Deloitte.

Vaccine certificates, cybersecurity, and trust:
A primer for credential verifiers

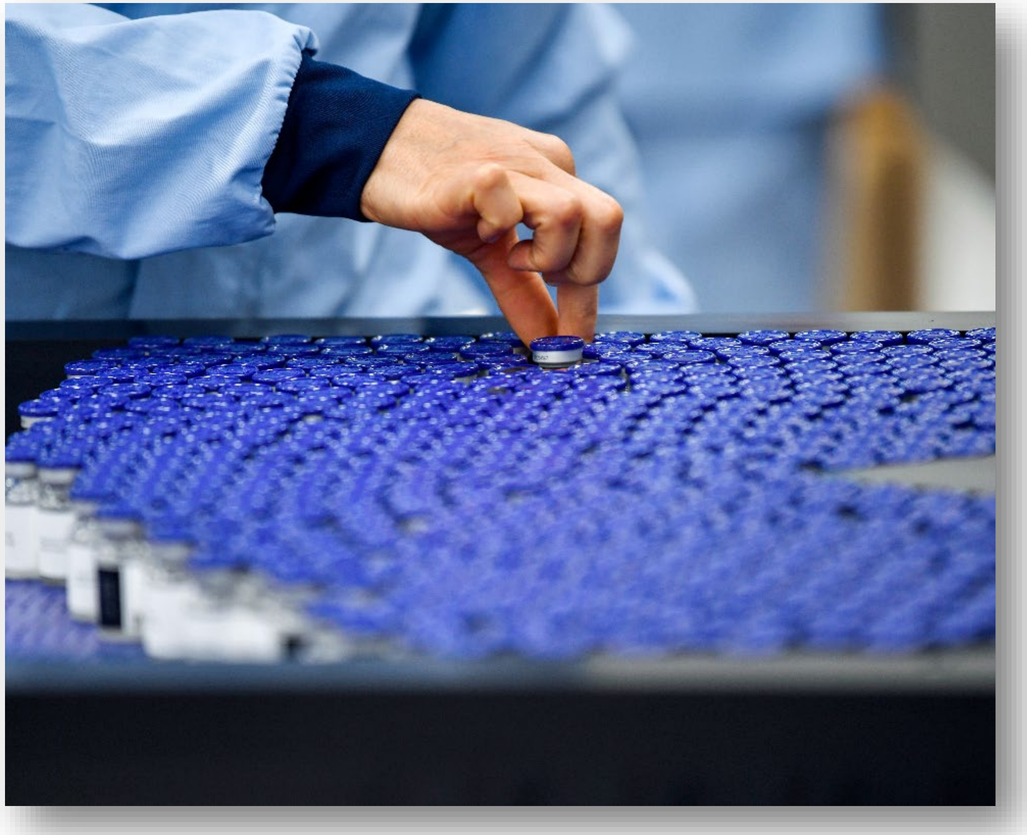
Trust can only be embedded into the health credential system if its rollout is firmly rooted in ethical imperatives.

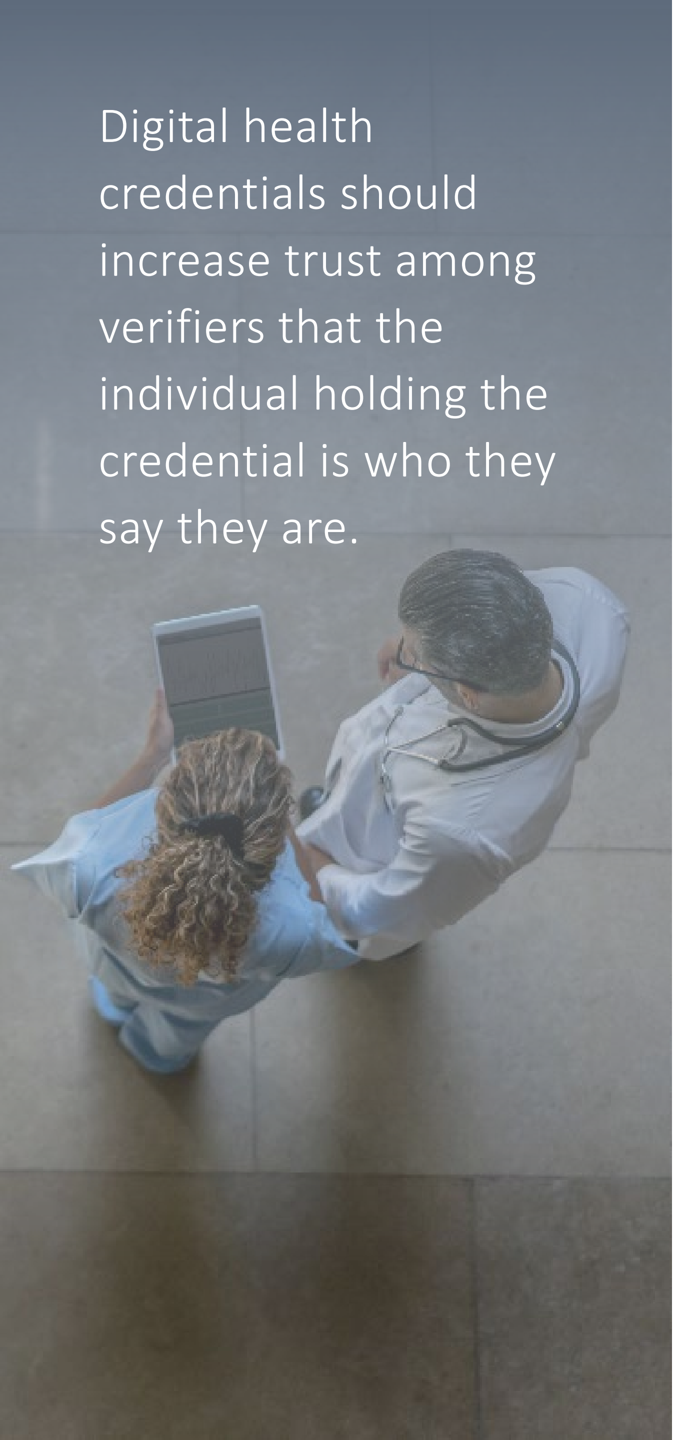
After a solid year of on-again/off-again global lockdowns, most of the world is itching to get back to "business as usual". This likely explains why putative credential verifiers—organizations ranging from airlines and entertainment venues to academic institutions—are eagerly awaiting the rollout of vaccine credentials.

The idea behind these vaccine credential certificates is fairly straightforward—in essence, they're supposed to provide people with proof that they've been vaccinated. Dig beneath the surface, however, and a swarm of complexities unfolds. In our first article in this series, which considers these issues through a cybersecurity lens, we briefly outlined some of these challenges, such as the complexities associated with ethics and trust, governance, data sharing, and data protection. In this second installment, we dive deeper into the ethical and trust-related concerns that credential verifiers will need to consider in reviewing both local and out-of-country vaccine credentials.

In considering issues related to trust, a definition may be useful. Deloitte views trust as an intricate balance between competence and intent—and an organization fully thrives only when both are present. Competence refers to an organization's ability to execute and deliver on its promises. Intent is the driver that underlies those actions and promises. Typically, organizations with good intent act transparently and for reasons beyond mere financial gain.

In exploring these topics, we'd like to stress that this is a huge and multifaceted issue, and this article considers only one small piece of a much larger mosaic. To fill out this story, we will continue to delve into numerous related topics in the weeks and months to come.





Digital health credentials should increase trust among verifiers that the individual holding the credential is who they say they are.

When ethics and evidence collide

While reliance on vaccine credentials isn't new—travelers and school children have long had to provide proof of immunization to relevant authorities—this is one of the first times in history that these credentials may be used for purposes that are not strictly medical. In essence, people may be required to share their health data simply to gain access to public places (such as sporting events or movie theaters) or to goods and services. Not surprisingly, this raises a host of ethical concerns.

Let's start with the very structure of these credentials. Currently, several governments, associations, industry groups, and technology companies are focused on rolling out digital health credentials, which can be securely stored on a mobile device in either an app or digital wallet. In addition to enhancing information security, digital health credentials should increase trust among verifiers that the individual holding the credential is who they say they are.

Except, what happens for people who don't have smart phones? To ensure these credentials are inclusive, accessible, and equitable, both digital and paper-based credentials will need to co-exist. Unless carefully designed, paper-based credentials increase the risk of fraud.

A second ethical challenge revolves around the privacy implications inherent in sharing personal health data with countless government agencies and private sector businesses. While people may be prepared to allow verifiers to scan some kind of barcode or a QR code that confirms their credentials are legitimate, they're less likely to be comfortable sharing actual health data.

That's especially true given that no universal standards currently exist to govern how that information will be collected, stored, or used. And it's doubly true given that no clear rules exist to determine who can become a verifier, which credentials verifiers may review, what additional information verifiers may choose to collect, how to protect anonymized data from becoming re-identifiable, and how to communicate this information with the general public.

Yet another ethical pitfall arises when you consider the implications of presenting these health credentials across multiple jurisdictions. Without an interoperable digital solution or standardized cross-border regulations, travelers will have little assurance that their private information is being adequately protected on an international basis—particularly in countries that lack robust controls. To enhance trust, verifiers planning to review multijurisdictional health credentials will need to consider how to develop a trust framework and implement tamper-proof systems that support interoperability.

And none of this takes into account the underlying ethical implications of requesting a "vaccine certificate" in the first place. What happens for the people who choose not to be vaccinated or who don't have access to vaccines? To avoid discrimination, verifiers will likely need the capability to review different types of health credentials—from vaccine certificates, to proof of immunization (e.g., antibody tests), to negative COVID PCR (polymerase chain reaction) test results.

[1] Forbes, February 25, 2021. "This One-Stop Digital ID App Wants To Cut Through The Vaccine Passport Noise," by Suzanne Rowan Kellerher. https://www.forbes.com/sites/suzannerowankelleher/2021/02/25/this-one-stop-digital-id-app-wants-to-cut-through-the-vaccine-passport-noise/?sh=

A cyber-secure foundation

While cybersecurity technologies, processes, and physical controls cannot resolve all these issues, they can go a long way towards alleviating some of the more critical ethical and trust-related concerns. Some of the controls that must be considered include:

- **Authentication**. To verify identities, vaccine certificates will need to embed high levels of authentication controls—from multifactor authentication that potentially combines digital health certificates with existing IDs (such as national passports) to biometrics. Interestingly, Airside Mobile recently partnered with Vision-Box to develop a digital app to enable biometric verification of a range of IDs, including digital health passports.

- **Access controls and security monitoring**. With health data being stored in both digital and paper-based formats, strict mechanisms to keep this information secure will be paramount.

- **Privacy and consent.** To prevent privacy infringement, data leakage, or the over-exposure of information, some countries are looking at ways to give citizens control over who they share their data with and what level of information can be accessed. Any solution adopted will also need to comply with the privacy regulations and standards emerging from national privacy regulators, as well as supervisory organizations such as the World Health Organization.

- **Data loss prevention (DLP).** To safeguard the sensitive data contained in digital health certificates, verifiers may need to implement DLP software solutions designed to detect and block data leakage.

- **Encryption.** As the risk environment shifts, encryption standards regularly evolve to keep pace. To limit data exposure if credentials are lost or stolen, verifiers will need to adopt these emerging encryption standards. This can be accomplished in a number of ways, including through the use of zero-knowledge proofs, which rely on cryptographic algorithms to verify the authenticity of digital health certificates without requiring users to share the underlying data.

- **Authorization**. A question that must be resolved involves determining which organizations will be considered valid issuers and authorized verifiers.

Another factor to consider is that credential verifiers themselves are not responsible for issuing these health certificates. Without interoperable standards or a central issuing authority, this vastly complicates the verification task. This is one reason why technologies such as blockchain are now being explored as potential solutions. In addition to providing immutable proof of vaccination (or immunity), digital ledgers such as blockchain would allow verifiers to ascertain that any credentials presented are authentic, up-to-date, and issued by a verified authority.

Bolstering cybersecurity capabilities in these ways can go a long way towards building greater trust in the verification process—while simultaneously supporting system transparency as a whole.

Going global

Admittedly, this is all easier said than done, especially considering that digital health certificates will need to be verified in multiple jurisdictions as travel begins to open back up. Given the differential legislative frameworks that prevail internationally, this will be no easy feat in practicality.

In the US, for instance, health information privacy rules such as the Health Insurance Portability and Accountability Act (HIPAA) tend to be fairly prescriptive around the controls that must govern personal health information (PHI). Similarly, the EU's General Data Protection Regulation (GDPR) sets out prescriptive elements and features strong enforcement. Canada, for its part, seems to have varying standards of consent-based private sector legislation and non-consent-based public sector legislation. And Australia's opt-out approach to PHI use for secondary purposes (such as research) makes it unclear how health data should be shared and managed. Developing a health certificate system that complies with each of these divergent rules can seem downright impossible.

To bridge these gaps, numerous initiatives are now underway to create frameworks for interoperability. These include the Good Health Pass Collaborative, the Vaccination Credential Initiative, the World Economic Forum's Common Trust Network, the Trust over IP Foundation, and IATA's Travel Pass Initiative, just to name a few. Specific countries and regions are also coming together to develop digital health ID standards, such as the EU's Digital Green Certificate; the "green passport" deal signed between Israel and Greece; national initiatives in countries ranging from Denmark, Germany, the UK, and Sweden to China and Japan; and New York State's Excelsior Pass designed to enable local businesses to safely reopen.

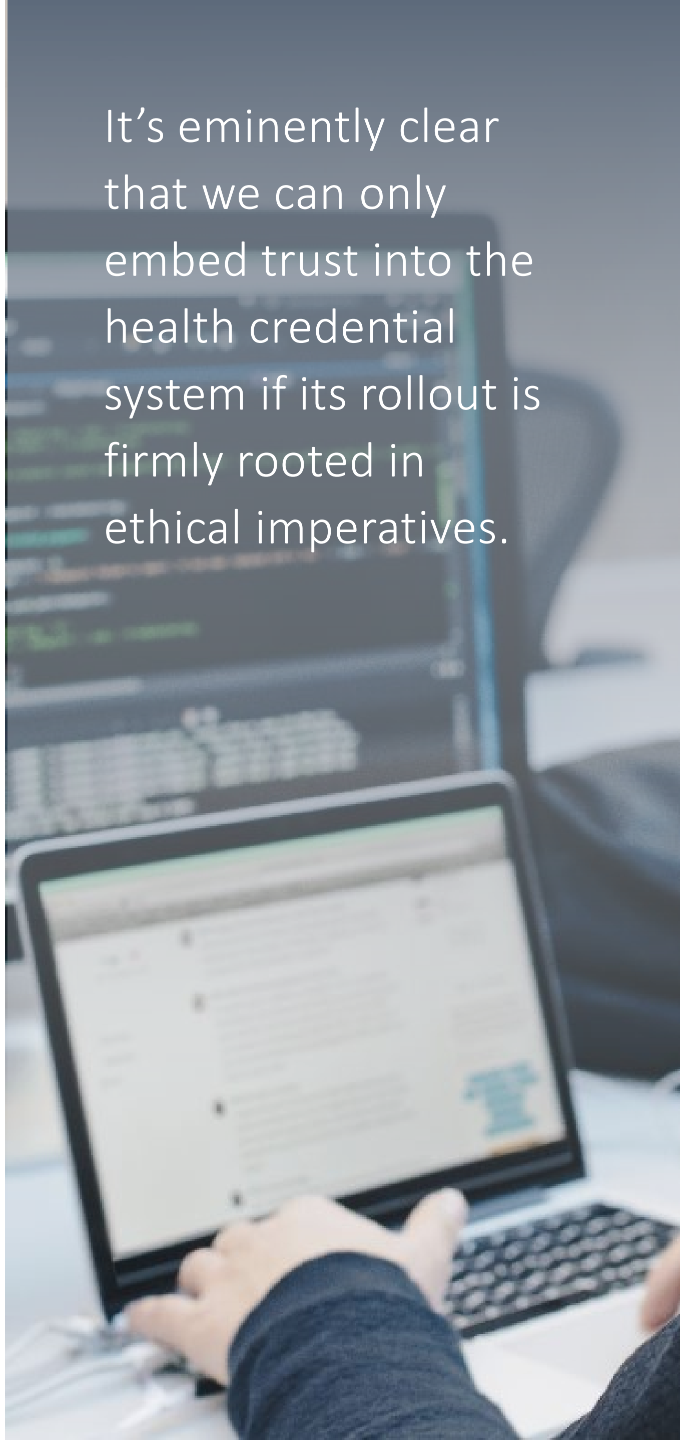
A new era of verification and trust

While it can be easy to get sidetracked by the countless programs that must be initiated to make digital health credentials work, these policies must ultimately revolve around the privacy rights of global citizens. Once again, technology solutions are outpacing policy considerations, raising ethical issues around people's fundamental rights and freedoms.

As credential verifiers attempt to tiptoe through the quagmire, there are several questions they should ask up front. For instance:

- When authorizing health credentials, what level of assurance are you prepared to accept as authoritative and accurate?
- Is there a way to review these credentials without accessing or storing private health data?
- Do you plan to create tiers of user experience? Do you even have the right to turn away someone who doesn't "pass" your verification process?
- How do you plan to convey your policies to customers to help drive transparency and build trust?
- Which technology partners can provide you with a system robust enough to weed out fraud and nimble enough to deliver a range of verification capabilities (such as vaccine credentials, negative test results, and antigen tests)?
- Does it make sense to build your own technology solution in-house or outsource it?
- Will you require consumers to sign a liability waiver?
- If you are presented with fraudulent credentials, how will you handle the situation?
- How will you avoid infringing on citizen rights if you lack the ability to trust and verify a consumer's credentials?

At this stage of the game, there are more questions than answers. Yet, despite the complexities, it's eminently clear that we can only embed trust into the health credential system if its rollout is firmly rooted in ethical imperatives.



It's eminently clear that we can only embed trust into the health credential system if its rollout is firmly rooted in ethical imperatives.

Authors and contacts

Emily Mossburg | Global Cyber Leader
emossburg@deloitte.com

Amir Belkhelladi | Canada Cyber Leader
abelkhelladi@deloitte.ca

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

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

Srini Subramanian | Global Risk Advisory GPS Leader
ssubramanian@deloitte.com

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

Contributors:

Esther Dryburgh| Risk Advisory – 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.

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.