



## Are vaccine credentials the next vector for cyber risks?

**To counter cyber risks associated with digital vaccine certificates, it's important to consider how we might build in protections from the outset by adopting checks and balances across several critical areas.**

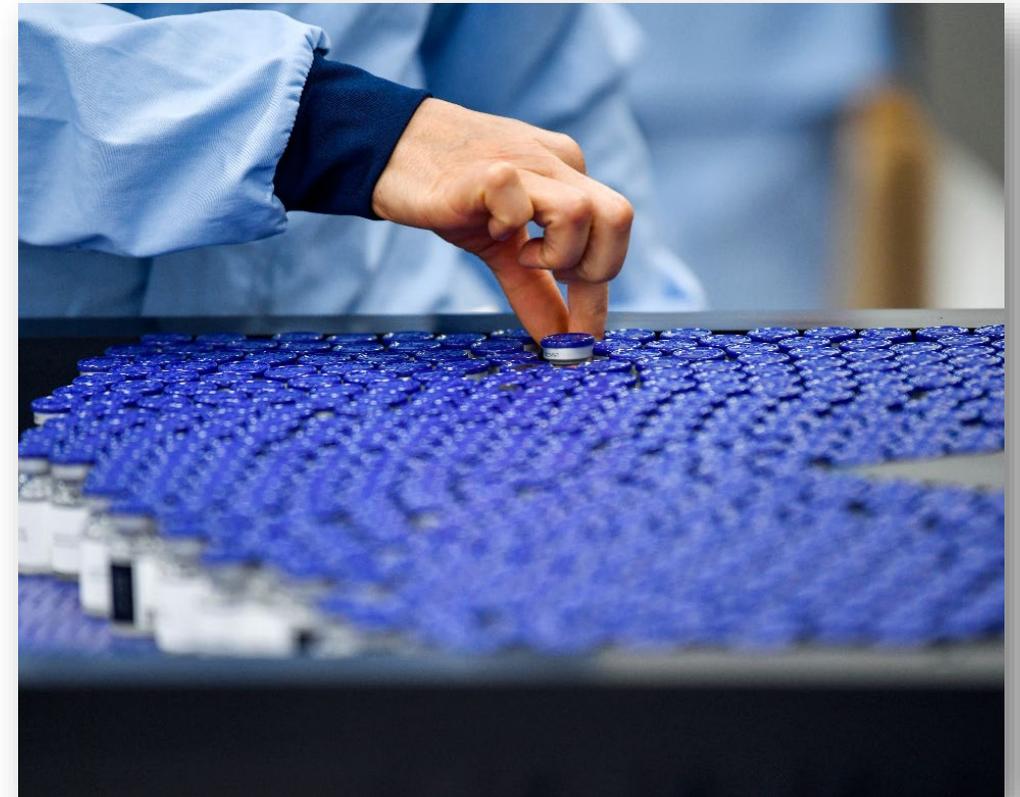
Following the formulation by the pharmaceutical industry of several viable vaccines to combat COVID-19, the prospect for a return to some semblance of normality is on the horizon. By stemming the spread of the virus, the hope is that vaccines will enable people to return to work, head back to restaurants and retail stores, attend public events, and recommence travel.

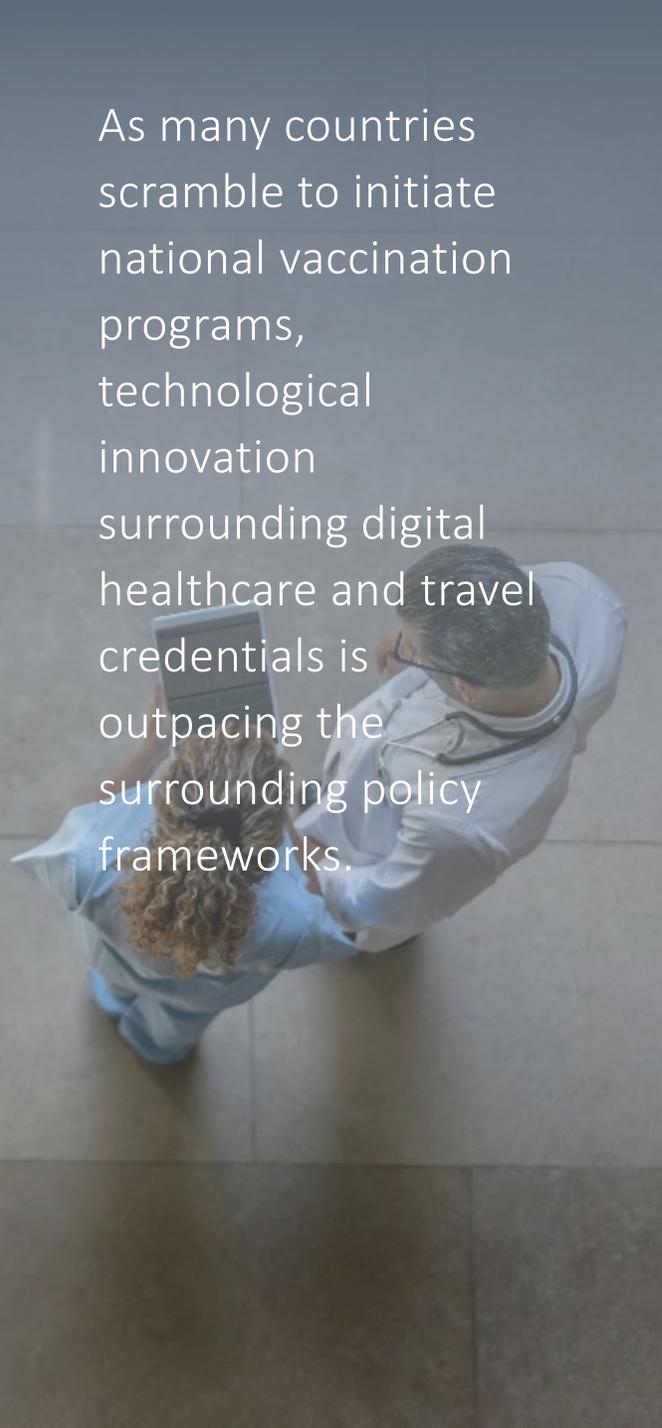
Implicit in these assumptions is the idea that people will be issued some kind of vaccine certificate they can use to establish proof of vaccination. It seems simple in theory. In practice, however, vaccine credentials are fraught with a wide range of complexities, many of which link back to cybersecurity concerns.

The two main challenges? The imperative to create digital versions of these certificates in addition to a secure paper-based solution, and the requirement to make the

credential both interoperable and capable of being shared with third parties globally. In essence, this means a digital proof-of-vaccination issued to a traveler in the UK must have the ability to be accepted and trusted by government authorities and private businesses in Singapore or Australia if it is to drive the benefits required to reopen the global economy.

To bridge the gap between the need for a vaccine certificate and the protection of an individual's digital identity (not to mention their privacy), governments, consortia, healthcare organizations, and the private sector are rapidly coming together to vault several hurdles in the current race against the clock. Here we set out just some of the issues that will need to be addressed in relatively short order—with the caveat that this is only the start of the conversation.





As many countries scramble to initiate national vaccination programs, technological innovation surrounding digital healthcare and travel credentials is outpacing the surrounding policy frameworks.

## Adopting checks and balances across several critical areas

### The aerial view

With over 2.5 million deaths attributed to coronavirus over the past year<sup>1</sup>, it comes as no surprise that many countries are now scrambling to initiate national vaccination programs. As of March 2, 2021, roughly 247 million vaccine doses had been administered around the world<sup>2</sup> with the number climbing daily.

The pace at which the world is moving to resolve this issue is commendable. What it means, however, is that programs and systems are sometimes being set up in days, without the rigor usually associated with longer-term initiatives. The upshot? Technological innovation surrounding digital healthcare and travel credentials is outpacing the surrounding policy frameworks.

In addition to heightening the risk of missteps and data misuse, this opens the door to becoming another cybersecurity target—an issue particularly prevalent in the healthcare space as medical data is not just sensitive; it's also valuable. In fact, health-related data is worth almost 50 times more on the black market than payment card data<sup>3</sup>, thanks to its inclusion of personally identifiable information that can be exploited for identity theft or fraudulent billing.

To counter these cyber risks, global consensus is aligning behind the relatively new technology of verifiable credentials and distributed identities. Sometimes referred to as self-sovereign identity (SSI), this method of digital identity differs from its centralized or federated cousins in that it places the holder (citizen) at the center of the interaction scheme and allows relying parties (e.g., airlines) to validate the vaccination credential against a public registry of issuers (often blockchain) rather than having to handle or store any of the individual's personal data.

While the nuances of how verifiable credentials operate solve some traditional issues with more centralized identity schemes, it is still important to consider how we might build in protections from the outset by adopting checks and balances across several critical areas. Some of these include:

### Governance

The number of players needed to establish effective vaccine credentials around the globe is staggering. Countless government agencies, intergovernmental organizations (such as the World Health Organization), consortia, and private companies must work cohesively to arrive at a solution—and while these stakeholders might currently be motivated to cooperate, fully articulated governance

structures will be necessary to prevent these relationships from breaking down over time. To help define the roles and expectations of each party in the ecosystem, public and private stakeholders have already come together in some countries to develop clearly articulated trust frameworks, such as the Pan Canadian Trust Framework and the UK's Digital Identity and Attributes Trust Framework.

Beyond clarifying roles, responsibilities, and accepted behaviors, however, these types of governance frameworks will also be required to enable stakeholders to pool their efforts. While everyone is trying to understand how a vaccine or test credential would work, it's important that cyber considerations are embedded firmly in the development. Mature governance structures will be critical if stakeholders hope to achieve consensus on common standards for security, authentication, privacy, and data sharing.

Admittedly, this task is complicated by the pace at which the world is moving. This means government policies around how countries control their borders, as well as their position on vaccine and test credentials, will need to be established as quickly as the technology that emerges.

<sup>1</sup>John Hopkins. "COVID-19 Dashboard by the Center for Systems Science and Engineering." <https://coronavirus.jhu.edu/map.html>

<sup>2</sup>New York Times, March 2, 2021. "Tracking Coronavirus Vaccinations Around the World." <https://www.nytimes.com/interactive/2021/world/covid-vaccinations-tracker.html>

<sup>3</sup>SecureLink, February 5, 2020. "Healthcare data: The new prize for hackers," by Ellen Neveux. <https://www.securelink.com/blog/healthcare-data-new-prize-hackers/>

### Ethics and trust

One of the key challenges inherent in a vaccine certificate is the fact that it relies on people's willingness to share their health data with responsible authorities. This willingness is precarious even in countries where populations trust public sector organizations. In countries where that trust is lacking, the very idea of sharing vaccine credentials may seem like a no-go.

Given the ethical quandaries associated with this initiative, using a trust framework and technological methods that are private by design are imperative. How do we prevent a government from using the vaccine record outside of approval to travel? How do you embed consent management and control with the user vs. the governmental body? We will discover that depending on the global geography in question there may be questions regarding the proper balance between civil liberties and the public interest? Are we setting a dangerous precedent by limiting citizen access to goods or services on the basis of health data?

While a mature cybersecurity stance cannot resolve all those quandaries, it can go a long way towards establishing a network of trust that accommodates a multi-player construct, even in jurisdictions where the complexities of gaining trust appear insurmountable.

### Data sharing

Before individuals can start flashing their vaccine certificates at airports and public venues, standards will need to be put in place to govern how their health data is shared, who has access to it, how long that data is being stored, and the purposes for which that it can be used. For instance, in addition to giving citizens the right to consent (or withhold consent) for the use of their personal data, Europe's General Data Protection Regulation (GDPR) strictly limits which entities can process individuals' health data and for what purposes. Those entities, in turn, are expected to provide full transparency about how they will process the data.

Data sharing complexities are one of the driving forces behind the distributed, verifiable credential model that is rapidly gaining prominence as a framework for vaccine and test credentials. While the specific technical protocols have not yet been solidified for vaccine credentials, standards are emerging that take validation protocols (such as W3C and HCL7) into account. As a result, governments and private sector consortia are aligning around these standards. Deloitte and other firms are working together on this global problem with both local groups and through broader industry initiatives like The Good Health Pass<sup>4</sup>.

Governments and organizations that are authorized to provide vaccine and test credentials need to provide that authenticity globally. Private sector organizations, such as airports and airlines, will need the capability to verify that the electronic or paper-based credentials provided by citizens are authentic and have been issued by a reliable source.

While it may have seemed like a somewhat distant future requirement just a few months ago, blockchain registries are now emerging as a critical part of the solution to enabling the type of global platform that is being architected.

### Data protection

To confirm that an individual has undergone (or is undergoing) the vaccination or test process, vaccine or test certificates may include personal identifiers—from names and addresses to health IDs and perhaps even biometrics. Given the value of this data, security controls must be paramount. This requires stakeholders to think through how the data will be managed, stored, and protected.

This task is further complicated by the need for global cooperation. There is a myriad of legal and regulatory structures already in place around the world and designed to protect this class of data.

These legal and regulatory protections and guidelines make this problem vastly more complex.

Take as example the following:

- [General Data Protection Regulation](#)
- [Vermont Act 171 of 2018 Data Broker Regulation](#)
- [California Consumer Privacy Act](#)
- [Brazilian General Data Protection Law \(LGPD\)](#)
- [India Personal Data Protection Bill](#)
- [Chile Privacy Bill Initiative](#)
- [New Zealand Privacy Bill](#)

Consider: on the data privacy front alone, every country has its own set of rules and regulations. Standards that seem onerous in one jurisdiction could be insufficient in another. Without effective cybersecurity stopgaps, the risk of data losses and privacy breaches mounts.

This likely explains why the self-sovereign decentralized model, with the individual as the holder of the credential in a wallet of their choice, is emerging as a logical requirement—as it significantly reduces or eliminates the amount of personal health data being stored or processed by third parties.

<sup>4</sup>Good Health Pass Collaborative. "Good Health Pass: A Safe Path to Global Reopening." <https://www.goodhealthpass.org/>

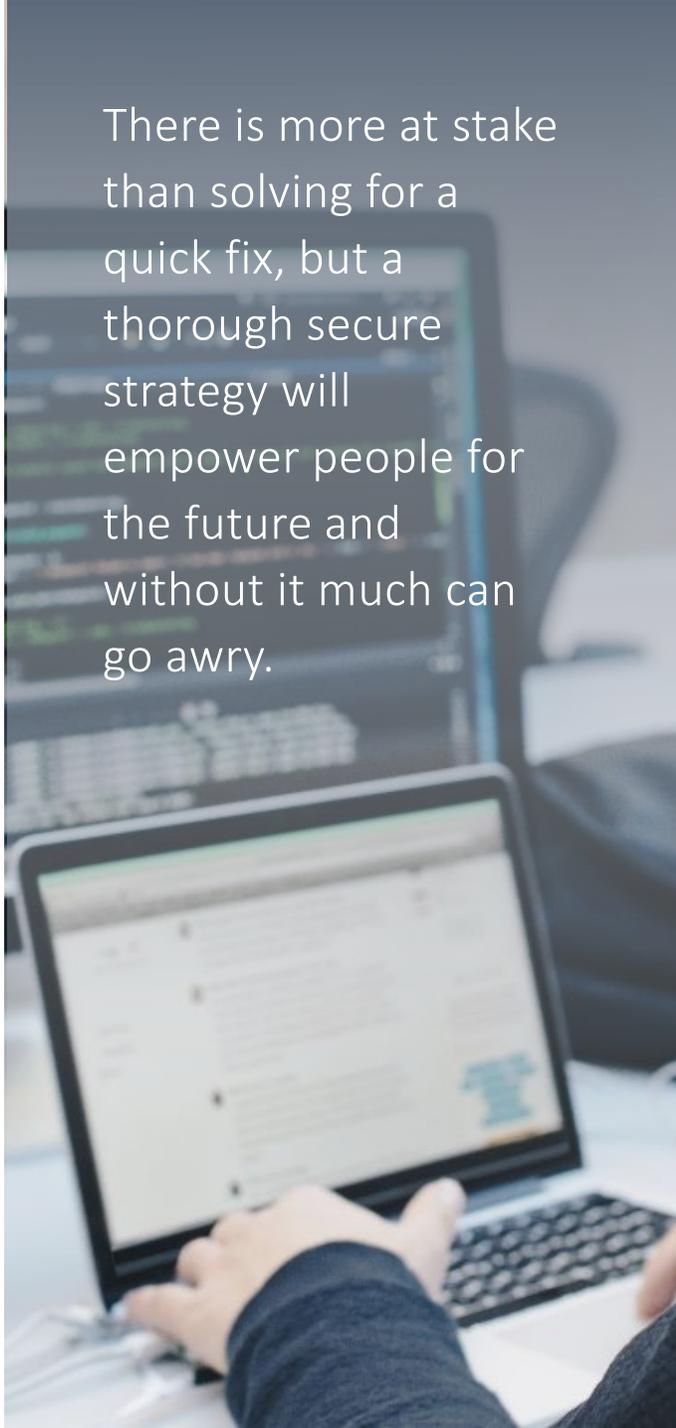
### Hurdling the gap

This surface review of a bare handful of cyber-related concerns clearly underscores the need for a rock-solid foundation as the world moves towards the adoption of digital vaccine credentials. There is more at stake than solving for a quick fix, but a thorough secure strategy will empower people for the future. Without it, much can go awry.

In the coming weeks, we will delve deeper into the cyber considerations touched on in this article that are needed to deliver a secure vaccine or test credential. In the interim, here's some food for thought: one of the barriers to governments investing in broader digital identity systems (Citizen Digital Identity) has been public adoption in the creation of early credentials. The need for a vaccine or test credential to safely open up the economy has completely changed this paradigm.

While governments and private sector players have been discussing Citizen Digital Identities and credentials, as well as their appropriate roles, the need for secure, useful, inclusive vaccine and test credentials may actually accelerate the development of broad-purpose, globally interoperable Citizen Digital Identities.

This clearly underscores that the last 12 months, while extraordinarily challenging, are also a testament to the ingenuity and capability of our global society. Now, as we collectively work to get our economies and citizens flourishing again, we will need to leave nothing behind in the execution, so that we can securely collect data, exchange information, enforce consistent policies, and establish the trust necessary for success.



There is more at stake than solving for a quick fix, but a thorough secure strategy will empower people for the future and without it much can go awry.

## Authors and contacts



**Emily Mossburg | Global Cyber Leader**  
emossburg@deloitte.com



**Annika Sponselee | Global Cyber Data and Privacy Leader**  
asponselee@deloitte.nl



**Amir Belkhelladi | Canada Cyber Leader**  
abelkhelladi@deloitte.ca



**Andrea Rigoni | Global Cyber GPS Leader**  
arigoni@deloitte.it



**Kishwar Chishty | Global Cyber LSHC Leader**  
kchishty@deloitte.ch



**Mike Wyatt | Global Cyber Identity Leader**  
miwyatt@deloitte.com

## Contributors:

**Esther Dryburgh | Risk Advisory – Deloitte Canada**

**Dan Shaver | Consulting – Deloitte Canada**

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see <http://www.deloitte.com/about> to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the “Deloitte organization”) serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 330,000 people make an impact that matters at [www.deloitte.com](http://www.deloitte.com).

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.