Digital Health Passports: Key Considerations for Interoperability and Data Exchange

Introduction

The HIMSS Interoperability & HIE Committee focuses on advancing standards-based interoperability and emerging health information technologies that lead to impactful health information exchange (HIE). The committee members consist of top industry experts who are leading efforts in thought leadership and key initiatives advancing interoperability. Building on the group's crucial work, the HIMSS Interoperability & HIE Committee authored a white paper on the highly relevant and current topic of digital health passports, taking a look at vaccine passports amidst the COVID-19 pandemic. The members of this group tackled what they felt are the most pressing considerations when developing and implementing digital health "passports" (e.g., digital credentials or passes that include such information as vaccination and infection testing status).

This white paper and attached summary table are intended to level-set the definition, purpose, technological approaches, and functionality of digital health passports. The paper also explores challenges related to policy, regulation, privacy, interoperability, and global health equity. This succinct resource seeks to highlight and promote leading practices on what is being developed and implemented by focusing on specific use cases within the U.S. and internationally. By exploring varied digital health passport initiatives such as the Vaccination Credential Initiative (VCI), European Union Digital COVID Certificate, World Health Organization (WHO) Smart Vaccine Certificate, as well as leading practices in diverse geographic areas, this white paper will enable HIMSS' audiences to better understand the opportunities and challenges relevant to current solutions and those under development.

Why Does This Matter?

Public and private organizations have turned to the concept of digital health passports in an effort to safely and securely restore certain activities currently impeded by the COVID-19 pandemic. This topic is particularly pertinent because it affects people outside of care delivery systems and has been implemented in workplaces, restaurants, country borders, and beyond. With multiple U.S. and global entities seeking to create their own version of a digital health passport, there is an increased risk of creating numerous disparate systems that are not interconnected and thus have no universal applicability. Incompatible standards along with solutions that are not designed for interoperability will likely lead these efforts to create a fragmented system that undermines both the adoption and the utility of digital health passports.

In addition to the technical considerations needed to develop solutions, there are several important policy and ethical considerations for effective implementation. These include equity, privacy, and civil liberties, including consideration of the needs of those who are medically or otherwise ineligible for vaccination. All of these interests and values must be protected and enhanced in this effort to restore intra-national and cross-border mobility in the face of the COVID-19 pandemic and as these digital credentials are more widely applied to other use cases. As emerging digital health passports are developed and implemented, guidance on best practices, and a better understanding of the technical, ethical and policy considerations in the U.S. and globally will help the industry with meaningful, scalable adoption.

Examples of Existing Technologies and Objectives

As of December 31, 2021

Digital Health Pass	Technology Descriptions and Initiatives
Clear Health Pass	The Clear Health Pass is accessed via Clear's mobile app for smartphones. The software uses biometrics to identify the user, can integrate lab results from COVID-19 testing at over 30,000 labs, link to a personal healthcare account in order to confirm vaccine records, and offer a real-time health survey to screen for symptoms.
Common Pass	The CommonPass mobile app (which can be used directly or through an approved third-party app that is part of the CommonTrust Network) allows individuals to access their lab results and vaccination records through existing health data systems, national or local registries, or personal digital health records. The CommonPass platform then assesses whether the individual's lab test results or vaccination records (1) come from a trusted source, and (2) satisfy the health screening requirements of the country an individual wants to enter.
European Union Digital COVID Certificate	The EU Digital COVID Certificate contains a QR code with a digital signature. When the certificate is checked, the QR code is scanned and the signature verified, to be accessed digitally or in paper format. The Regulation on the EU Digital COVID Certificate will apply for 12 months as of July 1, 2021.
IBM Digital Health Pass	IBM Digital Health Pass technology allows businesses to establish entry criteria and validate health credentials in a decentralized way using blockchain technology. It can allow an individual to

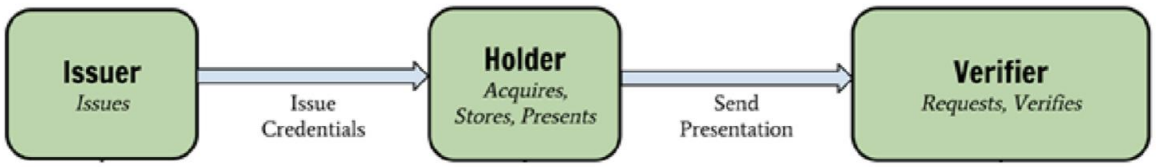
	manage their information through an encrypted digital wallet on their smartphone and maintain control of what they share, with whom and for what purpose, or is accessible utilizing a printable QR code.
International Air Transport Association (IATA) Travel Pass	IATA Travel Pass is a mobile app that helps travelers store and manage their verified certifications for COVID-19 tests or vaccines. This solution is powered by IATA Timatic.
Israel's Green Pass	Israel's vaccine pass. Effective on November 29, 2021, Green Pass is required for indoor gatherings of more than 50 participants. Accessible through website, smartphone app, self-service stations across the country, and via telephone at The Ministry of Health hotline.
Mvine-iProov passport	This technology enables people to register a test result or vaccination status without disclosing their identity. The medical professional administering the vaccine will be able to create the online certificate using a phone or tablet and then ask the user to add a selfie to their electronic certificate. The technology "does not discriminate against people based on the kind of smartphone they own, and there is a route for people who do not possess smartphones – i.e. a card-based method".
National Health Service COVID Pass	United Kingdom's official pass. The NHS app, which is used to book general appointments (not to be confused with the one currently being used to check-in to venues for contact tracing) is able to store negative test results and vaccine certification.
Scan2Fly Scan2Board	Air Asia developed Scan2Fly, an AI-based digital health pass in partnership with analytics company GrayMatter. AirAsia only accepts fully vaccinated passengers on its flights. GrayMatter also developed Scan2Board, a real-time Traveler Document Processing system where passengers can upload documents to automate the processing in a real time environment.
Vaccination Credential Initiative (VCI)	VCI™ is a voluntary partnership of public and private organizations committed to ensuring patients' access to a verifiable copy of their vaccination records in digital or paper form using open, interoperable standards.

	The breadth of VCI™ is to coordinate the standards and supply the implementation guides necessary to support the issuance of verifiable health credentials - signed clinical data bound to an individual identity. The open-source SMART Health Card Framework specifies the development and implementation specifications.
VeriFLY	VeriFLY was created by software engineering company Daon and consists of a digital health pass smartphone app. The app is flexible and aims to cater to various traveler requirements, with Daon adding that it would be possible to add a vaccine credential into the Verifly service in the future.
World Health Organization (WHO) Smart Vaccination Certificate Working Group	This group is focused on initiating key specifications, standards and a trust framework for digital vaccination certificates to offer effective implementation of interoperable digital solutions that contribute to safe COVID-19 vaccine delivery, monitoring, and verification.

Technical & Operational Considerations: Interoperability, Governance, Infrastructure and Data Exchange Needs

Digital health passports can be used in many different settings. Hence privacy, security and trust are paramount when it comes to capturing, storing and sharing key health information; these considerations must reflect the intended purpose. The technical considerations for a vaccination focused credential can be viewed from three different lenses as highlighted in W3C's Verifiable Credential Specification: Issuer, Holder and Verifier.

Conceptual Model



Adapted from Figure 1 of the W3C Verifiable Credentials specification

Source: https://spec.smarthealth.cards/

Issuer: An entity or organization that is capable of generating and issuing the verifiable credential. For digital health passports, this concept represents the organizations where a person received their vaccination, what vaccine a person received and potentially the results of a COVID-19 test. Any organization, (e.g., clinical labs, state agency such as a state department of health, community health center, healthcare provider, immunization registry) can take on the role of issuer. An issuer would create a paper or digital health card that would include the minimum data necessary for representing the vaccination details. In order to ensure privacy, only a limited set of data should be made available, depending on the use case. For example, an issuer responsible for generating a vaccination credential would likely omit such data elements as a person's phone number and address and include data related to the vaccination, such as vaccine code, manufacturer, status, date and location.

Holder: A person that received the verifiable credential. This actor would be the person that received the vaccine or a caregiver that received the health credential, whether paper or digital form. The holder is responsible for sharing this information with entities that they trust and that have a need to access this information. This model represents an opt-in scenario in which the holder takes an explicit action to share the information on the credential with the entity or organization for a specific intended use.

Verifier: An organization or entity that would need to verify a vaccine credential for various use cases such as safe to fly, back to school, back to work, etc. A verifier would verify that the health card information presented by the holder is valid and checked against trusted issuers. The verifier could also instigate certain decision-making rules on the data presented, such as a simple "Yes/No" for safe to travel based on various regulatory and organizational compliance requirements. Verifiers will also have many other responsibilities such as not storing or sharing the data except during the process of verification and making sure the digital signatures associated with the credential are valid. Verifiers can also build additional rules, such as applying or requiring a negative test result or vaccine dose count to enforce a specific policy, such as "allowed to fly".

Standards organizations like Health Level Seven® (HL7®) are currently defining FHIR® implementation guidelines 1 for vaccine and testing data to constrain the FHIR resources for these data elements to the minimum data necessary for the intended use. This implementation guide also accounts for multiple doses of vaccines, including booster shots. Vocabulary standards organizations like SNOMED have updated their nomenclature to include the new codes to support semantic interoperability. The key innovation supporting these new standards-based technical implementations is the SMART Health Card, which not only creates a framework to support many different use cases, but also provides tools to support implementation across all stakeholders.

In addition, implementation-focused organizations such as VCI and CommonTrust Network provide sustainability for digital passports by developing necessary data and interoperability standards and creating trusted entities. CommonTrust Network is a charitable organization that currently maintains a list of verified issuers. To be recognized as part of the CommonTrust Network, issuers must be confirmed as trusted entities and must issue verifiable credentials. VCI is a voluntary public private coalition that is working

to harmonize the standards and produce the implementation guides needed to support the issuance of verifiable health credentials.

Ethical Considerations: Privacy, Consent, and Vaccine Availability

Designing and implementing technical solutions that support public health recommendations while encouraging people to modify their behaviors in ways that reduce the transmission of disease, can sometimes produce conflicting objectives. With the COVID-19 pandemic, as the science is evolving and public health measures are increasingly politicized, maintaining the public's trust has become more of a challenge.

Digital health passes may change the pandemic-related experience of the average person to the extent that someone with a pass may be able to have a lifestyle akin to that of a person living before the COVID-19 era. A relevant example is TSA PreCheck, in which those who can afford the time and cost to undergo the background check are able to use separate TSA PreCheck lines at airports. Those lines offer essentially the same service offered to everyone before 9/11.

Digital health passes will be most effective where the protection or convenience they offer is worth the cost of implementation for both the individual and society. More broadly, development and implementation of a global system of interoperable digital health passes must take into consideration not only the COVID-19 pandemic but also other relevant public health needs, including future pandemics. In the United States, with its highly federated and fragmented health care delivery system, most early activity in issuing and requiring health passes has come from the private sector and educational institutions. In the face of such fragmentation, in the U.S. and globally, it is especially important that systems and processes issue and use health passes that adhere to standards published by a recognized country-level, or a global health care standards-development organization. Existing standards work (e.g., HL7® FHIR®), can support the needed standardization efforts for digital health passes via their respective input process for updates.\

Health IT developers (e.g., EHRs) whose systems interoperate with other stakeholders (e.g., immunization registries, provider organizations, and others authorized to use data from these systems), could then have access to vaccination records in a nationally standardized format. Similarly, patient portals and patient-facing apps could display these passports, or they may be placed in mobile digital wallets via standard methods. International interoperability may be facilitated through a global base standard that is then constrained and extended as needed for use in specific countries.

Considerations for Use of Passports in Denying Access

Requiring the use of health passports is a decision that should be made based on public health guidelines that reflect current scientific evidence. When evaluating requirements for, or use of, credentials, it is important to consider what kinds of entities can require use to approve or deny access. It is also important to consider if there should be exceptions, who would qualify for them, and what and how credentials should be verified. Policies reflecting these considerations may have a secondary function as signaling devices for

individuals to gauge the safety of a given event or activity, aiding in their decision whether to attend.

Technology-based solutions to support health passports need to consider both national and sub-national laws in the U.S. and other nations. Additionally, implementers should focus on what technology and policies are appropriate in terms of the level of assurance for both the identity of a person, and of the specific digital health documentation (e.g., the National Institute of Standards and Technology (NIST) Identity Assurance Level (IAL) 2 or 3). IAL2 offers a substantial degree of identity verification and validation while still allowing these processes to be completed remotely. IAL3 requires in-person contact. There is discussion as to whether IAL1 (i.e., multi-factor authentication) provides the level of verification that is needed for sharing and making decisions about health information, like a vaccination status.

Equity and Access Challenges

There are significant equity challenges regarding the roll out of, and access to, the various COVID-19 vaccines. Health passport requirements should be determined based on current public health guidance, taking into consideration vaccine availability. The rationale for such use depends on the severity of a pandemic and/or whether the disease becomes endemic.

As the industry develops needed technology for government and other organizations to identify and use specific tests and results in lieu of documentation of immunization, there are many considerations that need to be taken into account while the science and public health guidelines advance. It is important to recognize that what is built from a technological perspective must support multiple different approaches. Systems that provide feedback that is used in decision making need business logic that is based on clinical and epidemiological evidence. For example, if there is a medical consensus as to the reduction in risk of spread of COVID-19 from an individual who has a negative test, what kind of test was it? How long has it been since the test was performed? What is this individual's COVID-19 or exposure history? A negative test by itself may be acceptable in some circumstances, such as to attend a one-time event, but likely would not be considered equivalent to a vaccination status that is considered adequate protection.

Policy Considerations: United States & European Union

The following section highlights public policy considerations from the United States and European Union perspectives. It explores the recent policy contexts, privacy and security, and cross-border exchange for digital health passports.

U.S. Digital Health Passes Overview

Production and uptake of digital health passes has been affected by the primary role of U.S. states with respect to their constitutionally reserved public health powers. Concurrently, given the divisive political context in the U.S over vaccine mandates and vaccine credentials (AKA, "vaccine passports") at a national level, states' ability to drive the use of vaccine passes has presented an opportunity to move this agenda forward.

In addition, the federal government will face increasing pressure regarding vaccine passes as international travel increasingly opens up and depends on vaccination status. In this regard, it is noteworthy that the U.S. CDC Technical Instructions for provision of proof of COVID-19 vaccination status permit both paper and digital proof, with examples of verifiable digital proof including: The states, "Vaccination certificate with QR code, 1 digital pass via Smartphone application with QR code1 (e.g., United Kingdom National Health Service COVID Pass, European Union Digital COVID Certificate)". These technical instructions are used, in part, to implement recent CDC and U.S. Presidential orders and proclamations. The CDC technical instructions also provide very general guidance for reviewers of the credential to confirm their acceptability (i.e., determine record was issued by an official source (e.g., public health agency, government agency, or other authorized vaccine provider) in the country where the vaccine was administered).

California, New York and Louisiana are among those deploying SMART Health Cards developed by the Vaccination Credential Initiative (VCI) and other states are reportedly considering this approach, while other states are either not taking any action, or banning use of or requirements for COVID-19 vaccination and proof of vaccination status.

E.U. Digital Health Passes Overview

The Member States (MS) of the European Union are, in principle, autonomous when it comes to decisions regarding national healthcare. However, the COVID-19 pandemic has resulted in joint efforts to develop the common EU Digital Covid Certificate (EU DCC). Under the EU eHealth Network), representing all MS as well as the EU Commission, technical experts from several countries have worked intensively on the DCC solution, supported by semantic and legal expertise, and the technical solution is completed by a cross-border trust framework. The resulting regulation was adopted by the EU Parliament (2021/953 and 2021/954) and went into force for all MS on July 1st, 2021.

U.S. Privacy and Security Considerations

There are certainly privacy and security concerns in the U.S. and globally regarding digital health passes, including the extent to which the credentials reflect actual vaccination status and are not used in a fraudulent manner. It is noteworthy that the Smart Health Card Framework, while relying on validated data obtained from vaccination providers, vaccine registries and other authoritative sources, is designed (reflecting Privacy by Design principles) to provide maximum control by the card-holder on whether and when the information on the card is shared. It is also important to recognize that a digital credential can provide a level of convenience that is not met by having to retain and carry a paper credential (e.g., to meet requirements for international travel or entrance to public venues). The VCI Framework addresses critical privacy and security concerns through a multi-pronged strategy that, conceptually, is applicable to other models in the U.S. and globally.

The lack of a national immunization registry and variability even within states can be a limiting factor in timely and uniform rollouts of vaccine credentials. At the same time, a distributed approach to such credentials, as reflected in the VCI Smart Health Card

Framework, is well adapted to such variability, as vaccination providers and registries can issue credentials on a rolling basis. A major challenge, however, is how to issue credentials securely and authoritatively for vaccinations that were provided before these credentials were available, especially if they were not entered into a state vaccination registry.

E.U. Privacy and Security Considerations

The General Data Protection Regulation (GDPR) is the main EU regulation governing the handling of personal data, and it is applied by all member states of the EU. GDPR regulates the use and handling of personal information, clarifying and empowering the citizen's control over his or her personal data, for instance health data. Complementary to this regulation, the more recent EU regulation for the EU DCC states that the healthcare providers are responsible for providing the necessary information for issuing the DCC, but only by request from the individual.

The EU DCC system is constructed in such a way that the personal data of the DCC is not shared cross-border other than when the individual presents the DCC for verification/validation during travel, either by QR code scanning or by human examination. Data minimization (i.e., data controllers should collect only the personal data they really need, and should keep it only for as long as they need it) is a basic principle of the EU, similar to "minimum necessary" in the U.S., but focused more explicitly on length of storage, and consequently, personal data (e.g. vaccine status) should not be stored longer than necessary by the issuing authority.

At this point there is no federated solution within the EU for immunization records. However, work is ongoing to implement cross-border access and exchange of Patient Summaries which may contain vaccination records.

The DCC solution is based on a (pan-European) trust framework combined with the principle that the respective MS, most with a national vaccination registry, approves the vaccination doses given in that country.

U.S. Recognition of Passports Between Jurisdictions Within the U.S. and Internationally

There are at least three major policy dimensions that have been identified:

- **Recognizing credentials issued by another jurisdiction**. Issuers may include the government (where applicable) or private parties (e.g., sports venues, restaurants, employers, etc.). The use of standards, such as VCI and the Smart Health Card, can help address this issue without the need for formal agreements among jurisdictions. However, jurisdictions may vary in their requirements for "trusted issuers" of the credential and how close to the primary vaccination source that issuer must be (e.g., vaccination provider, state registry, provider who validates based on query to a registry or information provided by the patient). Note that with respect to recent U.S. CDC orders for international travel into the U.S., specific European credentials

are referenced, but only as examples, reflecting a non-restrictive approach to credential issuers and standards.

- **Differences among jurisdictions and private parties over adequacy of vaccination.** For example, adequacy of a vaccination may depend on when the vaccination was administered, what vaccine was administered, and whether a booster has been administered. Additionally, government (e.g., New York City) or private sector policies regarding vaccination credential requirements (e.g., for employment, to enter a venue, to enter a country or a state) and the level of verification required (e.g., paper record acceptable but digital credential also accepted, digital credential required) are also factors. It is important to recognize that many of the political battles over vaccination credential are more about the uses to which the credential will be put than the credentials themselves. The U.S. CDC Technical Instruction does specify accepted COVD-19 vaccines and definitions of "fully vaccinated".
- **Issues of equity** associated with requiring vaccination or specific models of proof, whether administered by a government or a private party. For example, one issue includes uneven ability to travel internationally. Government has an important role in mitigating potential inequities.

Furthermore, the use and acceptability will be limited by the extent of use and acceptance of standards. In the U.S., the VCI Smart Health Card Framework is a very promising development. Similarly, the DCC and the United Kingdom National Health Service COVID Pass also reflect a standards-based approach with all of these ripe for harmonization and alignment.

E.U. Recognition of Passports/Certificates DCC Between Jurisdictions Within the E.U. and Internationally

The E.U. holds a few major policy dimensions for cross-border exchange:

- **Free movement within the EU.** The EU DCC has been created with the purpose of restoring free movement within the EU for all citizens of the EU consistent with fundamental EU principles for free movement of persons within the EU.
- **Mutual Recognition of DCCs.** When it comes to mutual recognition of DCCs within the EU this is the basic idea of the EU DCC system, regulated and facilitated by agreed specifications and supported by a trust framework. Any departures from the basic principles regarding vaccination, recovery, and test certificates for time of validity and other factors, must be announced to the other MS beforehand, prior to applying them when verifying DCCs of incoming visitors.
- **The EU DCC has expanded outside its geography to non-EU countries.** There are a growing number of countries outside of the EU that apply for and join the EU DCC system. As of December 2021, 22 new "third countries" have joined the 27 Member States of the EU. Although the U.S. has not joined the DCC system, it does recognize

this credential as a valid approach in the CDC Technical Instruction cited previously.

Lastly, one promising approach would be for the U.S. to formally validate the European DCC and establish a mutual workstream, facilitated by HIMSS, with the objective of harmonizing the European (EU and UK) and U.S. approaches while advocating for national and international recognition of such a harmonized approach, and enabling passes and certificates to help control the spread of COVID-19. At the same time, as reflected by the above referenced U.S. CDC Technical Instructions, a nation or organization can recognize the validity of digital credentials from another nation without needing to embrace the policy specifics associated with that credential.

Acknoweldgements

HIMSS would like to acknowledge the remarkable work of the HIMSS Interoperability and Health Information Exchange (HIE) Committee in the development of this document.