Building robust and ethical vaccination verification systems

Baobao Zhang,^{1*} Laurin Weissinger,² Johannes Himmelreich,³
Nina McMurry,⁴ Tiffany Li,⁵ Naomi Scheinerman,⁶ Sarah Kreps¹

¹Department of Government, Cornell University,
214 White Hall, Ithaca, NY 14853, USA

²Fletcher School of Law and Diplomacy, Department of Computer Science, Tufts University
161 College Avenue, Medford, MA 02155, USA

³Maxwell School of Citizenship and Public Affairs
Department of Public Administration and International Affairs, Syracuse University
200 Eggers Hall, Syracuse, NY 13244, USA

⁴Institutions and Political Inequality Unit, WZB Berlin Social Science Center
Reichpietschufer 50, 10785 Berlin, Germany

⁵School of Law, Boston University
765 Commonwealth Avenue, Boston, MA 02215, USA

⁶Department of Medical Ethics and Health Policy, University of Pennsylvania
423 Guardian Drive, Philadelphia, PA 19104, USA

*To whom correspondence should be addressed; E-mail: bz377@cornell.edu.

December 30, 2020

As countries begin to vaccinate their populations against COVID-19, creating systems to verify vaccine records will be vital to reopening businesses, educational institutions, and travel. We consider the challenges of building vaccine record verification (VRV) systems that involve data sharing by health care

providers, methods for verifying vaccine records, and regulation of how entities (e.g., workplaces, schools, businesses, and airlines) may request proof of vaccination. In particular, we focus on the opportunities and risks associated with digital vaccine passport apps. We propose three ethical principles to guide the building of VRV systems: 1) aligning systems with vaccine prioritization, 2) upholding fairness and equity, and 3) building trustworthy technology that protects the public's health data.

In less than a year, scientists worldwide have developed effective vaccines against COVID-19. Public health authorities are now deliberating policies around the verification of vaccine records. Instead of focusing solely on the technical details, we consider vaccine record verification (VRV) as a system, as illustrated in Fig. 1. The system involves 1) data sharing by health care providers, 2) methods for verifying vaccine records, and 3) regulation of how entities (e.g., workplaces, schools, businesses, and airlines) may request proof of vaccination. Building robust and ethical VRV systems will be vital to reopening businesses, educational institutions, and travel.

Historically, governmental agencies have played a dominant role in VRV systems by issuing paper records. But now, non-profit organizations, corporations, and academic researchers are developing digital verification systems. For instance, a non-profit organization has created an app called CommonPass to verify users' COVID-19 test results and, soon, vaccine records for safer air travel. Tech companies, including IBM, are developing similar apps. Beyond airlines, other businesses, employers, and educational institutions may rely on digital vaccine passports in the future (*1*).

We acknowledge that building VRV systems for the COVID-19 pandemic poses both opportunities (e.g., more accurate verification) and risks (e.g., exacerbating health and economic inequalities). In Fig. 1, we pose key policy questions associated with each component of the

system and the system as a whole. We argue for increased oversight to govern the development and use of VRV systems. Based on our analysis, we endorse the following ethical principles to guide public health authorities, policymakers, health care providers, and software developers:

- Aligning VRV systems with vaccine prioritization
- Upholding fairness and equity to avoid discrimination against individuals who cannot access vaccines
- Building trustworthy technology that protects the public’s health data

Background

We consider how three existing public health surveillance measures could inform policies around verification of COVID-19 vaccine records.

Paper vaccine record cards

The idea of an internationally-recognized VRV system is not new. In the 1920s and 1930s, countries began tying air travel to health certificates to verify inoculation against certain diseases. In 1951, the World Health Organization (WHO) took existing measures a step further by establishing the International Sanitary Regulations that aimed to limit the international spread of disease. An International Certification of Vaccination, known as the *carte jaune*, followed in 1959 and logged an individual’s vaccination history to meet countries’ exit and entry requirements (2). The WHO publishes vaccine requirements, largely an annual update on yellow fever vaccination requirements across countries. The longstanding success of the *carte jaune* suggests that paper-based vaccine records should not be abandoned. (Indeed, countries including the U.S. and the U.K. are issuing paper vaccination cards.) Unlike digital health records, paper

records are less error-prone (e.g., not sensitive to internet connectivity), do not exclude those without smartphones, and can serve as a backup for digital verification tools.

Immunity passports based on antibody tests

In the middle of 2020, several countries considered adopting immunity passports in the form of a certificate or app that would verify that an individual has neutralizing antibodies against COVID-19 (3). These antibody immunity verification proposals were not adopted because they could have encouraged individuals to become infected with the virus. Furthermore, concerns about the sensitivity and specificity of serologic tests and the possibility that people can become reinfected with COVID-19 added additional roadblocks (4).

Vaccine records would eliminate many of the problems associated with immunity passports based on antibody tests. Nevertheless, one concern remains: Immunity passports, whether based on antibody or vaccine verification, could create a two-tiered society: those who have greater freedom to work, travel, and perform other activities versus those who do not. Therefore, we argue in our recommendations that public health policies must uphold fairness and equity by not punishing people who cannot (yet) access vaccines.

COVID-19 exposure notification apps

COVID-19 exposure notification apps, designed to supplement manual contact tracing, illustrate the potential problems associated with implementing technological solutions quickly in a pandemic. Although many countries have adopted the Google/Apple Exposure Notification system that is privacy-preserving, use rates in the U.S. and Europe remain relatively low (5). Concerns about vaccine passport apps are likely to be similar to concerns about contact tracing apps: privacy violations, government/private surveillance, and abuse of the collected data (6). Widespread adoption of vaccine passport apps requires overcoming public distrust of this new

technology and the government and private organizations that run them.

Challenges of building VRV systems

Health care providers

Health care providers that are vaccinating patients face challenges regarding the storage and sharing of vaccine records. VRV systems require the mass collection of health data, generally understood to be particularly sensitive information under most privacy law regimes (e.g., the EU General Data Protection Regulation). Electronic transfer of health information also incurs legal obligations under regulations like the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. Beyond legal concerns, the U.S. also faces information technology (IT) hurdles because many health care providers do not enter vaccine records into online immunization information systems (IISs) that facilitate data sharing. As of 2019, only 60% of U.S. adults' vaccine records were in IISs (7). Expanding health care providers' IT capacity would require considerable resources.

Another important question is with whom health care providers should share vaccine records and what specific data would be shared. Currently, there is a proliferation of third-party software developers building vaccine passport apps. Without oversight or credible information about these app developers, health care providers may be (rightly) hesitant to share vaccine records. Patients may also be reluctant to participate because they fear that these apps could leak sensitive medical data.

Verification methods

One central debate regarding verification methods is whether vaccine passport apps should supplement paper cards or replace them entirely in some cases. While some express concerns that paper records are easy to fake, paper vaccine records have a proven track record.

Well-designed vaccine passport apps can prevent fraud. Nevertheless, apps must be designed with privacy, security, and transparency in mind to protect medical and personal data. App-based verification will not work well in areas where health care providers do not have the technical capacity to share data, where many people do not own smartphones, or where people distrust the apps and the actors developing the apps.

One lesson from the exposure notification app experience in the U.S. and Europe is that public trust in new technology and the actors developing and managing this technology is vital for widespread adoption. In a survey conducted in early December 2020, we found that the U.S. public does *not* prefer paper records over cellphone-based verification. In our survey (results shown in Fig. 2), 54% of U.S. adults support requiring cellphone-based verification to travel on airplanes and public transportation, compared with 52% for paper records. Nevertheless, 46% said that requiring cellphone-based verification would violate privacy, compared with 39% for paper records. Even if vaccine passport apps were made mandatory, failing to establish a trustworthy and privacy-preserving app could cause long-term distrust in tech companies and governmental institutions.

Entities requesting proof of vaccination

While educational institutions and some employers have traditionally required proof of vaccination, many more entities (e.g., landlords, stores, restaurants, cinemas, airlines, and public transit) may soon request it as well. Who is allowed to request proof of vaccination, when they are allowed to begin request proof, and what type of verification they will (have to) accept are currently being debated.

From a legal perspective, U.S. law provides little recourse against discrimination based on immunity verification. Both states and private businesses have broad power to implement mandatory vaccination requirements. U.S. laws protecting health data (e.g., HIPAA and the

Genetic Information Nondiscrimination Act) do not prohibit discriminatory uses of immunity information. The Americans with Disabilities Act (ADA) also does not protect against discriminatory impacts of immunity verification. Indeed, the ADA allows employers to limit hiring to individuals who “shall not pose a direct threat to the health or safety of other individuals in the workplace.” The U.S. Equal Opportunity Employment Commission (EEOC) released guidance in December, stating that employers can legally mandate vaccinations, provided that accommodations are made for individuals with disabilities or those seeking religious exemption.

As immunity verification will likely impact fundamental rights like housing, education, and employment, the absence of strong legal protections is troubling. Laws should balance protecting the health of the public and preserving fundamental human rights. At the very least, entities should not make impossible demands on individuals, such as requiring them to jump the vaccine prioritization queue when vaccine supplies are limited, as we will discuss in the next section.

Guiding ethical principles

Based on our discussion of the associated challenges, we propose the following principles to guide the development of VRV systems.

Aligning VRV systems with vaccine prioritization

Public health authorities have made painful trade-offs in deciding which groups should be given priority in the COVID-19 vaccine queue (8). Proof of vaccination requirements need to be aligned with vaccination prioritization. Only those who can get a vaccine ought to be subject to mandatory proof of vaccine. When VRV is required for international air travel, for example, then anyone who is at the back of a vaccine queue but who urgently needs or wants to travel, can neither get a vaccine nor travel. This dilemma could create incentives to change vaccine prioritization plans to allow travel for those who are otherwise at the back of the queue, thereby

undermining the principles that informed the vaccine prioritization plan in the first place. Plans informed initially by medical and social needs could be amended to satisfy economic or political interests instead. However, vaccine verification could complement and substitute for required pre/post-flight testing and mask-wearing to make travel safer.

Upholding fairness and equity

The COVID-19 pandemic has exacerbated existing socioeconomic inequities by disproportionately harming ethnic minorities and low-income individuals (9). VRV systems should ameliorate rather than exacerbate these inequities so that those most exposed do not then suffer the most scrutiny when unprotected. Individuals who cannot access vaccines while supply is limited should not be denied public services, employment, education, or travel. Likewise, those who cannot receive the vaccine for health reasons (e.g., those with severe allergies) should also not face discrimination. Furthermore, governments and/or employers should pay for not only the vaccines but also medical treatments for severe side-effects. Finally, as we noted earlier, official paper vaccine records should be accepted so that those who do not own smartphones are not discriminated against.

The fairness and equity principle should be applied internationally as well as domestically. While the vaccines will likely be widely available to the public in developed countries in 2021, some low-income countries will not see mass vaccination in the upcoming year (10). Developed countries should not curtail immigration and travel from developing countries by imposing strict vaccine requirements that cannot be met.

Upholding fairness and equity may be costly: the public must adhere to measures to prevent COVID-19 spread (e.g., social distancing, mask-wearing, and surveillance testing) until vaccines are widely available and herd immunity is reached. Nevertheless, keeping these preventative measures in place is prudent until we have more data regarding whether vaccination

prevents asymptotic transmission (11).

Once COVID-19 vaccines are widely and easily available, entities may — and perhaps ought to — require vaccine verification. Permitting such policies would be in line with the individual autonomy of entities in the private economic sphere and protect individuals’ health. Moreover, such requirements would likely incentivize vaccination.

Building trustworthy technology

Any vaccine passport app should be privacy-preserving and secure. As a core technical design tenet, the app and its back end should only collect and store data necessary for the app to function. All data should be securely deleted once it is no longer needed. Developers should avoid including any functionality that tracks unnecessary data or and avoid implementing any third-party tracking or dependencies (12, 13). All data communications should remain end-to-end secure between user devices and the data controller’s infrastructure. Vaccine passport apps should also maximize privacy-preservation: individual users should be able to verify their vaccination status without sharing personally identifiable (PII) or personal health information (PHI) with the verifying entity. This is technically and cryptographically feasible (14).

The application and back-end should implement strong and positive security controls. Program logic and back-end protections should include role-based access controls to ensure that users can only access the information they require to complete the specific tasks assigned to their role within an organization during a particular time frame. PHI and PII should never be collected, accessed, used, analyzed, or shared without verified expressed user opt-in. Furthermore, the data controller should implement strong internal controls and safeguards to prevent staff from accessing any personal data without appropriate process, such as third-party approval, the four-eyes principle (i.e., two individuals being required to complete the process), documentation, and alerts to affected individuals.

The most effective way to increase the trust in, and the security of, the solution is to use an open-source approach for application and back-end services, as demonstrated by the German Corona Warn App. This approach allows for crowd-sourced (automated and manual) security review (15). Trust in institutions, both private or governmental, develops slowly and has taken serious hits in recent years (16). However, the availability of source code would allow regulators, security experts, and the press to peruse and improve the source code of the app, building necessary trust in the VRV system.

References

1. N. Singer, Vaccinated? Show us your app. *New York Times* (December 13, 2020).
2. J. G. Frierson, *The Yale Journal of Biology and Medicine* **83**, 77 (2010).
3. R. C. H. Brown, J. Savulescu, B. Williams, D. Wilkinson, *Journal of Medical Ethics* **46**, 652 (2020).
4. N. Kofler, F. Baylis, *Nature* **581**, 379 (2020).
5. A. Blasimme, E. Vayena, *Science* **370**, 760 (2020).
6. B. Zhang, S. Kreps, N. McMurry, R. M. McCain, *PLoS ONE* **15** (2020).
7. US Centers for Disease Control and Prevention, 2019 iisar data participation rates, *Tech. rep.*, US Centers for Disease Control and Prevention (2020).
8. G. Persad, M. E. Peek, E. J. Emanuel, *JAMA* **324**, 1601 (2020).
9. J. Patel, *et al.*, *Public Health* **183**, 110 (2020).
10. O. Dyer, *BMJ* **371** (2020).

11. D. V. Mehrotra, *et al.*, *Annals of internal medicine* **M20-6169** (2020).
12. A. Lerner, A. K. Simpson, T. Kohno, F. Roesner, *25th USENIX Security Symposium (USENIX Security 16)* (USENIX Association, Austin, TX, 2016).
13. B. Krishnamurthy, C. Wills, *Proceedings of the 18th International Conference on World Wide Web*, WWW '09 (Association for Computing Machinery, New York, NY, USA, 2009), p. 541–550.
14. D. Thilakanathan, R. A. Calvo, S. Chen, S. Nepal, N. Glozier, *JMIR Medical Informatics* **4**, e15 (2016).
15. T. Sonnekalb, *et al.*, *Proceedings of the 3rd ACM SIGSOFT International Workshop on Software Security from Design to Deployment* (2020), pp. 15–18.
16. Edelman, Edelman TrustBarometer 2020, *Tech. rep.*, Edelman (2020).

Acknowledgments

We are grateful for Farah Hasnie’s graphic design of Fig. 1 and Benjamin T. Miller’s copy-editing. Original survey research for this commentary was funded by a Social Science Research Council Just Tech Covid-19 Rapid-Response Grant and received IRB approval from Cornell University. The authors declare that there is no conflict of interest.

Fig. 1. Policy questions for building a vaccine record verification (VRV) system. The VRV system has three components: 1) data sharing by health care providers, 2) methods to verify vaccine records, and 3) regulations regarding how entities (e.g., airlines, stores, restaurants, schools, and workplaces) could demand proof of vaccination. We pose policy questions for building each component of the VRV system as well as for the system as a whole.

(a)

(b)

Fig. 2. U.S. adults’ attitude toward vaccine passports (certification on cellphone versus paper card). These survey results came from a survey of $N = 2,000$ U.S. adults that we conducted between December 4 and 5, 2020. In one section of the survey, respondents were randomly assigned to evaluate three out of 12 public health policies. One of the policies stated: “Once a vaccine becomes available, to use public transit or travel by train/plane, everyone would be required to show a government-issued certification on their cellphones confirming that they have been vaccinated against COVID-19.” Another policy had the same wording except “paper card” replaced “certification on their cellphones.” Respondents were asked how much they supported or opposed the policy using a 0 to 100-point scale. In (a), we present the distribution of responses. Categories in the figure divide the raw responses into five categories shown on the scale (0-20 = strongly oppose, 21-40 = somewhat oppose, 41-60 = neutral, 61-80 = somewhat support, 81-100 = strongly support). We also asked respondents to predict whether certain outcomes will happen if the government were to adopt the policy. In (b), we show responses to four of the eight outcomes most relevant to this commentary. The results were weighted to match marginal distributions of age, gender, region, race, income, and education in the U.S. adult population using data from the 2018 American Community Survey.