
MIT SafePaths Card (MiSaCa): Augmenting Paper Based Vaccination Cards with Printed Codes

Abstract

In this early draft, we describe a user-centric, card-based system for vaccine distribution. Our system makes use of digitally signed QR codes and their use for phased vaccine distribution, vaccine administration/record-keeping, immunization verification, and follow-up symptom reporting. Furthermore, we propose and describe a complementary scanner app system to be used by vaccination clinics, public health officials, and immunization verification parties to effectively utilize card-based framework. We believe that the proposed system provides a privacy-preserving and efficient framework for vaccine distribution in both developed and developing regions.

1 Introduction

Without an effective curative or preventative measure, the unprecedented coronavirus disease 2019 (COVID-19) pandemic has led to a significant amount of human deaths (1,900,000 at the time of publication[3]). However, now with the advent of vaccines, we face the challenges of strategic, equitable and privacy preserved ways for last-mile vaccine distribution[11].

First, the vaccine recipients must be dynamically prioritized to ensure an equitable reach, especially as multiple vaccines with different protocols are approved in various areas. In addition, once a citizen's first dose is administered, they must follow through with their second dose as well. Also, a communication plan must also be put in place to combat inevitable rumours, misinformation, and conspiracy theories aiming to disrupt citizen engagement in the vaccination process [10, 12]. It must also address the mistrust of vaccines in society [13], especially within previously marginalized minority populations[16]. This is why we must take a user-centric approach that preserves trust — vaccines are meaningless if citizens aren't willing to take them[9]. Lastly, the health outcomes (effectiveness, safety, long-term effects, etc) of the vaccines must be effectively monitored in a privacy-preserving way[2].

In today's society, multiple technological systems are being utilized by the Center for Disease Control (CDC) to combat these challenges [5, 15, 4]. For example, the Vaccine Administration Management System (VAMS) streamlines the vaccine distribution process for jurisdictions, employers, and healthcare providers. In addition, it's an effective user-centric system as it allows for vaccine recipients to schedule appointments, receive records of their visit, and receive reminders for a second dose [8]. The Immunization Information Systems (IIS) are a group of privacy preserving database systems that track all vaccinations within various areas [6]. Lastly, the Vaccine Adverse Event Reporting System (VAERS) is the prominent system for the monitoring of health outcomes [7, 1].

In our previous work, we detail the MIT SafePaths app-based protocol for vaccine distribution. In this paper, we introduce a separate user-centric card protocol that uses printed codes as a supplement to traditional paper based vaccination cards.

Please view our repository with more information, screenshots, and videos about the our system: <https://github.com/Path-Check/vaccine-diary>.

2 Card Flow

2.1 Overview

Here we present a vaccine distribution system utilizing physical SafePaths cards and four digitally signed QR code stickers (henceforth termed *Coupon*, *Badge*, *Passkey*, and *Status*). The digital signing of a QR code is simply a secure process of verifying the authenticity of the information contained in the QR code [14]. These QR code stickers are simply QR codes printed onto adhesive stickers that can then be attached to a user's physical card.



Figure 1: The 4 digitally signed QR code stickers (*Coupon*, *Badge*, *Status*, and *Passkey*) present on the SafePaths cards.

The digital signature of the QR codes take place as below **Certificate = (message, signature(messages))**

For each sticker below the message is as follows -

- **Coupon** = (number, total, city, phase, (age, job, comorbidities/sick))
- **Badge** = (coupon, dose_info, Hash(passkey()))
- **Status** = ((vaccinated = 0,1,2), Hash(passkey()))
- **Passkey** = (name, DOB, salt)
= hash:sj2d8k8hy7j

Name	Equation	Description	Example
Coupon	$\{m, \text{sign}(m)\}$ where $m = (i, \text{zip code, job type})$	Coupon code is signed by CDC and indicates the zip code and job type of the receiver	{ 37, 5000, Springfield, 1B, Teacher }
Badge	$\{m, \text{sign}(m)\}$ where $m = (\text{dose_info, coupon, hash(passkey)})$	Badge is available after 2 doses and it gives the information pertinent to the vaccine shot.	{ [Pfizer, "1st Dose", 1/1/2021], fe4c2, 3be33c20cc4c85a0c32f7bf5b4 }
Status	$\{m, \text{sign}(m)\}$ where $m = (\text{status, hash(passkey)})$	Contains bare minimum information to prove the user is vaccinated	{ vaccinated, 8f6de6db }
Passkey	ID = User_PII Key = salt	Key is the random salt used for increasing the entropy of hashed data	{ John Doe, 6363fe744f74ee8f280958 }

Table 1: This outlines the four QR codes and what information is digitally signed in it.

Our solution is intended to decouple the health information and personally identifiable information (PII) in this process. Thereby, we are essentially proposing to separate the eligibility of the vaccination from the distribution of it. This way we can have the health information centralised, whilst the PII information decentralised.

2.2 Vaccine eligibility confirmation

To accommodate the several-stage vaccination policies that countries have begun to employ, SafePaths cards will be distributed containing one digitally-signed *Coupon* QR code. This would be provided by a central government agency such as the CDC and made available to users either by an employer or local government location. A pseudo random identifier generated for this *Coupon* serves as the identifying information for the user throughout the remaining workflow. This *Coupon* would initially come with SafePaths cards while the remaining three adhesive stickers must be obtained and placed onto the card following vaccination events.

2.3 Vaccine administration

Check-in at a vaccination clinic would require the verification of a user's *Coupon*.

Upon vaccination, the vaccination clinic would create a digitally-signed record of immunization and print it as a QR code on an adhesive sticker. This adhesive sticker (henceforth referred to as the *Badge*) would contain information regarding vaccine lot, manufacturer, and first/second dose information. The *Badge* would also contain information regarding the time, date, and location of vaccination.

The vaccination clinic would also create a unique encryption key to encrypt the *Badge*. This key, as well as encrypted PII such as name, age, sex, etc. would be stored on a *Passkey* QR code, printed onto a *Passkey* QR sticker. This *Passkey* is required for decryption of PII and in-depth vaccination information (time, date, location of vaccination).

At this stage, a vaccine recipient would then have *Coupon*, *Badge*, and *Passkey* QR stickers.

2.4 Second Dose

When a user attempts to receive a second dose of a vaccine, the vaccination clinic would utilize a user's *Badge* to determine the appropriate vaccine type and dose and the *Passkey* to confirm a user's identity. Again, the user *Passkey* contains information that solely exists on the physical card carried by a user. Use of this sticker is required to decrypt in depth vaccination information for a patient contained in the *Badge* (location of vaccination, date, etc.). Once final vaccination has been performed, the vaccine clinic would create a fourth and final *Status* QR code sticker for a recipient's SafePaths card, which would simply indicate whether or not a user has been vaccinated. *Status* would not contain any further information and therefore would be unencrypted.

2.5 Record-keeping

User vaccination records could be linked by anonymized upload to a centralized system using a user's pseudorandom identifier. The user's *Passkey*, containing their encryption key that decrypts their PII, would not be uploaded to the CDC without consent. Alternatively, we propose an anonymous record keeping function in our Scanner App section.

2.6 Vaccination verification

Verification of immunization status might be required in various scenarios such as airline travel, return to school/work, etc. Vaccine verification at these venues would follow the receipt of a second COVID-19 dose.

Information regarding an individual's vaccination status would be digitally signed by the vaccine clinic onto the *Status* sticker. When scanned, this sticker would provide the verifier with information regarding whether or not an individual has been vaccinated. If further verification of identity is required, the verifier could make use of a consenting individual's *Passkey* sticker to decrypt the holder's name. With this method, a user would have multiple levels of information they can share,

beginning with vaccination status in the unencrypted *Status* sticker, basic personal information (i.e. name) that must be decrypted using the *Passkey* sticker, and finally full personal vaccination information encrypted in the *Badge*.

2.7 Safety and efficacy monitoring

Short and long-term monitoring of health outcomes would rely on self-reporting. These cards could still facilitate the anonymous information upload by interacting with existing centralized systems such as VAERS or V-Safe while bypassing PII input. All health and symptom information could instead be tied to a user's pseudorandom ID. We also propose a scanner app solution in the Scanner Flow section that could aggregate symptom reporting and vaccine record data anonymously.

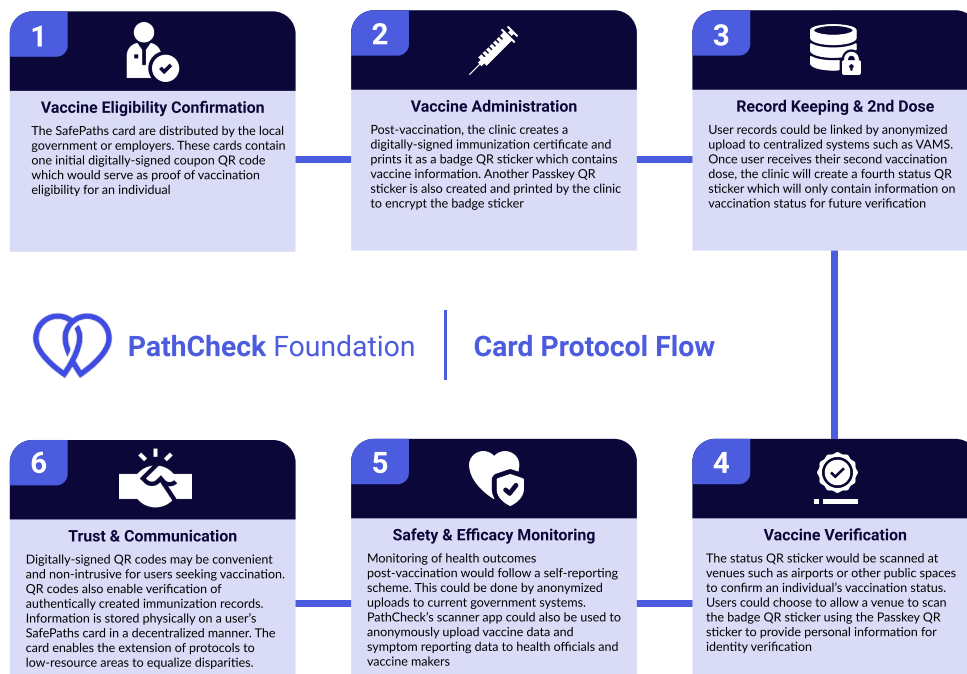


Figure 2: Card protocol workflow diagram.

3 Scanner Flow

3.1 Overview

Here we discuss the systems that must be built for vaccine clinics and distributors in order to enable the use of the SafePaths card framework presented above. We present several relevant protocols as well as the functionality of a proposed vaccine distributor/verifier scanner app. This scanner app would be necessary to function with the encrypted QR codes described above.

3.2 Vaccine eligibility confirmation

Phased vaccination using the SafePaths card system requires the distribution of SafePaths cards containing digitally signed *Coupons* to appropriate subsets of the population during each stage of vaccination. There are several ways that this might be achieved. We propose potential solutions below, though we recognize that these strategies must be determined by individual jurisdictions to meet the circumstances in different locations.

1. Disseminate to businesses to provide to employees (eg: hospitals, restaurants, etc. as appropriate)

2. Make available at local government building (similar to DMV process of obtaining a driver's license)
3. Mail out to individuals based on employment/other factors (via background check systems, centralized databases such as IRS)

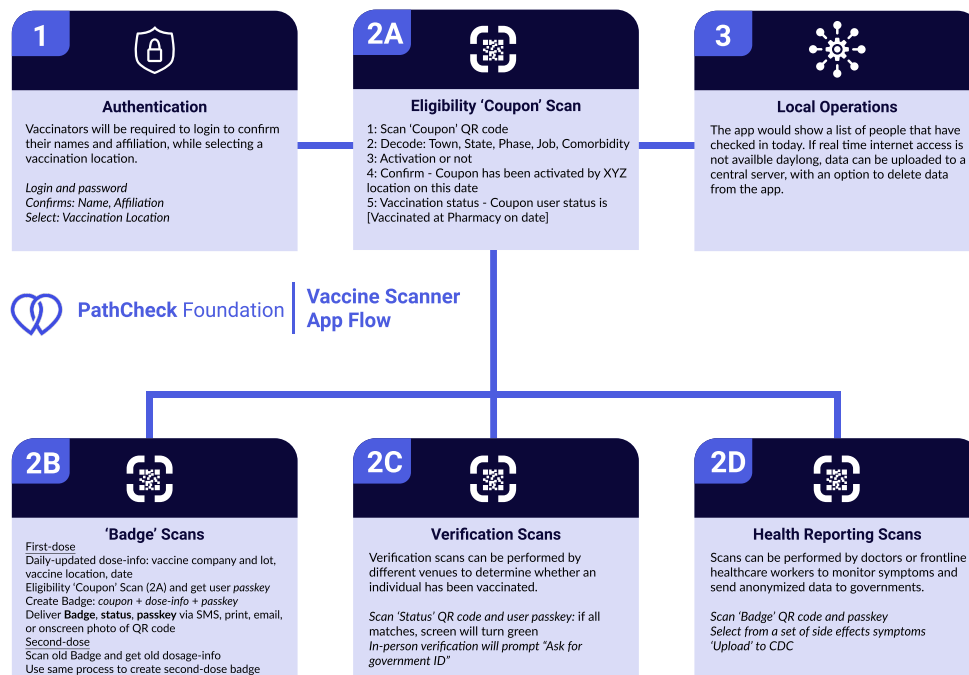


Figure 3: Scanner app protocol workflow diagram.

3.3 Vaccine administration

To confirm an individual for vaccination scheduling/check-in, a clinic must verify the authenticity of a vaccine recipient's QR *Coupons*. The first function of our proposed scanner app would be to scan a vaccine recipient's *Coupon* to determine authenticity and prevent the use of a single *Coupon* by multiple individuals. This would be achieved by scanning the digital signature present on a SafePaths *Coupon* and verifying its digital signature.

The second function of our proposed scanner app would be to create digitally signed *Badge* and *Passkey* stickers for post vaccination. This would make use of our previously described algorithm [14] for secure recording of vaccine information into a *Badge* sticker, encrypted using the encryption key present in the *Passkey*. After creating these stickers, the proposed scanner app would not store any information regarding a recipient's encryption key; that information would only exist within the *Passkey* sticker.

3.4 Second dose

Second dose administration functionality would be implemented into the scanner app in the same manner as described in the previous section for 'Vaccine Administration'. A *Status* sticker would be created by the scanner app in a similar manner to the *Badge* sticker, also drawing on the methods described in our cryptographic protocol [14].

3.5 Record-keeping

Another critical function of our scanner app would be the ability to integrate with existing systems, such as VAMS in the United States. Ideally, our app would be able to automatically provide vaccination record information to VAMS while replacing PII with pseudo identifiers.

Alternatively, our scanner system would also have the capability to directly aggregate vaccination record data in an anonymized fashion, retaining population-level statistics such as vaccination prevalence in a given jurisdiction that might be important for public health policy development. Details concerning clinic location, vaccine dose, and vaccine manufacturer could be stored by the scanner app and aggregated for public health official viewing.

3.6 Vaccination verification

Our proposed scanner app would enable vaccination verification simply by reading immunization status contained in a user's *Status* sticker. For further identity verification, a form of ID (such as driver's license) can be compared with the decrypted PII from the scanner app using an individual's *Passkey* sticker. The scanner app would not store this information following completion of the immunization confirmation.

4 Conclusion

In this early draft, we present a complete protocol for a physical card-based system for phased vaccine distribution, individual vaccination, second-dose adherence, and symptom follow-up. Due to their physical nature and simplicity, digitally-signed QR codes may be a convenient and non-intrusive modality for some users seeking vaccination. Digitally-signed QR stickers enable verification of authentically created immunization records, and the encryption schema presented using a unique passkey sticker ensures that user PII can only be decrypted with the user's consent. This information is stored physically on the user's SafePaths card in a decentralized manner wherein a user must provide their physical passkey sticker for decryption of PII. These cards also extend privacy-focused protocols to low-resource areas and populations, equalizing disparities in access to individual-centric solutions and frameworks for COVID-19 vaccination. The centralized health data collected (which is rid of all PIIs) can be used by the concerned authorities to have population aggregated view of the vaccine adherence in a region. Furthermore, such privacy preserving dashboards which show aggregated data can help the authorities take informed decisions.

References

- [1] U.S. FOOD & DRUG ADMINISTRATION. Vaers overview, 2019.
- [2] Joram Borenstein and Rebecca Weintraub. Rolling out the covid vaccine is a huge it challenge, 2020.
- [3] Center for Disease Control and Prevention. Cdc covid data tracker, 2020.
- [4] Center for Disease Control and Prevention. Using digital technologies in precision public health: Covid-19 and beyond, 2020.
- [5] Center for Disease Control and Prevention. Using telehealth to expand access to essential health services during the covid-19 pandemic, 2020.
- [6] Center for Disease Control (CDC). *About Immunization Information Systems (IIS)*, 2020. <https://www.cdc.gov/vaccines/programs/iis/about.html>.
- [7] Center for Disease Control (CDC). *VAERS | Vaccine Safety | CDC*, 2020. <https://www.cdc.gov/vaccinesafety/ensuringsafety/monitoring/vaers/index.html>.
- [8] Center for Disease Control (CDC). *VAMS | COVID-19 Vaccination Reporting Systems | CDC*, 2020. <https://www.cdc.gov/vaccines/covid-19/reporting/vams/index.html>.

- [9] Schoch-Spana M, Brunson EK, Long R, Ruth A, Ravi SJ, Trotochaud M, Borio L, Brewer J, Buccina J, Connell N, Hall LL, Kass N, Kirkland A, Koonin L, Larson H, Lu BF, Omer SB, Orenstein WA, Poland GA, Privor-Dumm L, Quinn SC, Salmon D, and White A. The public's role in covid-19 vaccination: Human-centered recommendations to enhance pandemic vaccine awareness, access, and acceptance in the united states. *vaccine.*, Oct 2020.
- [10] Manuel Morales, Rachel Barbar, Darshan Gandhi, Sanskruti Landuge, Joseph Bae, Arpita Vats, Jil Kothari, Sheshank Shankar, Rohan Sukumaran, Himi Mathur, Krutika Misra, Aishwarya Saxena, Parth Patwa, Sethuraman T. V., Maurizio Arseni, Shailesh Advani, Kasia Jakimowicz, Sunaina Anand, Priyanshi Katiyar, Ashley Mehra, Rohan Iyer, Srinidhi Murali, Aryan Mahindra, Mikhail Dmitrienko, Saurish Srivastava, Ananya Gangavarapu, Steve Penrod, Vivek Sharma, Abhishek Singh, and Ramesh Raskar. Covid-19 tests gone rogue: Privacy, efficacy, mismanagement and misunderstandings, 2021.
- [11] Kathleen Dooling MD MPH. Phased allocation of covid-19 vaccines, 2020.
- [12] Saad B. Omer. Rapid development of a vaccine won't help much if people refuse to take it, 2021.
- [13] Lorenzo Palamenghi, Serena Barelllo, Stefania Boccia, and Guendalina Graffigna. Mistrust in biomedical research and vaccine hesitancy: the forefront challenge in the battle against covid-19 in italy. *European journal of epidemiology*, 35(8):785–788, Aug 2020. 32808095[pmid].
- [14] Abhishek Singh, Ramesh Raskar, and Anna Lysyanskaya. Safepaths: Vaccine diary protocol and decentralized vaccine coordination system using a privacy preserving user centric experience, 2020.
- [15] Charlotte D. Smith and Jeremy Mennis. Incorporating geographic information science and technology in response to the covid-19 pandemic, Jul 2020.
- [16] Eric Toner, Anne Barnill, Carleigh Krubiner, Justin Bernstein, Lois Privor-Dumm, Mathew Watson, Elena Martin, Christina Potter, Divya Hosangadi, Nancy Connell, Crystal Watson, Monica Schoch-Spana, Tener Goodwin Veenema, Diane Meyer, E. Lee Daugherty Biddison, Alan Regenber, Tom Inglesby, and Anita Cicero. Interim framework for covid-19 vaccine allocation and distribution in the united states, Aug 2020.