Mobile Apps: A Decentralized Approach to COVID-19 Vaccination Coordination Prioritizing Privacy, Efficiency and Equity

Section 1: Background

The ethical need for efficient and rapid disbursement of limited COVID-19 vaccine doses demands that every step in the vaccine distribution process is carefully planned in advance to address the many challenges that have been described. These difficulties span areas in the logistics, monitoring of health outcomes, user-centric issues, and communication surrounding COVID-19 vaccines.

In this paper, we describe six critical functions that we believe vaccine management platforms must perform. We examine existing vaccine distribution systems, and present a model for a privacy-focused, individual-centric mobile app framework.

We believe that our decentralized, mobile app approach can address many challenges in COVID-19 vaccine distribution, supplementing other approaches while preserving patient privacy and maximizing public engagement. We also describe an alternative framework making use of digitally-signed QR code certificates for users that may not have access to mobile app capable devices.

Section 2: Use cases and functional requirements of vaccine management platforms

We have identified six critical functions that must be performed by user-facing systems in the continued distribution of COVID-19 vaccines. Each addresses important challenges that we have previously identified and described in equitable vaccine distribution.

2.1 Vaccination eligibility verification

The current phased vaccination schedules adopted by several national governments prioritizes specific subsets of the population for vaccination in order to maximize the societal benefit of initially limited vaccines. In the United States, healthcare workers and long-term care facility residents and workers will be the first to receive a vaccine, with following phases including essential workers, seniors, and those with high-risk medical conditions [1].

Confirming that an individual is a member of one of these eligible populations will be important in preventing fraud and ensuring that those who need vaccines receive one. However, this process is complicated by the importance of protecting recipient privacy; eligibility requirements depend in some cases on private individual information and measures must be set in place to ensure that this data is not misused.

2.2 Vaccine scheduling and administration

Coordinating the vaccination of large groups within small time windows will require efficient scheduling systems to optimize the number of individuals being vaccinated. These scheduling systems must be accessible and interoperable with an assortment of vaccination sites across a diverse range of populations and locations.

2.3 Second dose coordination and record linkage

Most vaccine candidates that are likely to reach widespread distribution require two-dose vaccination schedules for full immunogenicity. For maximum public utility it is imperative that individuals consistently receive both doses of a COVID-19 vaccine.

Furthermore, because studies have not been performed to determine whether taking a first dose COVID-19 vaccine from one manufacturer can be effectively complemented by a second dose from another manufacturer, current guidelines recommend that individuals should receive both vaccine doses from a single manufacturer. Effective systems must be implemented to facilitate this process and to monitor the relative efficacy of multi-manufacturer dose schedules if these guidelines are changed in the future. Record keeping and reminder systems must be developed to ease the logistical burden of coordinating adherence to these specific vaccine protocols. Again, privacy will be important in ensuring the protection of user data and records created to facilitate two-dose vaccination.

2.4 Vaccination verification

As the population continues to become increasingly vaccinated for COVID-19, methods of assessing and confirming vaccination status may be important for the relaxation of certain public health measures and shutdowns. There is some precedence for differing guidelines and policies for individuals that have and have not been vaccinated for other diseases, and these same immunity based-policies could be implemented in the United States and in other nations. Secure, fraud-resistant methods must be developed to confirm that an individual has been vaccinated if policies dependent on immunization status are enacted.

2.5 Safety efficacy monitoring

The novelty of COVID-19 vaccine platforms as well as the limited Phase III clinical trial data on their long-term efficacy and side effects can be supplemented by long-term health data collection. This will be important in the development of vaccination policies, public health measures, and can further elucidate differences in side effect manifestation and efficacy in diverse populations. Furthermore, this data can be used for quality assurance processes and aid vaccine manufacturers in improving vaccine technologies. Several challenges exist in the secure, privacy-focused collection of this individual protected health information (PHI).

2.6 Trust and communication

Every intersection between user engagement and any vaccine management system is an opportunity to build trust and provide transparent communication between all stakeholders involved in the vaccine distribution pipeline. Effective communication across these user-facing systems as well as thorough messaging surrounding their features and usage will be important in gaining public trust and increasing engagement.

Section 3: Centralized approaches

Centralized systems including the Vaccine Administration Management System (VAMS), the Vaccine Adverse Events Reporting System (VAERS), and the V-Safe After Vaccination Health Checker platform are being developed by the government to address various required functions across the pipeline of vaccine distribution. Some of these are developed in conjunction with private sector companies. The primary intended audience for these systems varies, and therefore there is also variance in user-experience.

3.1 User Flow

VAMS is a multifunctional, end-to-end platform for vaccine distribution and monitoring meant to be used by healthcare providers, employers, vaccine clinic managers, and vaccine recipients. The system includes processes for vaccine eligibility prioritization, appointment scheduling, dose recording, second dose reminders, and vaccination status verification. The separate Vaccine Adverse Event Reporting and V-safe After Vaccination Health Checker platforms enable the reporting of side-effects and symptoms that may be associated with vaccination.

While centralized systems such as VAMS are able to comprehensively monitor all aspects of the vaccine distribution pipeline and provide standardized protocols for vaccination and follow-up monitoring, they face several challenges in implementation and adoption from a user-centric perspective.

3.2 Challenges

3.2.1 Privacy and data security

VAMS requires input of extensive PHI including questions concerning HIV status, cancer diagnosis, and other pre-existing conditions. The centralization of data regarding vaccine distribution and efficacy opens the potential for the loss of personally identifiable information (PII) and PHI for large portions of the population if security breaches occur.

3.2.2 Logistics and efficiency

Due to requirements for the input of substantial amounts of information, usage of centralized government systems including VAMS, VAERS, and V-safe is a comparably time-intensive and complex process. This is the case not only for vaccine recipients, but other parties that might interact with these systems. For instance, employers must upload employees and employee contact information to VAMS in order to facilitate vaccination and clinic managers must set up online portals and inventory systems in VAMS. This can create unnecessary friction in the vaccine distribution pipeline.

3.2.3 Engagement and user-trust

Existing barriers to user trust and current vaccine hesitancy trends may be exacerbated by centralized systems requiring the input of large amounts of PII. State officials have voiced concerns that the collection of this PII is unnecessary for the monitoring of health outcomes and efficacy, and may be used for other purposes such as the identification of undocumented immigrants [2]. This has the potential to discourage vaccination in minority populations that are already being disproportionately affected by COVID-19.

3.2.4 Monitoring of health outcomes

Though centralized systems promise to comprehensively monitor health outcomes by the collection of large volumes of information, there are challenges to the use of this information in improving continued vaccination efforts. First, despite increased information collection, decreased user engagement can actually create a net deficit in reported vaccine side effects and efficacy when compared to lower-friction, privacy-focused solutions. Second, there has been no clear messaging on how collected data will be used and it is unclear whether vaccine manufacturers will be provided access to this information in order to continue to improve vaccine development.

Section 4: A decentralized, app-based approach

4.1 Vaccine Recipient User Flow

Our proposed mobile app approach for vaccine coordination focuses primarily on user engagement and individual health outcomes. This app will be computationally lightweight while also fulfilling numerous functions across eligibility confirmation, vaccine scheduling, side effect reporting, and vaccination verification. We also believe that it will be easily integratable into existing systems such as VAMS, ideally supplementing these approaches.

Entry into our proposed decentralized app-based solution for vaccine distribution would be non-restrictive. Any individual has the opportunity to download the open-source app and can begin to utilize features including the FAQ, symptom/vaccination dashboards, etc.

4.1.1 Vaccine eligibility confirmation

In order to book a vaccination appointment, the app will require a state or local government issued confirmation. This might take the form of a physical vaccine "coupon" provided to individuals physically either through mail, by an employer, or at a government pickup site. Verification of a user's eligibility for vaccination will be managed by the jurisdiction in providing these "coupons." Once a coupon is obtained by a user, it can be inputted into the app. At this point, our proposed app will not require the user to provide any personally identifiable information (PII) such as email address, phone number, name, etc.

4.1.2 Vaccine scheduling and administration

Following the input of a valid vaccine coupon, a user has the ability to create a vaccination appointment. Because the user's app has been verified by the input of a coupon, there is the opportunity for anonymized vaccination. Information about vaccination clinics and the vaccination methods that they support will be listed within the app (drive-through, walk-in, anonymous, etc.). Once a user has confirmed a vaccination appointment, they will receive a QR code that can be used to sign-in at a vaccination clinic.

The process of receiving a vaccine can also proceed anonymously. First, a user will be asked to provide relevant information concerning their eligibility for a COVID-19 vaccine within the app. For instance, current COVID-19 vaccines have not yet been tested in children, pregnant women, and in immunocompromised populations. Once a user has provided this information, the app will determine if the user is still eligible for vaccination. PHI and PII is not stored and is only used for the purpose of eligibility confirmation. Once this information is confirmed, the app will generate a QR code for check-in at a vaccination clinic. It is at this point that our proposed vaccine app solution might interface with VAMS in order to supply basic vaccine information. No PII will be transferred, but information about the clinic, first or second dose status, and non-identifying information such as age-range, race, and sex may be communicated to VAMS for record-keeping purposes. A randomized user identifier will be transmitted to VAMS in the place of a user's name.

4.1.3 Second dose coordination and record-linkage

Following vaccination, an individual can receive second-dosage information by using the mobile app to scan a clinic-provided QR code. In some cases, this might be in the form of barcodes already being created by various vaccine manufacturers for each dose. Otherwise, these codes might be printed by vaccination clinics or provided on physical information sheets handed to recipients following vaccination. Upon scanning this code, the app will store information about the vaccine dose an individual has received and schedule a reminder for a second-dose appointment with the same vaccine. The vaccine app will also generate a unique vaccine 'stamp' indicating that the user has received the first dose of a COVID-19 vaccine. Second-dose scheduling and vaccination follows the same workflow as above.

4.1.4 Vaccine verification

Following second-dose vaccination a vaccination verification badge will be generated for an individual. This can be used in the same way as a VAMS generated vaccination certificate as public health policies change and evolve to accommodate various forms of proof of vaccination status.

Additionally, our proposed app will enable a health verification challenge-based communication system enabling quick identification of vaccinated users in a privacy-minded, anonymous fashion. If vaccination becomes a requirement for entry to venues or participation in events, this system can be used to quickly and privately identify vaccinated individuals.

4.1.5 Safety and efficacy reporting

Following the receipt of a first-dose COVID-19 vaccine, a user will be periodically prompted to complete a symptom and side effect survey to monitor any potential side effects of COVID-19 vaccines. This enables the tracking of both long and short-term side effects as well as the efficacy of these vaccines. This data is not initially automatically uploaded from a user's device. Instead, it is stored for an individual to personally use in symptom and side-effect tracking and for comparison against aggregated trends. Should a user so choose, they are able to send an anonymized report of their data for aggregation and inclusion in studies surrounding long-term efficacy and effects of COVID-19 vaccines. We envision this anonymized data being provided to both vaccine manufacturers for quality control and vaccine technology improvement as well as government agencies for the continued development of public health policies. This anonymous data sharing is another point of potential contact between a decentralized app and systems such as VAERS or V-safe. At this stage a user is still not required to input PII, but can choose to do so if they desire a response from a government agency regarding any side effect or symptom concerns. Users can also receive notifications regarding safety and efficacy via push notifications rather than via personal contact information.

4.1.6 Trust and communication

App based platforms are ideal for the transparent and simplified transmission of information and educational resources. Our proposed app would contain clear guidelines sourced from government public health policy. Further, the open-source, open standards nature of the app allows careful examination by the public to build user trust.

It should be noted that user engagement with our proposed app solution will not end following vaccination. Continuing users will continue to be periodically prompted to input updates to their health status and any side effects that they may experience. This longitudinal platform can help supplement efforts to study and monitor the long-term efficacy and side effects of COVID-19 vaccines. At any point a user can choose to delete the app, clearing all data recorded by it.

4.2 Challenges

4.2.1 Privacy and data security

Our proposed app-based decentralized solution is intended to be exceedingly privacy-focused with little opportunity for data breaches or spoofing. The primary potential vulnerabilities exist only if a user should misplace their smartphone or with the possibility of targeted cyber attacks. However, because there is no centralized repository for personal information, these attacks cannot result in the loss of multiple individuals' records.

4.2.2 Logistics and efficiency

For an individual user, an app-based solution would be designed for convenience and user experience. We have outlined several points at which such an app might be interoperable with centralized systems such as VAMS and VAERS, but there still may be challenges in developing cooperative relationships enabling this interoperability. Nonetheless, our proposed app would be a highly efficient single source of all vaccine-related functionality for an individual user.

4.2.3 Engagement and user-trust

A primary difficulty in adoption of a vaccine management app arises if public messaging is ineffective in detailing the privacy-minded characteristics that set open-source, decentralized app-based solutions apart from centralized frameworks. User engagement and trust will hinge largely on effective communication and education surrounding the privacy and ease of use of app based solutions and the many privacy-preserving features they enable in contrast to existing centralized systems such as VAMS. The open-source nature of our approach enables a comprehensive description of features and security measures with complete transparency, which may be complemented with effective educational messaging to increase understanding of the relative benefits of app-based solutions.

4.2.4 Monitoring of health outcomes

While an app-based solution may solve several challenges faced by centralized systems with respect to privacy, convenience, and user engagement, it may still be difficult to properly incentivize users to report symptoms. Furthermore, should the app use anonymized data in aggregate for statistical purposes, there may be hesitancy and privacy concerns despite the lack of collected PII.

Section 5: Paper card with digitally-signed QR certificate approach for those without access to mobile apps

In cases where a user does not have access to a smartphone, there is still the possibility for privacy-focused, decentralized solutions for vaccine management and coordination. We propose a method whereby individuals receive three digitally-signed QR code stickers on a physical COVID-19 vaccine card (SafeBadge Card) that can be utilized for various vaccine distribution functions. These digitally signed QR stickers will be referred to as a vaccine coupon, badge, and passkey for the following description of user flow. Here a digitally-signed QR code refers simply to a QR code with information created by an entity in a verifiable, secure manner.

5.1 Vaccine eligibility confirmation

The first of the three vaccine stickers present on a SafeBadge card would be a unique vaccination coupon designating the holder of the card for vaccination during a given priority stage. Similar to the useflow presented for our proposed app solution, this coupon would be provided by a central government agency such as the CDC as a digitally-signed QR code and made available to users either by an employer or local government location. A pseudorandom identifier generated for this coupon code serves as the identifying information for the user throughout the remaining workflow.

5.2 Vaccine scheduling and administration

A privacy-minded framework for COVID-19 vaccination utilizing digitally signed QR codes would allow the booking of appointments using the pseudorandom identifier associated with a user's initial coupon sticker described above. Check-in at a vaccination clinic would require the verification of eligibility information contained in the QR code coupon. Upon vaccination, the vaccination clinic would impute a digitally-signed certificate of immunization on the second QR sticker, or the badge sticker. This sticker would contain information regarding vaccine lot, manufacturer, and first/second dose information. The vaccination clinic would create a unique encryption key for the recipient to encrypt identifying information such as name, age, sex, etc. into this badge sticker. This information would only be possible to decrypt using the unique encryption key for an individual which would be imprinted into the third QR sticker, or the passkey sticker.

5.3 Second dose coordination and record-linking

User records could again be linked by anonymized upload to a centralized system such as VAMS using the pseudorandom identifier associated with a user's coupon sticker along with an encrypted version of the user's badge sticker. The user's passkey sticker and information would not be uploaded to the CDC for decryption. When a user attempts to receive a second dose of a vaccine, a vaccination clinic would be able to use a user's passkey and badge sticker to determine the appropriate vaccine type and dose. Again, the user passkey sticker contains information that solely exists on the physical card carried by a user. Use of this sticker is required to decrypt PII for a patient contained in the badge sticker.

5.4 Vaccination verification

Vaccine verification 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 second vaccine sticker (badge sticker). This could then be used in conjunction with the passkey sticker for vaccination verification if COVID-19 immunization becomes a prerequisite for access in any scenario.

5.5 Safety and efficacy monitoring

Long and short-term monitoring of health outcomes would rely on self-reporting schemas in the context of digitally-signed QR code passes. These passes could still facilitate the anonymous transfer of information by interacting with existing centralized systems such as VAERS oe V-Safe while bypassing unnecessary PII input. All health and symptom information could instead be tied to a user's pseudorandom ID.

5.6 Trust and Communication

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 a user's consent. This information is stored physically on a user's SafeBadge card in a decentralized manner wherein a user must provide their physical passkey sticker for decryption of PII. These cards also are able to extend privacy-focused protocols to low-resource areas and populations, equalizing disparities in access to individual-centric solutions and frameworks for COVID-19 vaccination.

Section 6: Conclusion

The centralized and high information volume requirements of VAMS, VAERS, and V-safe facilitate country-level insights into vaccine distribution at a granular level stratified by a variety of individual identifiers. However, several challenges also exist in the widespread adoption of these systems due to concerns over data privacy and barriers to ease of use of these systems. Here we propose an app-based solution for vaccine coordination that can supplement centralized approaches and is user-focused, privacy-preserving, efficient, and easily scalable.

Key characteristics of our proposed vaccine monitoring app include the opportunity for anonymity and privacy in most steps of the vaccination process. Furthermore, this app consolidates each of the six most critical functions in COVID-19 vaccination into a single platform, streamlining the user experience and ideally increasing engagement. Our app also provides the opportunity for large scale, participatory data collection efforts to monitor side-effects and efficacy of COVID-19 vaccines without compromising privacy, ideally providing a source of de-identified health information for government policy development and vaccine manufacturer insights.

We also propose our SafeBadge card-based approach to extend privacy-preserving vaccine management systems to low resource areas and those without access to mobile devices.

Crucially, our privacy-preserving app and SafeBadge card systems would be interoperable with other vaccine coordination monitoring and administration platforms such as VAMS and VAERS, reducing the difficulty of integrating this new approach. We believe that this app-based approach can incentivize vaccination for individuals valuing personal privacy including undocumented immigrant populations and those with pre-existing health conditions.

FAQ

What are the benefits of this app for various stakeholders?

For public health agencies:

1. Interoperability between existing systems with processes for easy information sharing.
2. Coordination and Efficiency: Reduced dependency on digital IT systems working seamlessly with one another (hospital EMR systems, clinic management systems, centralized monitoring systems).
3. Feedback and monitoring: App-based reporting of symptoms and efficacy directly from vaccinated individuals can be reported in near real-time.
4. Communication: Possibility for targeted, contextual messaging and information sharing.
5. Data aggregation and dashboard visualization: Granular data anonymously reported from users can be used to monitor population-level trends.

For users:

1. Privacy: End-to-end system for vaccination without requiring the sharing of PII.
2. Equity: Allows anonymous access to all marginalized and vulnerable populations. The VaxSafe card system extends this to those without mobile app access.

3. Efficiency: Single platform for all functions of COVID-19 vaccination. Reduced requirement for redundant and intrusive data input.

For pharmaceutical companies and vaccine makers:

1. Quality assurance: Clear pipeline for side-effect data sharing that can supplement adverse event reports from VAERS. Opportunity for collaboration to build systems reporting the most relevant efficacy and side-effect information to monitor long-term side effects and efficacy.
2. Messaging: Opportunity for ‘recall’ of vaccine lots with reduced efficacy and ability to alert affected users.

How will we encourage users to download the app?
First, we believe that the benefits of a privacy-focused app will attract users prioritizing data-security in the COVID-19 vaccination process. We also believe that the efficiency and ease of use of our proposed vaccination framework will appeal to many individuals. Additionally, we plan to tap into an already large existing user-base of EN contact tracing app users. Finally, we will build on existing partnerships with medical centers and state governments.

Is this vaccine app a replacement for existing CDC or state systems? No. Systems such as VAMS/VAERS/V-Safe/IIS/IZ will still be important in widespread COVID-19 vaccination efforts. Our proposed app would provide an alternative method for vaccination that is privacy-sparing, efficient, and equitable while serving as a supplemental source of vaccine monitoring information.

How will this interface with VAMS/VAERS/V-Safe/ IIS/IZ? What changes are required?
Vaccine diary, second-dose and health status alert, and informational features of our proposed app would be independent of existing systems. The input of vaccination information upon administration of a vaccine and side effect/efficacy reports are two areas with potential for integration with government systems.

To verify and record vaccine administration, vaccination clinics or governments would need to provide signed QR codes that can be printed / copied by pharmacies or by users. This QR code would have information regarding the lot, manufacturer, and dosing of a vaccine which can then be verified by others with the appropriate digital key.

For interoperability of symptom/side effect reports, state or federal systems will need to allow the pseudorandom identifier associated with a user to be used for data identification purposes rather than PII such as name, address, etc. This is already part of the PPRL (privacy preserving record linkage) protocol for VAMS and IIS.

If you don't have PII, how can doctor or healthcare provider get in touch with the user?
Doctors and public health officials can contact users regarding pertinent information about their specific vaccine lot and other important details via app-mediated push notifications and contextual alerts. This is similar to ‘recalls’ in auto-parts, food safety, toys, etc.

What difference will it make? Wouldn't everyone be vaccinated anyway?
Significant chunks of the population still exhibit vaccine hesitancy and many may be unwilling to receive a COVID-19 vaccine. This app aims to potential barriers to vaccination by protecting data privacy, creating a convenient, streamlined user experience, and providing multiple vaccine-related functionalities in one platform.

Is this app primarily a vaccine passport or verifiable credentials?
This app does support vaccine verification while also including modules surrounding eligibility confirmation, dose scheduling and reminders, health assessments and symptom reporting, and providing users with push-notifications and contextual alerts.

How will you reach marginalized and low-resource communities?
We have also proposed state-produced physical vaccine cards that can be used for many of the functions of our app solution. This enables a privacy-focused solution for vaccination. Please see a thorough explanation in section 6.

Why should user trust the app?
Our app is developed using open-source code and open standards.

Why do centralized systems including VAMS and VAERS require so much PII and HPI?

PII including name, date of birth, and contact information is primarily used for user identification, contact, and record-keeping.

Health information is stored to determine eligibility for vaccination based upon exclusion criteria and to track the interactions between various medical conditions and vaccination.

Other personal information might be used for aggregate analysis and statistical purposes regarding equitable distribution among diverse populations.

Our app-based approach addresses each of these functions without the use of PII.

Identification of an individual for record-keeping is performed using a pseudorandom identification number rather than name or date of birth. Previous health information can be inputted into the app for exclusion determination where it is not stored. As soon as the app determines eligibility for vaccination information shared in these questions will be deleted. Symptom and adverse event reporting can be performed either anonymously or with personal information that might lend insight into vaccine and medical condition interactions. All demographic information can be anonymized and aggregated for reporting.

What if the user does not have a smartphone?
We expect users seeking a privacy oriented approach to vaccination to use a physical card containing a digitally-signed QR code from the government.

What is PathCheck and what role can it play?
PathCheck is a nonprofit organization originating in Dr. Ramesh Raskar's lab at MIT. We are the world's largest open source, open standards nonprofit organization for COVID-19 and conduct research across a broad array of problems stemming from the pandemic. PathCheck was the first organization to launch an EN app for contact tracing in COVID-19, successfully partnering with 6 US states and territories.

What is MIT SafePaths? What is its role?
MIT SafePaths is a set of standards protocols and algorithms. These are included as part of the open-source tools developed by MIT to help combat the COVID-19 pandemic.