that every adult in the UK is to be offered a first dose of a coronavirus vaccine by July 31st, 2021. As plans for opening the economy, and travel, after a year of cyclical lockdowns are revealed, the issue of vaccine certification has come to the forefront. The ethics, data protection and equitable access aspects of this have been subject to debate.

One thing is certain: there will be demand for trusted and certain certification of COVID-19 transmission risk both within the UK and internationally. Industries such as aviation, hospitality, tourism, and sport have a vested interest in verifying individual risk of COVID-19 transmission.

Any infection clusters linked to these industries pose a threat to future profitability and lead to potential liability associated with those infection clusters causing individual morbidity and mortality. In the context of international travel, many countries that have been more successful than the UK in supressing COVID already require proof of a negative test for entry and have begun to adapt travel restrictions to account for vaccination.

However, immunity to COVID-19 is not guaranteed. Although vaccination prevents serious disease and hospitalisation in most fully vaccinated individuals, it has a variable impact on the ability of the individual to transmit the virus. As our knowledge of the virus, emerging variants and the long-term efficacy of available vaccines develops, the definition of 'COVID safe' will change based on geographical location and epidemiological context, rather than spring from a globally applicable standard. Therefore, it is not a case of 'immunity certification', but of stratification of transmission risk relating to the specific individual and context.

Additionally, in the UK, where public health must be balanced with an individual's right to bodily autonomy, vaccination should not be a prerequisite for accessing public spaces. Therefore, any solution surrounding 'immunity certification' instead must function as a certification that the individual is at a low risk of transmitting COVID-19 through a combination of vaccination and testing status, with the potential to incorporate future innovations such as reliable antibody status and lateral flow testing.

Any solution must deliver certification dynamically, and tie together both vaccination and testing information from various public and private sector sources to provide an individual risk of COVID transmission. 'A Case for Digital Health Passports' from the Tony Blair Institute for Global Change supports this integration of vaccination and test status, and calls for solutions that are adaptable, transparent and reliable.

The integration of these also allows for adaptability for international travel, in which different countries may have different conditions for entry related to the type of vaccine given, or different levels of quarantine exemption dependant on the individual's vaccination and testing status.

Current information on vaccination and testing status in the UK is siloed in various public and private sector databases, and verification of a negative test requires only the presentation of a static and easily forged online PDF. As we begin to move more freely, the issue of forged certification and unverified test providers will become more apparent. Any solution that allows a return to some version of normality must be transparent, reliable, and tied to the identity of the presenter to prevent forgery.

Building trust through individual empowerment

SICCAR proposes a distributed system to maintain the safety and veracity of personal data. Such systems will only be effective if they can be demonstrated to work in secure and reliable ways within and across domains of activity and industry.

This raises significant challenges for digital data security, privacy, and trust where relevant data is aggregated by a single body in a centralised approach. Generally, a decentralised approach is better set to support privacy, less vulnerable to attack, and more resilient against failure. Additionally, this approach allows the individual to be the messenger of their own data. SICCAR proposes the integration, rather than aggregation, of this data.

The current approach to health data is paternalistic. Individuals are not in control, and often must jump unnecessary administrative barriers with several different organisations to access their own information. Personal data must be in control of the individual, and accessible by the relevant parties only in a revokable, time and context-specific manner. By democratising the individual's access to their own data and not leaving this in the control of any single institution, reasonable digital rights concerns may be addressed. In addition, by empowering the individual to present their own data verifiably, the administrative burden of widespread demand for vaccination and testing certification on already stretched healthcare providers can be avoided.

It is essential that this process involves the minimum possible disclosure of personal data, and that any disclosure is transparent to the individual. Moreover, for these systems and processes to be trusted, the individual must be empowered with consent, and confident that this consent is defensible in a permanent manner and cannot be eroded by changes in policy or priority. This allows for trust in the system, better uptake by the population and therefore better control of the virus.

International cooperation for travel and migration

For international travel and migration, any solution must provide authenticity of vaccination and testing across organisational and state boundaries. The highly distributed and international nature of this problem makes it unlikely that there will be agreement on a single authority which could be entrusted with this data whilst satisfying the data privacy requirements of each individual nation.

Many nations and regions are already working on their own solutions, with the Ada Lovelace Institute tracking these efforts. The solutions enacted on a national level must operate in a way externally trusted and verifiable, and with standards-based and interoperable systems. Only by doing so can we ensure that certification is internationally applicable, and the world can remain open.

As we move forward, different nations are also likely to decide the level of risk they are willing to accept in the context of COVID-19. Any solution must be adaptable to this and give the citizen the option to present the level of information required.

Individuals travelling from countries of low endemicity may not need to present any proof of COVID status, whilst those travelling from areas of high endemicity may have to provide proof of vaccination, including the brand and dose interval, in addition to recent test status. The variable nature of these requirements makes a static certification ineffectual.

It is also necessary to have a demonstrable chain of custody across stakeholders in the vaccine and test ecosystem, including vaccine manufacturers, transportation, and those private and public healthcare organisations responsible for administering tests and vaccines.

Integration of these systems, for example, allows vaccine certification to be revoked if a specific batch is found to be faulty. This approach can also provide assurance of protection of commercially sensitive information across borders and industries, which will have increasing relevance as new and innovative testing and vaccination solutions come to market.

Not just a COVID problem

Coronavirus is not the first, and will not be the last, pathogen to pose a global challenge. By having the infrastructure in place to verify relevant health data easily and securely, we will also ensure a quicker and less disruptive response to the next threat. Additionally, we can set a precedent of removing unnecessarily administrative barriers for individuals to access their own health information to provide their status to different bodies when needed.

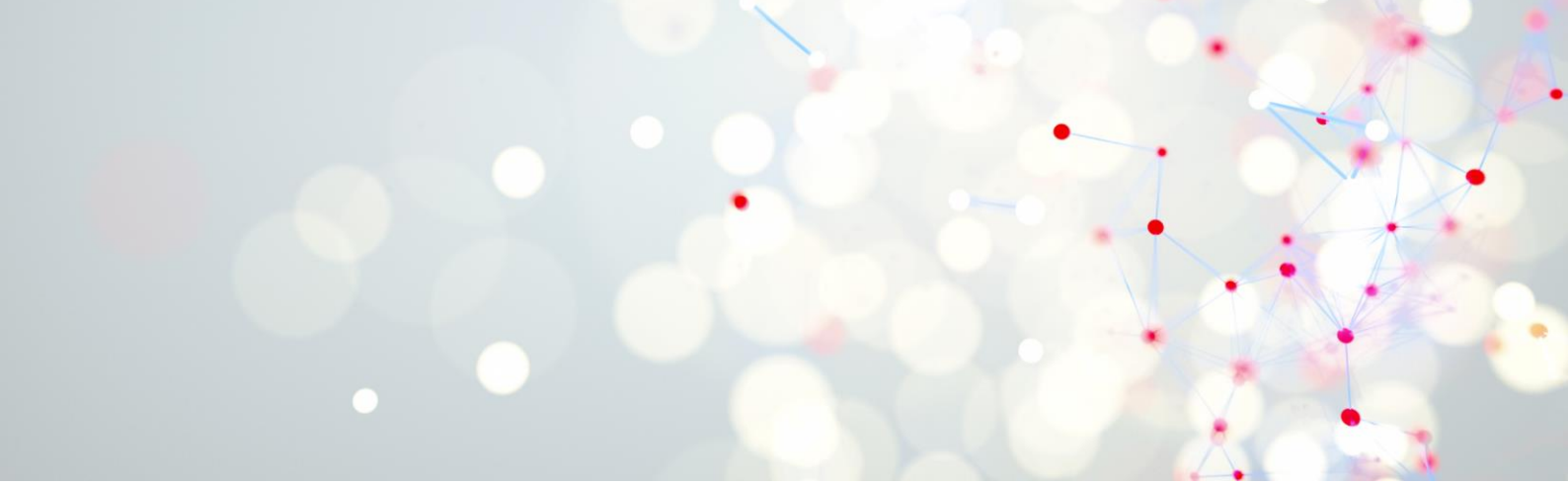
Verifying health status between systems is not a new problem. The UK lags behind other countries in taking a unified approach to health data management - even moving between GP practices within the same health board or trust can present a logistical challenge in transferring notes. This is amplified further if moving between the four nations. Additionally, in the context of occupational health, many health and care workers and forced to consistently reverify their vaccination record when changing workplaces and, if unable to do so, are subject to invasive and unnecessary tests for conditions such as hepatitis B and tuberculosis.

The COVID-19 vaccine is also not the first to be a prerequisite for travel. Yellow fever vaccination is a condition of entry to many countries in Africa and the Americas. This is currently certified using a paper booklet, in which the details of the vaccination are recorded. There is therefore capacity for any solution verifying COVID risk status to also include other health verification when relevant and requested by the individual. This is already being considered by the African Union, who have created the COVID 19 Trusted Travel portal and incorporated Yellow Fever vaccination status into this.

Ethical and privacy implications

A verifiable certification of COVID vaccination and testing status will allow society greater freedoms in participating in public life. However, there are ethical implications to making these freedoms conditional on health status. It is our responsibility to ensure valid exemptions from vaccination are recognised, that there is equitable access to both vaccination and testing, and subsequently to the certification of this. Additionally, health data must be protected, and not subject to future misuse or sale.

The UK's prioritised approach to vaccination based on age and clinical vulnerability is a reasonable one. Our socialised healthcare system goes some way to alleviating concerns that access to vaccination and testing will be reserved for the rich and well connected. However, there is still significant inequity to healthcare access throughout the UK. Already vulnerable groups such as refugees and homeless people are less likely to be registered with a GP or other primary health services, and so may miss their call to vaccination.



Vaccination supply chain issues mean that some rural communities will receive a different offering than their urban counterparts. Additionally, certain social groups have an entrenched and justifiable mistrust of health services due to the historical context, and so may be hesitant to receive vaccination or permit an outside body access to health data.

These factors must be considered when deciding how COVID vaccination and testing status will impact on public life, and reasonable mechanisms put in place to alleviate this.

The concerns around aggregating data for health status certification are legitimate. Centralising the health status of individuals leaves this information vulnerable for abuse and relies on the ongoing benevolence of government in protecting its citizen's data. Therefore, SICCAR proposes a distributed solution, in which the consent of the individual is enforced and unforgeable. This approach removes the requirement for a central database, allowing integration rather than aggregation, of data sources, and allows for the individual to reliably permission and track who is accessing their data.

Setting a precedent

Some answer to the question of verifying COVID risk status is inevitable. The worst-case scenario is an unequal, bloated system in which individuals are forced to jump through administrative hoops to access their own health data, and front-line healthcare staff are unfairly burdened with providing this certification.

It is the responsibility of the UK Government to embrace innovation and actively participate in defining good data sharing practice both within the UK and internationally.

There is an opportunity to set the tone for ethical data handling, and personal data autonomy, for years to come. To shy away from this challenge would be to willingly cut the UK population off from participation in the global economy, with a far-reaching economic and social impacts.

Define good data sharing practice with SICCAR

Continue the conversation with Maarja-Liis Ferry and the team at SICCAR.

SICCAR is the UK's leading data sharing platform, enabling growth, compliance and security for organisations that want to excel.

Distributed for cyber resilience, SICCAR delivers a single source of truth for trusted real-time information. SICCAR structures and simplifies data sharing across organisations, solving any challenges around data governance and privacy.

Send us a message:
info@siccar.net

Visit our website:
www.siccar.net

Call us:
+44 131 460 7768