DIGITAL ID SYSTEMS AS AN ENABLER OF EFFECTIVE COVID-19 VACCINATION[1]

PRACTITIONER'S NOTE

NOVEMBER 25, 2021

Context

With the need to vaccinate their populations rapidly and inclusively, countries have been scaling up existing digital health assets or introducing digital solutions and platforms to support their vaccination campaigns and start reopening their economies. However, these mass vaccination programs present several unprecedented challenges, such as global supply and market constraints, the need to vaccinate most adults, and considerable social and economic pressures to reduce restrictions.

Of the countries that have been able to achieve the outcomes of speed, inclusion, and impact of their mass vaccination programs, two key success factors have included: (1) the availability, reliability, and interoperability of data on beneficiaries at the individual and aggregate levels, including information such as demographics, employment, and health status; and (2) the unique and secure identification of targeted beneficiaries, which in most cases is the entire population. These two elements greatly assist with planning, administering prioritization, and facilitating other aspects of the vaccine delivery life cycle, from preregistration to monitoring adverse events and issuing proof of vaccination.

Specific foundational ID systems (such as national IDs and population registries), functional IDs in the health sector, and government-recognized digital ID systems should never be a condition to access vaccination, but these systems can be leveraged by countries to improve service delivery, such as simplifying the verification of eligibility, contacting of beneficiaries, scheduling and managing appointments, linking doses and their vaccine status to medical records, and potentially associate the beneficiary with an insurance or social protection program for financing purposes. Furthermore, ID systems can also support the chain of trust in the issuance of (paper or digital) vaccine certificates. Coupled with strong data protection, information security, and safeguards against exclusion, countries were able to rely on their identification systems to ensure an equitable, efficient, and transparent delivery of COVID-19 vaccines.

WORLD BANK GROUP

ID4D.WORLDBANK.ORG

What Are ID Systems?[2]

ID systems comprise databases, processes, technology, infrastructure, credentials, and legal frameworks for the capture, management, and use of personal data to identify and verify people, including the issuance of credentials, such as physical cards and documents and non-physical equivalents, such as digital certificates and unique numbers. They also act as registries. Broadly speaking, ID systems come in two forms:

- **Foundational ID systems and registries such as national IDs, population registries, and civil registries:** Intended to cover the general population and be used as a primary authoritative source of core identity attributes of people and to authenticate them for a wide variety of transactions.

- **Functional ID systems and registries such as passports, driving licenses, and health insurance member registries:** Primarily intended for specific sectors or transactions, and often rely on foundational ID systems to ensure that core identity attributes are accurate and that the person is unique and real (i.e., not fictitious). Functional IDs may be used for broader purposes, especially as foundational IDs if none exists.

The term "digital ID systems" can be used to either describe foundational or functional ID systems that use digital technology throughout the identity life cycle, such as for data capture and storage, identity authentication, and/or provide credentials that can be used remotely in an online environment (e.g., for logging into an e-service portal). The benefits of using digital technologies in the context of ID systems is that they can, in fact, promote better data protection and utilization, including facilitating auditability and access management, and efficient data management, interoperability, and re-usability.

Box 1. Key databases acting as authoritative sources of foundational identity information

Common types of foundational ID systems include civil registries, universal resident or national ID systems, and population registers.

Civil registries: A continuous, permanent, compulsory, and universal recording of the occurrence and characteristics of vital events pertaining to the population, as provided through decree or regulation in accordance with the legal requirements of each country.[3] Vital events concern the life, death, and civil status of individuals, including live birth, death, fetal death, marriage, divorce, separation, annulment, adoption, legitimation, and recognition (of paternity).

National identification (ID) system: A foundational identification system that provides national IDs (NIDs)— often a card—and potentially other credentials. In many countries, a primary function of national ID systems has been to establish and provide recognition and proof of nationality and/or residency status.

Population registries: A database of every individual that has the right to reside in the country, including citizens and noncitizens, children, and adults. Population registers typically contain demographic data and life-event information that is the basis of or exchanged with other identification systems and databases, such as national ID systems, civil registers, and others.[4]

---

2   World Bank. 2019. *ID4D Practitioners' Guide*. https://id4d.worldbank.org/guide.
3   UNDESA. 2014. *Principles and Recommendations for a Vital Statistics System*, Revision 3. New York, NY: United Nations Department of Economic and Social Affairs, Statistics Division. https://www.un.org/development/desa/capacity-development/tools/tool/principles-and-recommendations-for-a-vital-statistics-system-revision-3/.
4   Harbitz, M. and Kentala, K.. 2013. *Dictionary for Civil Registration and Identification*. Washington, DC: Inter-American Development Bank. https://publications.iadb.org/en/dictionary-civil-registration-and-identification
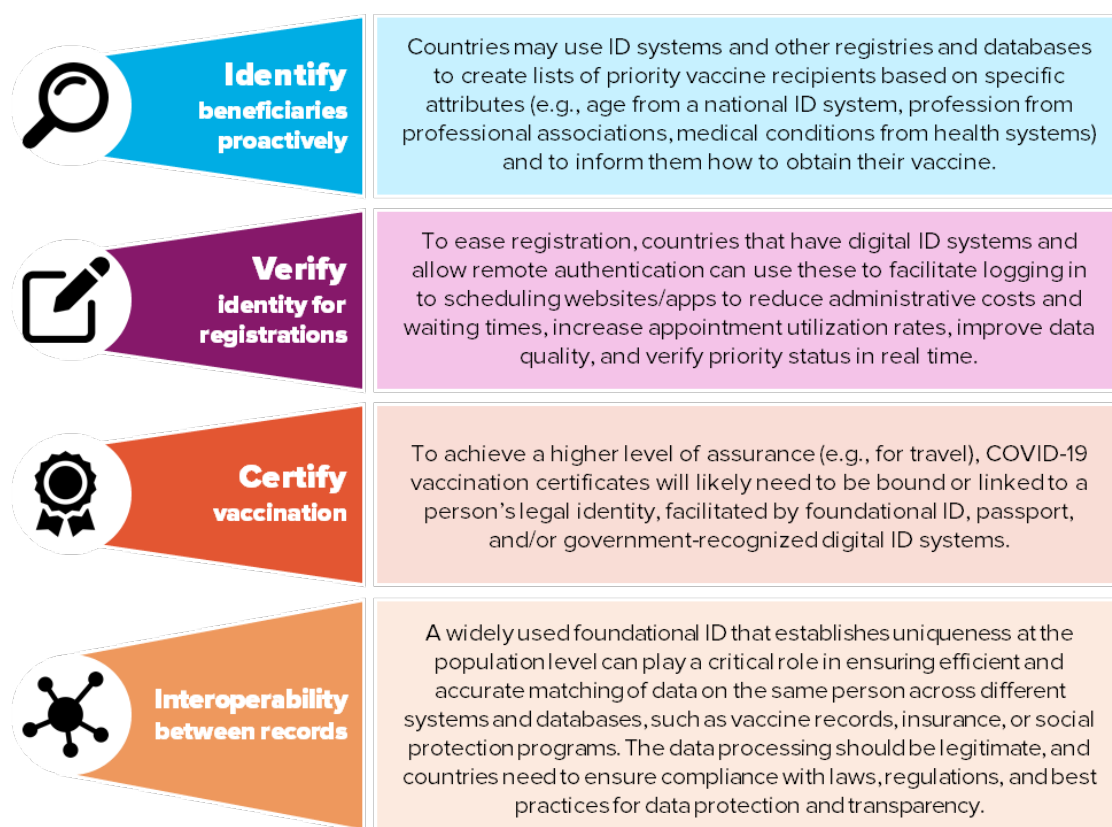
What makes a "good" ID system?

If designed and implemented well, ID systems can enhance delivery of public and private sector services, such as health care, social protection, and banking. However, ID systems in whatever form also come with risks, especially in relation to data protection, exclusion, and technology lock-in. In order to provide a guiding framework to help countries to maximize the benefits and mitigate the risks, the World Bank Group and 30 other international, regional, private sector, nongovernment, and academic organizations have developed and endorsed the *10 Principles on Identification for Sustainable Development*,[5] which cover the themes of inclusion, design, and governance.

In addition, it is critical that the processing of information contained in databases and the use of ID systems as part of the COVID-19 vaccine delivery is done in line with legal frameworks and best practices for data protection.

What Role Do ID Systems Play in Supporting Vaccine Delivery?

Figure 1. The Potential of ID Systems to Support Vaccine Delivery

Identify beneficiaries proactively
Countries may use ID systems and other registries and databases to create lists of priority vaccine recipients based on specific attributes (e.g., age from a national ID system, profession from professional associations, medical conditions from health systems) and to inform them how to obtain their vaccine.

Verify identity for registrations
To ease registration, countries that have digital ID systems and allow remote authentication can use these to facilitate logging in to scheduling websites/apps to reduce administrative costs and waiting times, increase appointment utilization rates, improve data quality, and verify priority status in real time.

Certify vaccination
To achieve a higher level of assurance (e.g., for travel), COVID-19 vaccination certificates will likely need to be bound or linked to a person's legal identity, facilitated by foundational ID, passport, and/or government-recognized digital ID systems.

Interoperability between records
A widely used foundational ID that establishes uniqueness at the population level can play a critical role in ensuring efficient and accurate matching of data on the same person across different systems and databases, such as vaccine records, insurance, or social protection programs. The data processing should be legitimate, and countries need to ensure compliance with laws, regulations, and best practices for data protection and transparency.

Icons: Flaticon.com

Source: World Bank, 2021

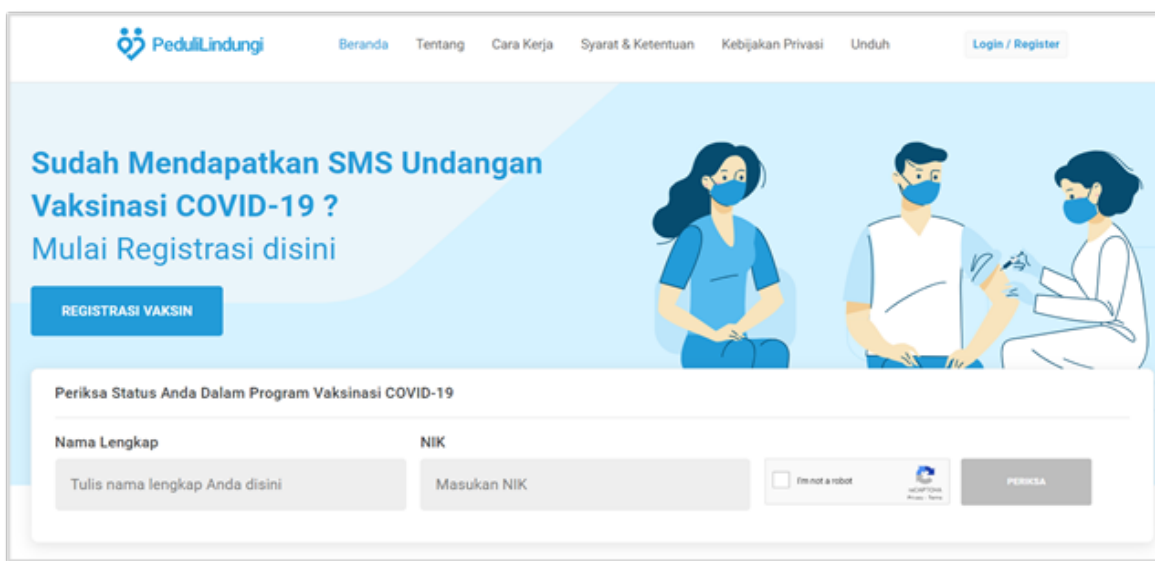
5   See: https://id4d.worldbank.org/principles.

Identify and prioritize beneficiaries proactively

The initial limited availability of COVID-19 vaccine supply means that many countries need to strategically prioritize the allocation of vaccine doses, based on different phases and criteria relative to risk factors (e.g., comorbidity, geography, age groups, employment), with a progressive widening of target groups.

Countries that can rely on a universal foundational ID system or high-coverage functional ID systems are able to identify the majority of their population and thus the majority of beneficiaries, supporting a more rapid and effective delivery of vaccines. This empowers countries to: (1) objectively, verifiably, and efficiently associate each person with a category of prioritization; (2) provide a way of directly contacting individuals (postal mail, email, phone, Citizen Box), and (3) facilitate the registration of vaccine recipients. These assets can also enable countries to be more proactive, including contacting people directly when they are eligible for vaccination (rather than waiting for eligible persons to preregister or register). Mechanisms to correct prepopulated prioritization lists should always be foreseen.

When associating data from different databases, countries should ensure compliance with applicable data protection laws and regulation. Countries should have a clear legal mandate to repurpose existing databases for the purpose of vaccine delivery. In addition, countries should process such data while respecting common data protection principles, such as lawfulness, purpose limitation, and data minimization. The sensitive nature of health data processed as part of a vaccine delivery program necessitates robust technical and organizational measures to ensure appropriate data security.

Figure 2. Prioritization Check in Indonesia

Using their ID number (NIK), individuals can check on the PeduliLindungi website whether they have been prioritized for vaccination and ask to be included in the list if they are eligible.

Source: PeduliLindungi.id

Typical ID systems and registries that can be leveraged to establish the eligibility of individuals against prioritization criteria are, for example:

• Foundational ID systems (for age and location);

• Human resource management systems, payroll or pension registries (for specific professions like health workers, teachers, and other essential workers like police officers, childcare providers, etc.);

- Health insurance systems or health information systems (for co-morbidities, disabilities);
- Social registries (for lower-income and vulnerable populations).

To provide vaccinations free of charge in an equitable manner, countries may have a diverse financing and subsidy strategy to ensure that the whole population is covered either by their participation to a health insurance system or alternative mechanism. Planning and implementation will depend on the ability to categorize beneficiaries in different ways, such as their insurance, employment, or economic status. This information should not be in foundational ID systems, but governments may be able to work in conjunction with health insurance or social assistance providers to deliver specific social assistance programs. In India, the 530 million people covered by the governmental scheme Ayushman Bharat providing free access to health care, receive a COVID-19 vaccine for free even if they seek vaccination in a private facility.

Verify the identity at registration and point of care

Identification and authentication of a patient should not be established as a condition for access to vaccination. Because of the risk of exclusion, existing IDs—especially a specific ID or small set of IDs—should never be a requirement for accessing vaccination. People without any ID should be able to be vaccinated. The application of ID systems as part of the vaccination life cycle should only be used as an optional channel to enhance the accessibility and delivery of vaccination, such as to improve the quality of data in vaccination records and to enable remote service delivery (e.g., AEFI monitoring or vaccine certificate retrieval). Alternative processes can be implemented to collect basic biographical information (such as name, date of birth, address, and contact details) to ensure continuity of care.

Identification of patients, based on the presentation of a national ID, passport, driving license, or health insurance card, is performed when possible to ensure that the person is part of a priority group or to establish/link a patient record in its name in order to ensure appropriate medical follow-up in the case of multiple doses vaccination protocols. An authentication is usually done manually by comparing the name or picture present on the ID document to the patient file. Absence of identity documentation should never be a barrier to access care.

Countries with a digital ID system for online transactions may leverage these as a voluntary option to ease the registration of beneficiaries for the vaccination, enabling people to remotely access a vaccine scheduling website and/ or ease the identification process of the patient at the point of care.

Figure 3. Registration for Vaccination in Denmark
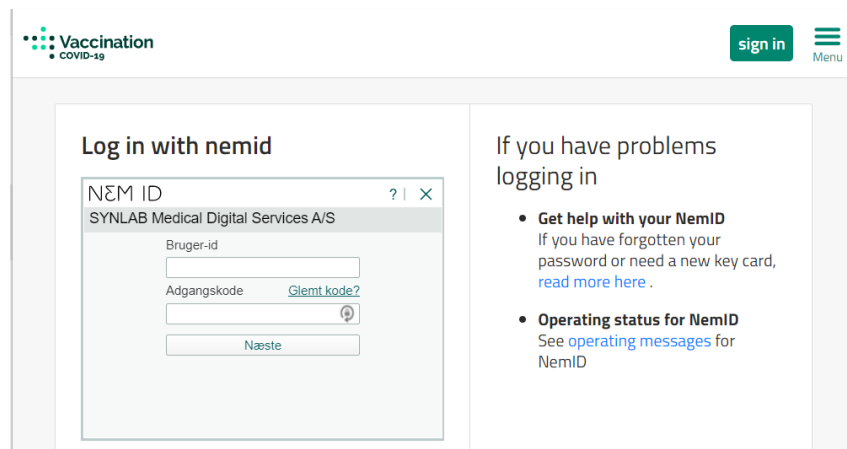
Denmark residents can use their Digital ID NemID to log in to the website allowing them to register for vaccination. Their eligibility is automatically checked, and a link is created with their medical record.

Source: Vacciner.dk

Benefits of using digital ID systems for verification at point of care include:

- Reduced administration costs and waiting times because of digitized and automated processes
- Enhanced data quality by limiting the manual data collection and verifications at the vaccination centers and in any subsequent interactions
- Increased appointments utilization rate as beneficiaries can modify/cancel their appointment more easily and check their eligibility criteria in real time, as well as more easily held accountable for missing an appointment (i.e., if there was no link with their legal identity)

Ensuring uniqueness of patients at the points of care is the function of digital ID systems that would bring these benefits. The authentication of beneficiaries at vaccination centers ensure the accurate data in the vaccination record (including that it is associated with the right person) and ensuring timely follow-up for dose schedule compliance. Having accurate data in the vaccination record is also particularly important for overall monitoring purposes and for the retroactive issuance of vaccination certificates.

Some countries that cannot depend on existing foundational or functional ID systems may consider exploring the use of standalone biometric recognition to establish uniqueness. One advantage of biometric recognition is they may allow the identification/retrieval of a vaccine record if the beneficiary and their record cannot be identified in another way, such as when a beneficiary has lost their vaccine card. However, the data protection and privacy risks associated to the use of biometric recognition technology are high and countries should only process biometric data where this is necessary (i.e., no other reasonable and less intrusive options are available) for a task carried out in the substantial public interest with a clear basis in law that provides adequate safeguards. There is little evidence that ongoing vaccination programs require such a high level of assurance regarding beneficiaries' identity. If people are mandated to provide their fingerprints or other biometric modalities to access immunization or to receive follow-up vaccines, this could also lead to the exclusion of significant segments of the population who may be unwilling or unable to provide this data.

Certify vaccinations

Beneficiaries must be able to access and prove their vaccination status, including when and where they were vaccinated and the brand and batch number, as well as, if needed, the details for a second (or more) appointment. First and foremost, this information serves crucial medical needs, such as providing a proof of vaccination, ensuring continuity of care, monitoring adverse effects, and in case there turns out to be problems with a particular batch or location.

There have also been discussions about vaccination certificates for other use cases such as international and domestic travel, high-risk employment such as health and aged care, and events with large crowds, either to restrict these activities to vaccinated persons or to enable a risk-based approach for their management, such as reduced quarantines. In its guidance document, he World Health Organization (WHO) raises awareness about ethical issues linked to the use of vaccine certificate as health pass.[6] The application of these other use cases, while potentially supporting public health, social, and economic measures, come indeed with significant risks of exclusion as the vast majority of the global population remains unvaccinated and certain populations may not be able to be access existing vaccines for health reasons.

Whatever the use case, vaccination certificates should ideally be accurate, trustworthy, and inclusive. The risk and consequences of forgery and fraud will be considerable, especially if other use cases are implemented. Accuracy and trustworthiness therefore depend on reliable data in the underlying vaccination records and the ability to verify the physical or digital certificates (e.g., a QR code), whether that is through physical security features such as stamps or

---

6   WHO. 2021. Digital documentation of COVID-19 certificates. https://www.who.int/publications/i/item/WHO-2019-nCoV-Digital_certificates-vacci-nation-2021.1

holograms, or through digital mechanisms and ideally decentralized ones such as public-private key cryptography. Technological and legal safeguards (e.g., sunset clauses for use cases and privacy enhancing technologies) will also boost trust in vaccine certificates among the population. These have not been a feature of the existing "Yellow Cards" (officially called International Certificate of Vaccination or Prophylaxis). In order to not overcomplicate matters and to be inclusive, the certificates should focus on purely proving the occurrence and characteristics of a vaccination event, and not on the identity of the holder. The same characteristics apply to proof of test results and recovery status.

Figure 4. Examples of Different Formats of Vaccination Certificates
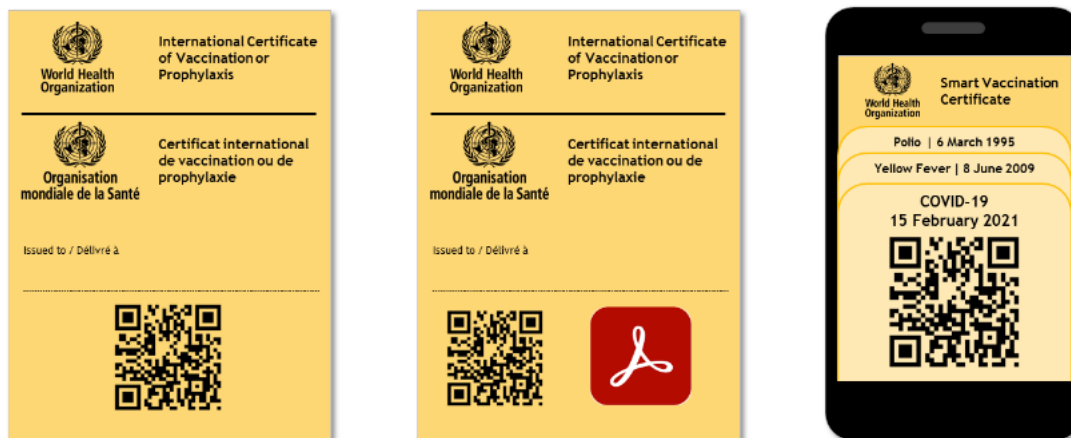
Source: WHO.

If needed, ID systems can play a role for use cases that require a higher-level of assurance, such as international travel. Binding the person presenting a vaccination certificate to that certificate can depend on the linkage with another ID, such as a passport or digital ID, which can come in the form of matching demographic information. Some private sector and civil society initiatives such as CommonPass,[7] Good Health Pass Collaborative,[8] and Vaccine Credentials Initiative[9] are exploring the use of emerging Verifiable Credentials standards[10] to allow vaccine certificates to be stored in a digital wallet, which may also be linked to a digital ID for the identity of the holder. The travel industry, particularly International Air Transport Association (IATA) through its TravelPass program, is also exploring how vaccine certificates can be integrated into existing apps that are used for international travel and already linked to a person's passport.

The European Commission has launched its own Digital Green Certificate (DGC) for travel within the European Union (EU). It consists of a digital proof that a person has either been vaccinated against COVID-19, received a negative test result, or recovered from COVID-19.[11] The document will include as key identity attributes the name and date of birth of the vaccine recipient, that will be compared upon control at a border crossing to an official travel document (e.g., passport, ID card) to verify the identity of the holder. Member states' representatives in the eHealth network agreed to guidelines describing the technical specifications for the DGC, which include an optional personal identifier attribute to be defined by each country, such as a citizen ID and/or document number or identifier within the health system/ Immunization Information System (IIS)/registry.[12]

---

7   For more information about the initiative, see CommonPass's website at https://commonpass.org/.
8   For more information about the initiative, see Good Health Pass's website at https://www.goodhealthpass.org/.
9   For more information about the initiative, see VCI's website at https://vci.org/.
10   For more information about the initiative, see W3C's website at https://www.w3.org/TR/vc-data-model/
11   For more information about the COVID-19: Digital green certificates, see the European Commission's website at https://ec.europa.eu/info/live-
      work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/covid-19-digital-green-certificates_en.
12   eHealth Network. 2021. *Guidelines on verifiable vaccination certificates - basic interoperability elements (release 2)*. https://ec.europa.eu/health/
      sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf.

Figure 5. Examples of EU Digital Green Certificate

Source: European Commission.

Adherence of vaccination certificates to international standards is necessary to ensure their cross-border interoperability and seek global acceptance. WHO established a working group to set Smart Vaccination Certificates (SVC) standards, and released interim guidance, which included a minimum data set and a concept for a global trust framework for verification.[13] The minimum data set includes: full name of the vaccinated person (required); date of birth (required if known); sex (optional, recommended); and a unique identifier (optional, recommended) for the vaccinated person, according to the policies applicable to each country. There can be more than one unique identifier used to link records (e.g., passport, national ID, health insurance number, or vaccine client number). However, the SVC was disbanded in June 2021, with WHO announcing a shift to a broader scope of vaccination, test, and recovery certificates as part of a new initiative to produce guidance documents on Digital Documentation of COVID-19 Certificates.[14] The new guidance document will not address the trust framework to enable countries to verify the authenticity of issued certificate. Complementary initiatives from International Civil Aviation Organization (ICAO) and IATA might address the specific needs of interoperability in the context of international travel.

Enable the interoperability between systems

It is important to be able to uniquely and consistently identify patients throughout the vaccination delivery life cycle, across the different health-related information systems and across health care facilities. The digitization of patient records and an accurate and consistent identification allows for a better automation and streamlining of medical procedures, as well as facilitate exchange of information between the different health care providers: medical staff, pharmacies, laboratories, hospitals, clinics, and so forth.[15]

There are three types of identifiers that can be used to identify patients in the COVID-19 immunization context: foundational identifiers, functional health identifiers or the insured across the health sector, or system-specific identifiers (used for the mass vaccination program). In a study performed by the European Centre for Disease Prevention and

---

13   WHO. 2021. *Interim guidance for developing a Smart Vaccination Certificate – Release Candidate 1.* https://www.who.int/news-room/articles-detail/call-for-public-comments-interim-guidance-for-developing-a-smart-vaccination-certificate-release-candidate-1.
14   https://www.who.int/news/item/04-06-2021-revised-scope-and-direction-for-the-smart-vaccination-certificate-and-who-s-role-in-the-global-health-trust-framework.
       New guidance expected to be published on August 6, 2021.
15   For more information, see ID4D report on: http://documents1.worldbank.org/curated/en/595741519657604541/The-Role-of-Digital-Identification-for-Healthcare-The-Emerging-Use-Cases.pdf.

Control (ECDC) on a subset of European countries, it was found that 69% of countries used the foundational identifier given at birth or emigration, 25 percent used an IIS program-specific functional identifier, and 6.3 percent reuse a national functional health sector identifier.[16]

Figure 6 High-Level Overview of an Immunization Information System and Association with Other Databases
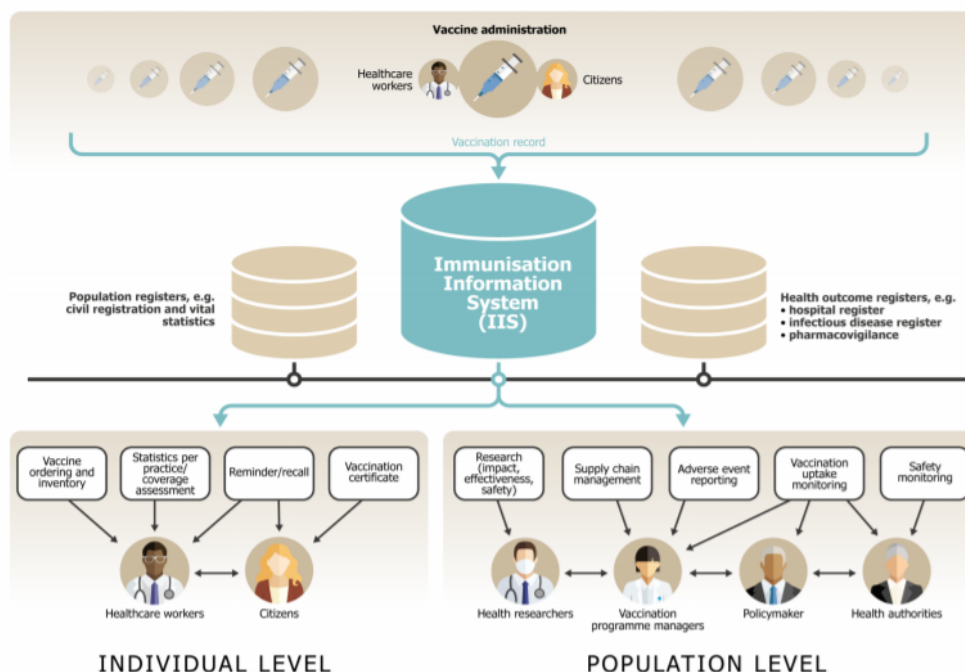
Source: ECDC, designing and implementing an immunization information system.

The use of a unique identifier (and possibly a foundational ID) or indexes linking different identifiers can also enable the electronic immunization registries to communicate with population registers or the civil registers to verify information at enrollment and promote smooth communication between all systems of the health ecosystem, such as the hospital Health Management Information System (HMIS) software, electronic medical records, health insurance claim systems, and population screening registries (e.g., cancer screening register). The aforementioned ECDC study indicates that 81 percent of the studied EU countries use data from population registries in their IIS.

Unique patient identification, coupled with high-assurance authentication mechanisms, can be particularly useful in the case of a vaccination protocol requiring multiple visits in a specific timeframe. Reliable identification of patients across health care facilities and practitioners makes it possible to deliver vaccines with more flexibility and convenience from the vaccine recipients' perspective, while also enabling health authorities to promote and monitor adherence to vaccine protocols, as well as enabling opportunities for continued follow-up. Preventing the duplication of health records for the same individual can also reduce waste and errors in the vaccination campaign.

However, it is important that such systems are implemented with adequate safeguards. In order to preserve the privacy of patients and protect sensitive data against cyber threats, it is recommended to put in place mechanisms such as sectorial unique identifiers or tokenized equivalents as substitutes for a unique ID number that can be more easily revoked or replaced when needed (e.g., a data breach). Additionally, creating linkages between different databases for

---

16   ECDC, designing and implementing an immunization information system, see: https://www.ecdc.europa.eu/sites/portal/files/documents/designing-implementing-immunisation-information-system_0.pdf.

the purpose of facilitating exchange of patients' information requires a clear lawful mandate and will raise potential risks of surveillance and repurposing of the data processed. Where information can be lawfully shared between agencies, data-sharing agreements should stipulate the limited purpose, duration, and other conditions upon which such data is being disclosed by the different governmental agencies and registries involved in setting up Electronic Health Records (HER) systems, as well as include robust minimal security requirements. A digital ID system can contribute to enhance the security of EHR by improving the ability to provide audit logs of access to the record.

Application Examples

- Chile has relied on the high coverage of its health care system and the provision of a national identifier at birth to scale up its national immunization program that was already distributing flu shots and childhood vaccines every year and calling on a very specific group of people each day for injections.

- Denmark developed a website for self-booking appointments that uses NemID, the government-recognized digital ID that is linked to their civil registration number (CPR), which matches to their health record. A hotline is available for people who cannot use this service.

- India built the Co-WIN platform to orchestrate its vaccine rollout and are accepting the foundational ID (Aadhaar) or at least 11 other IDs for people to register on the app and manage appointments. The digitally verifiable vaccine certificates are linked to the recipient's Aadhaar.

- Israel used the existing link between its national population registry and the health system to notify people to schedule appointments and to scale up its universal childhood immunization registry to manage deployment, which has been the fastest in the world.

- Thailand's foundational identification system based on the national population register and a unique identifier (PID) is being used to track vaccinations, to produce vital statistics that guide public health policy, and to monitor health system performance.

- Uruguay is linking individuals' national ID number to the records in the Vaccine Information System that is used for all type of vaccinations. Individuals can verify using their ID number and date of birth if they have been prioritized and able to book an appointment.

Conclusions and Recommendations

The decision on what ID systems to use for vaccine deployment—and how—must be based on whether this will enhance delivery and not hamper any person's access in line with the *10 Principles on Identification for Sustainable Development*.[17] It will also depend on the level of digitization of the country.

- **The onboarding of new sectors within a country's ID ecosystem is a long-term effort and should be carefully planned ahead of crises like the COVID-19 pandemic.** The existence of a unique identity in the country should, however, be considered to ease identity management in newly developed systems or existing ones under upgrade, to support the vaccination campaigns with the view of a long-term integration. Existing foundational and functional ID systems can be used to facilitate the registration for vaccination programs.

- **A specific ID should never be a requirement to receive a vaccine.** There must always be alternatives and exception handling—such as for migrants, refugees, and people without any ID. The coverage of the registries used to prioritize beneficiaries or organize the vaccination campaign should also be carefully assessed in order to avoid risks of exclusion.

- **Alternative mechanisms to digital platforms should be in place to address digital skills and connectivity divide.** There must be nondigital and assisted options for people with limited digital capabilities, especially the elderly and

---

17   For more information about the Principles, see World Bank's website at https://id4d.worldbank.org/principles.

persons with disabilities. Consideration should also be taken with regard to the potential difference in connectivity across the country, and the ability for health care providers to access the digital identification and authentication functions of the ID system.

- **The use cases must adhere to local legal frameworks and best practices for data protection,** such as lawfulness, transparency, data minimization, proportionality and security. The sensitive nature of health data necessitates robust technical and organizational measures to ensure appropriate data security. It is recommended that governments wishing to process data for vaccine targeting strategies adopt a clear and detailed norm (policy/regulation/law) explaining the purposes of such processing, who the data subjects are, the duration and so forth. The use of digital vaccination certificates is an opportunity to implement privacy-enhancing approaches, such as zero-knowledge proofs, decentralized wallets, and verifiable credentials, which would be paradigm shifting for how data are used, re-used, and validated.

Additional Resources and Articles

2021. [Principles on Identification for Sustainable Development: Toward the Digital Age - Second Edition](#).

WHO. 2020. [Guidance on developing a national deployment and vaccination plan for COVID-19 vaccines](#).

WHO. 2020. [WHO SAGE Roadmap for Prioritizing Uses Of COVID-19 Vaccines In The Context Of Limited Supply](#).

WHO. 2021. [Monitoring COVID-19 vaccination - Considerations for the collection and use of vaccination data](#).

WHO. 2021. [Digital documentation of COVID-19 certificates.](#)

World Bank. 2018. [The Role of Digital Identification for Healthcare: The Emerging Use Cases](#).

World Bank. 2019. [ID4D Practitioner's Guide](#).

World Bank. 2020. [ID and COVID-19: Overview of Country Examples in Safety Protocols and Practices](#).

Contact

Digital Development team: [Digital4vaccines@worldbank.org](#).

ID4D team: [id4d@worldbank.org](#).

ABOUT ID4D AND DDP

The World Bank Group's Identification for Development (ID4D) Initiative uses global knowledge and expertise across sectors to help countries realize the transformational potential of digital identification systems to achieve the Sustainable Development Goals. It operates across the World Bank Group with global practices and units working on digital development, social protection, health, financial inclusion, governance, gender, and legal, among others.

The mission of ID4D is to enable all people to access services and exercise their rights by increasing the number of people who have an official form of identification. ID4D makes this happen through its three pillars of work: thought leadership and analytics to generate evidence and fill knowledge gaps; global platforms and convening to amplify good practices, collaborate, and raise awareness; and country and regional engagement to provide financial and technical assistance for the implementation of robust, inclusive, and responsible digital identification systems that are integrated with civil registration.

The work of ID4D is made possible through support from the Bill & Melinda Gates Foundation, the UK Government, the French Government, and the Omidyar Network.

To find out more about ID4D, visit id4d.worldbank.org. To participate in the conversation on social media, use the hashtag #ID4D.

The **Digital Development Partnership (DDP)** offers a platform for digital innovation and development financing. DDP brings public and private sector partners together to advance digital solutions and drive digital transformation in developing countries. [www.digitaldevelopmentpartnership.org](#).

WITH SUPPORT FROM:

A COLLABORATION BETWEEN:

WORLD BANK GROUP
Digital Development

WORLD BANK GROUP
Health, Nutrition & Population