The Australia Institute
Research that matters.
Centre for Responsible Technology

Please Check-In: A blueprint for a safe, fair and ethical vaccination 'passport'

Proof of vaccination IDs could be a clear way forward, once privacy and ethical considerations are properly addressed

Jordan Guiao
Research Fellow, Centre for Responsible Technology

August 2021

About The Australia Institute

The Australia Institute is an independent public policy think tank based in Canberra. It is funded by donations from philanthropic trusts and individuals and commissioned research. We barrack for ideas, not political parties or candidates. Since its launch in 1994, the Institute has carried out highly influential research on a broad range of economic, social and environmental issues.

About the Centre for Responsible Technology

The Australia Institute established the Centre for Responsible Technology to give people greater influence over the way technology is rapidly changing our world. The Centre will collaborate with academics, activists, civil society and businesses to shape policy and practice around network technology by raising public awareness about the broader impacts and implications of data-driven change and advocating policies that promote the common good.

Our philosophy

As we begin the 21st century, new dilemmas confront our society and our planet. Unprecedented levels of consumption co-exist with extreme poverty. Through new technology we are more connected than we have ever been, yet civic engagement is declining. Environmental neglect continues despite heightened ecological awareness. A better balance is urgently needed.

The Australia Institute's directors, staff and supporters represent a broad range of views and priorities. What unites us is a belief that through a combination of research and creativity we can promote new solutions and ways of thinking.

Our purpose – 'Research that matters'

The Institute publishes research that contributes to a more just, sustainable and peaceful society. Our goal is to gather, interpret and communicate evidence in order to both diagnose the problems we face and propose new solutions to tackle them.

The Institute is wholly independent and not affiliated with any other organisation. Donations to its Research Fund are tax deductible for the donor. Anyone wishing to donate can do so via the website at https://www.tai.org.au or by calling the Institute on 02 6130 0530. Our secure and user-friendly website allows donors to make either one-off or regular monthly donations and we encourage everyone who can to donate in this way as it assists our research in the most significant manner.

Level 1, Endeavour House, 1 Franklin St
Canberra, ACT 2601
Tel: (02) 61300530
Email: mail@tai.org.au
Website: www.tai.org.au
ISSN: 1836-9014

Summary

Mass vaccination is needed to mitigate against the effects of COVID-19 and to help Australia start to ease restrictions. Vaccination 'passports' can be an effective way to track vaccination records and status within the population however some key technical, privacy and ethical considerations needs to be addressed to ensure they benefit all Australians.

In developing proof of vaccination, the Australia Institute's Centre for Responsible Technology have developed some fundamental principles which form the blueprint for a safe and ethical vaccination 'passport', including:

- **Privacy by design** – respects the data privacy of Australians
- **Purpose limitations** – only uses data for the intended purpose of verifying COVID vaccination status
- **Flexible user control and consent** – managed by users directly
- **Data minimisation** – only capture the minimal amount of data
- **Data use transparency** – have clear and unambiguous terms and conditions
- **Data expiry** – data expires after its intended use is fulfilled
- **Safety and security** – safe from fraudulent and harmful access
- **Allows for legitimate exemptions** – considers use cases for all Australians, including those who are legitimately exempt
- **Covers groups not eligible for Medicare** – including temporary workers, residents and international students
- **Adopts a partnership with the private sector as needed** – considers the best product use cases and leverages the private sector as required
- **Allows for verifiable non-digital format** – caters to Australians with no/limited digital access
- **No biometric capture** – doesn't use problematic biometrics for identification

Only in using these principles as part of the development of passports can Australians have the confidence that vaccination passports are safe, fair and consider everyone.

Introduction

As states around Australia go in and out of lockdown, mass vaccination is widely recognised as one of the main ways the country will be able to live with the virus into the future. The ability to identify who has and who has not been vaccinated therefore, will be key in ongoing monitoring of the virus within the population, as restrictions ease and mobility increases.

While many see vaccination 'passports' as simply an extension of the current compliance regime we have in place as part of being a citizen of Australia, (like driver's licenses and national passports), and advocate it as a way out of lockdown,[1] some questions have been raised about the ethical implications of such a program.[2] The digital nature of this identification has also thrown up technical and privacy considerations such as cyber security and fraud[3], and data ownership and wider data sharing.

Polling conducted by The Australia Institute found that the vast majority of Australians (75%) are primarily concerned with their privacy and cybersecurity online.[4]

Figure 1: Specific issues of concerns from the Big Tech Power Report: How Australians feel about the power of Big Tech and its impacts on Australian society:

Concern levels	Privacy	Cyber bullying	Cyber Security	Abuse	Free Speech	Addiction	Disinformation
Concerned	75%	74%	75%	73%	48%	57%	72%
Neither	19%	18%	19%	17%	32%	25%	21%
Not Concerned	6%	8%	6%	9%	20%	18%	7%

[1] Minns (2021), *Vaccine passports are our safe passage to normal life. Ignore your MPs' backlash, Premier,* https://www.smh.com.au/national/nsw/vaccine-passports-are-our-safe-passage-to-normal-life-ignore-your-mps-backlash-premier-20210902-p58o7e.html

[2] Smith (2021), *Moral and legal dilemma of vaccine passports for Australia,* https://www.news.com.au/national/politics/moral-and-legal-dilemma-of-vaccine-passports-for-australia/news-story/14037a52b21668bbe4f8be525ed97de7

[3] Lefroy (2021), *Alarming problem with Australia's Covid vaccination 'passport',* https://au.news.yahoo.com/alarming-problem-australia-covid-vaccine-passport-113442614.html

[4] Guiao (2021), *Big Tech Power Report: How Australians feel about the power of Big Tech and its impacts on Australian society,* https://d3n8a8pro7vhmx.cloudfront.net/theausinstitute/pages/3645/attachments/original/1625631795/Big_Tech_Power_Report.pdf?1625631795

Currently, the most widely available proof of vaccination is through the Federal Government-managed MyGov app, which can be used to access a digital certificate after the full two doses.[5] Users must be eligible for Medicare which tracks COVID vaccination status.

Figure 2: Instructions from the Services Australia website on how to get proof of vaccination

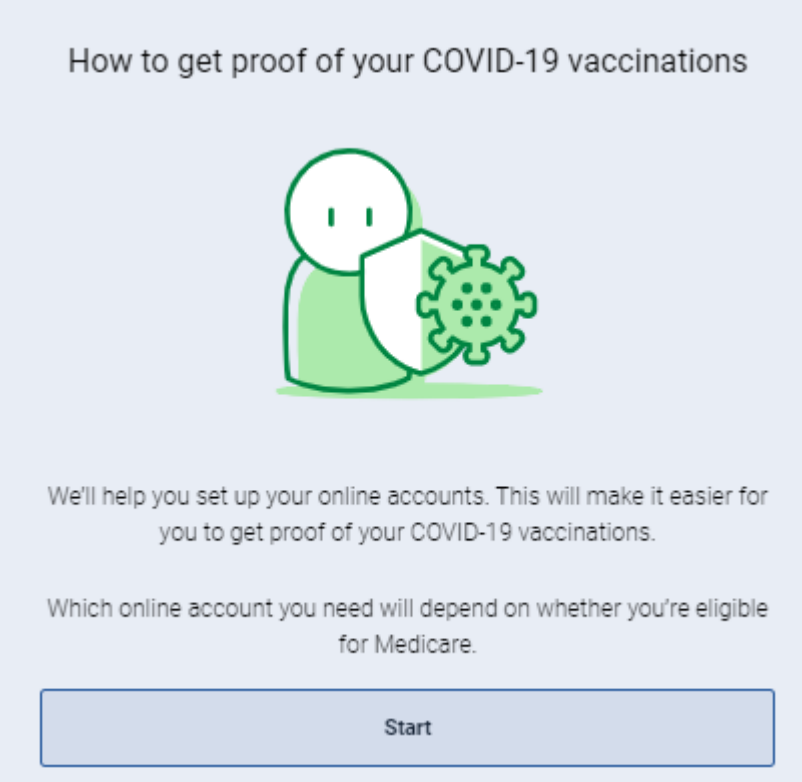
You can get an immunisation history statement or COVID-19 digital certificate to show proof of your vaccinations.

How you get proof depends on your situation. This includes if you need to create a myGov account or link services, or enrol in Medicare.

If you're 14 or older, you'll need to get your own immunisation history statement or digital certificate using either your:

- Medicare online account through myGov
- Express Plus Medicare mobile app.

If you're not eligible for Medicare, you can still get proof using the Individual Healthcare Identifiers service (IHI service) through myGov.



[5] Services Australia (2021), *How to get proof of your COVID-19 vaccinations,* https://www.servicesaustralia.gov.au/individuals/subjects/getting-help-during-coronavirus-covid-19/covid-19-vaccinations/how-get-proof-your-covid-19-vaccinations

States around Australia are exploring integration of vaccination passports through their own COVID check-in apps, which differ state by state. States are investigating the best ways to integrate proof of vaccination as part of the overall check-in/QR Code system, which is used for contact tracing and tracking.[6]

There are also some market-driven products available that collect other forms of identification required by regulated industries. An example is OnePassport – a subscription-based product already widely used in aged care and child care, which verifies worker qualifications such as working with children checks.[7] Online wallets, such as Apple Wallet and Google Pay can also be used to display proof of vaccination through integration with the MyGov digital certificate.

As the requirement for proof of vaccination scales to become part of national public policy, there needs to be further investigations into what the ideal product/ecosystem for vaccination passports should look like, with the relevant considerations addressed.

[6] McLeod (2021), *Plan to get Sydneysiders back to pubs with vaccine passport trial,* https://www.news.com.au/lifestyle/health/health-problems/plan-to-get-sydneysiders-back-to-pubs-with-vaccine-passport-trial/news-story/cc659bb9892e337a55e342884de92f15

[7] OnePassport (2021), *OnePassport website*, https://onepassport.co/

Key Considerations

TECHNICAL:

- **Operational Model** – Currently development is being spoken of as a purely government-led initiative, with States developing their own versions, and the MyGov app currently live.[8] There are both pros (consistency and accountability, coordination with public health responses) and cons (limits options and may exclude non-Australian citizens) in a purely government-led initative. A purely market-driven initiative would likely have good product experience while also likely having privacy and surveillance issues, and lack transparency. A mixed model of government and private sector collaboration may be an ideal solution with government ensuring security and consistency while allowing broader integration with private products.

- **Ease of Use** – As proof of identification requirements scale this process needs to be made easy as the public need to use it ahead of specific entry to venues and workplaces. Any ongoing updates required, whether software driven or for boosters/updated vaccinations need to be easy to update as well.

- **Security** – The current version of the vaccination certificate made headlines for the wrong reasons when a software developer was able to hack the system and create a forgery in mere minutes.[9] South Australian independent senator Rex Patrick was also able to create a forged certificate which was confirmed by the government.[10] This lack of security is clearly a fundamental issue and any wider adoption of the passport would need to have a minimum level of security and prevention from forgeries before the public can use it with a degree of confidence.

- **Integration/Interoperability** – While a centralised Federal government-led passport would simplify product adoption, already the States are confirming that they are exploring their own version of the passport. At a minimum passports systems would have to account for integration (ability for different systems to connect/communicate usually through middleware) or interoperability (ability for

[8] Crowe (2021), '*Vaccine passports' to combine jab records with QR check-ins for more freedoms,* https://www.smh.com.au/politics/federal/vaccine-passports-to-combine-jab-records-with-qr-check-ins-for-more-freedoms-20210820-p58kmh.html

[9] Purtill (2021), *COVID vaccine certificates can be forged within 10 minutes due to 'obvious' security flaw*, https://www.abc.net.au/news/science/2021-08-23/covid-19-vaccine-certificates-forged-in-10-minutes/100390578

[10] Doran (2021), *Senator Rex Patrick forges COVID-19 vaccine certificate to expose security flaw,* https://www.abc.net.au/news/2021-08-04/senator-rex-patrick-forges-covid-19-vaccine-certificate/100346974

different systems to connect/communicate seamlessly) between these two systems so that the public will not have to use two different versions. Any market driven alternatives would also need to consider this. Interoperability becomes a larger concern once other passport versions – for example from those overseas need to be considered. Interoperability also has the potential to facilitate scope creep and unintended impacts if use cases aren't mapped out properly and defined.

PRIVACY:

- **Data access** – The combination of access needed to both the Australian Immunisation Register (AIR) and Medicare could open up access to potentially sensitive health information. Access should be carefully limited. Storage should also be restricted to a reasonable timeframe for use and subsequently deleted from passport records, or from venues using and processing the passports.

- **Data use** – Similar to data access, there should be safeguards in place so that records are used only for what it is intended – which is proof of vaccination. Often software developers and organisations take the opportunity to use data captured for secondary usage, usually for performance or optimisation purposes, but this is rarely clarified and users are rarely given the opportunity to consent. Recently it was revealed that Queensland and Western Australian police used their COVID check-in apps to solve unrelated crimes which is a clear abuse of the data captured by those apps.[11]

- **Data management and control** – Public health data regularly contains sensitive and private information. By digitising this information, there is potential for unwanted access or accidental disclosures to occur. Users/individual Australians should maintain complete control over the data in their passports. They should also be reasonably notified of any data processing, storage or capture of their details from any venues or other platforms that use the passport, or integrate/export details. Their consent should be obtained and have the ability to opt-out.

ETHICAL:

- **Access and coverage** – There is the potential for a large section of the population to not have access to the passport. Even those who are covered, but might have difficulties accessing digital services such as mobile phone and internet access, which could include the elderly, people with disabilities or those in remote areas may have

[11] Galloway (2021) '*Breach of trust': Police using QR check-in data to solve crimes,* https://www.smh.com.au/politics/federal/breach-of-trust-police-using-qr-check-in-data-to-solve-crimes-20210903-p58om8.html

trouble getting access. It is important then, that all use cases are planned and catered for to prevent many groups from being excluded.

- **Discrimination and human rights issues** – The examples of excluded groups above demonstrate how many people could be left behind and discriminated against because they are unable to have valid vaccination passports. The Australian Human Rights Commission notes that several groups could potentially face discrimination, including individuals with valid medical reasons for not getting vaccinated, including people with disabilities, marginalised groups that may seek to avoid contact with government agencies including migrants, and any young people or those who are last in line to receive the vaccine.[12] They also note that these exemptions may result in inadvertent revelations of a person's private health information – for example by revealing that they have a disability.

[12] Australian Human Rights Commission (2021), *Human rights considerations for vaccine passports,* https://humanrights.gov.au/our-work/rights-and-freedoms/human-rights-considerations-vaccine-passports

A blueprint for a safe, fair and ethical vaccination 'passport'

A successful vaccination passport could be developed which addresses all the key considerations presented in the previous section. The Office of the Australian Information Commissioner along with state and territory privacy commissioners and ombudsmen have produced the "National COVID-19 Privacy Principles" to create a standard national approach to any initiatives aimed at addressing the pandemic.[13] While these principles have some valuable recommendations, they do not fully address all the known risks and considerations of digitally enabled identification and monitoring as part of a national vaccination rollout.

We recommend the following principles to be developed for any vaccination passport:

- **Privacy by design** – Any proof of vaccination software should have privacy by design in its build. The Australian Privacy Commission have clear privacy principles, which should be adhered to and complied with.[14] These include conducting privacy impact assessments, with privacy protections overseen by relevant legislation with clear rules for breaches and clear accountabilities.

- **Purpose limitations** – Ensuring data is collected, stored and processed only for the express purpose it was intended for which is proving COVID immunisation status. No other secondary uses should be applied to data that is collected, stored and processed by the issuing body, developers or users such as venues.

- **Flexible user control and consent** – Ultimately users should have complete control over their data and the way it's managed. There should be flexible controls so that the level of disclosure can be managed, specifically as it could relate to other health or personal conditions or identification that users may want to keep private.

- **Data minimisation** – Ensuring only the minimum amount of data necessary is captured.

[13] Office of the Australian Information Commissioner (2021), *National COVID-19 Privacy Principles*, https://www.oaic.gov.au/privacy/guidance-and-advice/national-covid-19-privacy-principles/

[14] Office of the Australian Information Commissioner (2021), *Australian Privacy Principles*, https://www.oaic.gov.au/privacy/australian-privacy-principles/

- **Data use transparency** – How user data is used should be laid out in clear terms and conditions that all users can easily understand, containing clear and unambiguous definitions, minimal jargon and simple, succinct language.

- **Data expiry**– Data storage should have an expiry date tied to the purpose limitations of the vaccination passport – that is, once proof of vaccination has been fulfilled, data captured should expire or have the ability to be deleted. Should another phase or requirement for the data be generated, then a new set of terms and conditions should be consented to.

- **Safety and security** – Given the basic security flaws in the current digital certificate that were discovered, safety and security of any updates or new versions of the software should be rigorously tested for security and fraud. Safety devices, (like an official government watermark, a real-time clock, or holographic ticks or marks) should be utilised. Software should comply with the latest security standards online and regularly reviewed and updated for security purposes.

- **Allows for legitimate exemptions** – Some people (like the immunocompromised, people with disabilities, or with specific health conditions) will have legitimate reasons for not being able to get vaccinated, and these use cases should also be recorded and captured with any verification system, so that records are verified. This prevents people with no legitimate reasons from gaming the system or using this as an excuse to breach public health orders and hijack compliance systems.

- **Covers groups not eligible for Medicare** – Passports should allow coverage for people in Australia who are currently non-citizens, including residents, those with temporary working visas, international students and any other groups not eligible for Medicare.

- **Adopts a partnership with the private sector as needed** – As the urgency to contain the virus and mitigate against its effect grows, the government needs to look at the most effective and efficient operational models to provide this service to Australians. While there are different pros and cons from different operational models, the combination of a government and private led partnership is likely to be the most effective way of developing proof of vaccination. As complexities around the use cases for vaccination passports grow, including needing to account for overseas versions and irregular use cases, the government must provide options which cover all available use cases to ensure no one is left behind.

- **Allows for verifiable non-digital format** – While the majority of the Australian population have access to the Internet and smart devices, there are still those who

do not – which could include the elderly, people with disabilities or those who live in remote regions, a verifiable and official non-digital format needs to be supplied for these individuals so they are not excluded.

- **No biometric capture** – Biometric capture as a means of identification (for example using voice recognition, facial recognition or fingerprinting) is an ethical minefield and an area that has yet to have sufficient scrutiny and ethical frameworks applied to it. Biometrics should be avoided until the appropriate considerations and consultations have been further developed with the community and relevant experts.

Conclusion

Vaccination ‘passports’ are potentially critical tools to help Australians move forward from the lockdowns and restrictions of COVID-19. However some key technical, privacy and ethical considerations needs to be addressed to ensure that the passport is safe and fair to all Australians. A blueprint for the ideal vaccination passport should develop key principles like privacy by design, purpose limitations and data minimisation to ensure equity in this crucial public health policy.