Digital Identity in Health

Making health care more effective, efficient, and secure for Canadians

Insights from Interac Corp.

"A secure digital identity could eliminate minutes, hours, or even weeks of delay currently caused by the need to show or send physical copies of identity cards or other credentials."

Introduction

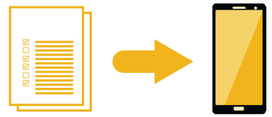
As in most developed countries, health care in Canada comprises a significant portion of the economy: in 2015, such spending – almost $5,800 per person – amounted to 10.4% of our GDP*. To compete and prosper in a technology-driven world, Canadians need secure, ubiquitous, and convenient digital identity systems, and a sector as important as health care – in both its public and private-sector aspects – stands to benefit greatly from digital identity in at least three ways.

First, and most obviously, through improved efficiencies. The need to identify oneself when seeking access to health services comes up frequently in every process: booking a doctor's appointment, picking up a prescription, checking into a hospital, registering in a new province. Even health care professionals need to identify themselves when requesting access to patient records or prescribing medications. At each step, a secure digital identity could eliminate minutes, hours, or even weeks of delay currently caused by the need to show or send physical copies of identity cards or other credentials. A system made faster through digital identities would be a less expensive system, freeing up resources that could be used in higher-impact areas.

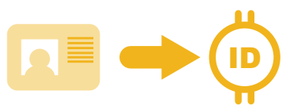
Second, by reducing the risk of heath care fraud – a continuing concern for governments and taxpayers. Provincial health cards may be applied for with forged documents, or, being physical, they may be forged themselves. Paper-based prescriptions may be falsified, or filled in the wrong person's name. Health service providers may bill payors (whether governments or insurance companies) for services not actually rendered. And while the total cost of health care fraud is difficult to estimate, it is likely that the expensive processes and manpower devoted to keeping fraud in check could be significantly reduced through digital identity systems.

Key benefits from digital identity

Efficiency



Security & fraud reduction



Improved outcomes

Finally, by improving health outcomes, which is a goal that patients, governments, and private-sector providers alike can support. Getting the right services to the right person without error – and preventing services or drugs being given to the wrong person – with the speed, efficiency, and convenience that secure digital identities enable, is key to raising the effectiveness of the health system as a whole. In short: healthier Canadians, at less cost.

This paper sets out five guiding principles that we think should lie at the foundation of any broadly-adopted digital identity system, and walks through three examples of how such capabilities could improve our health care system for the benefit of all Canadians.

* Source: Canadian Institute for Health Information https://www.cihi.ca/en/how-does-canadas-health-spending-compare-internationally

Our principles

Digital identity is easy to theorize about, but architecting and implementing a comprehensive, secure, and sustainable system is another matter entirely – and an important part of getting it right is having a clearly articulated set of principles to guide the effort. We believe that there are five:

User control & convenience

No one wants to entrust a system with their personal details if those details are going to be transferred to and stored by numerous parties – especially if this happens without the user's control or knowledge. At the same time, an identity system must be convenient and easy to use; if it isn't, it won't be adopted by Canadians already used to intuitive apps on mobile devices.

Ubiquity

Security risks abound when people have to create different identities and passwords for each public and private service they access: they'll often default to a single, easy-to-remember (and easy to crack) password, for example. At the same time, a digital identity that only applies to a handful of services will probably not be well adopted. A ubiquitous system is a more convenient and more secure system.

Security via abstraction

Even with the best user controls, identity data will end up in the hands of many different players in the health care ecosystem. A highly effective way of securing that data is to "abstract" it, by replacing a private identifier with a publicly-available one (like a person's email address) or by replacing it with a randomized number that serves as an authorized "token" for the purposes of the transaction – and is not useful for any other purpose.

Standards & openness

In any dynamic system, it's difficult to predict what the future will look like – so it's important to build today's solutions on universally-agreed standards. Not only does this reduce costs by eliminating the expense of building and then later having to adapt custom, one-off solutions, but it enables solutions built by others in the future to "plug into" the initial solution. Openness as an approach encourages adoption, innovation, and flexibility.

Trusted brand

No user is likely to adopt an identity solution built or maintained by an organization they don't trust; the question of identity is simply too important, and the impact of identity theft too great, to leave this to chance. Further, building a solution will require the cooperation and coordination of many players, and these players need to trust each other and the organization leading the effort.

Example 1

Prescriptions

The simplest example of the impact digital identity can have on the system – and on the patient experience – is the doctor's visit and prescription process.

Here's how it could work in a future with digital identities.

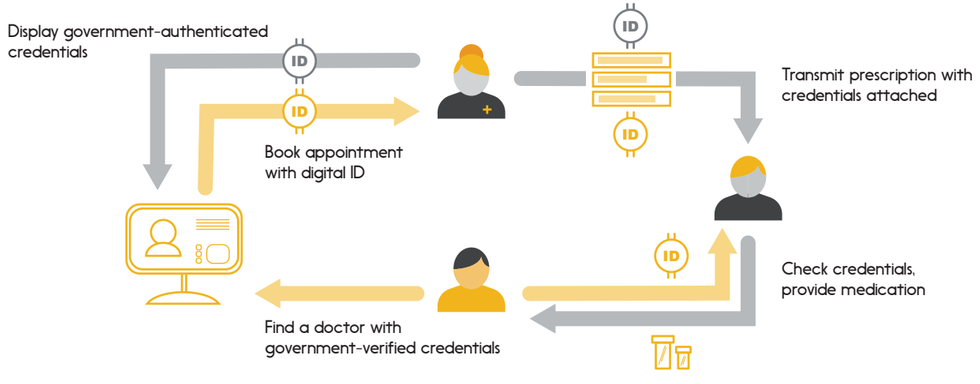
A person has a cough they can't seem to shake. Because they're new in town, they use an online, government-provided registry to find a local doctor, easily verifying their credentials because the doctor's licence is shown and has been digitally authenticated by the provincial ministry of health. Using their mobile device (since they're out shopping at the time), they access their doctor's website and book an appointment, authorizing it with the digital identity they carry in their device's mobile wallet. The appointment instantly appears in their calendar with a reminder notice enabled for the day before.

When they arrive, a quick tap with their phone sends their identification to the office's admission system, which marks them as "in the waiting room". With a reference to their digital identity, it also time codes their file for ministry billing purposes as soon as they've been called into the examination room.

The doctor prescribes some medicine for the patient's cough, and digitally signs the prescription so the pharmacy can validate both that the prescription is intended for this particular patient and that it was written by a licensed doctor – ensuring that a "chain of custody" is preserved from start to finish. The doctor sends that prescription electronically to the patient's preferred pharmacy.

The patient goes to their pharmacy to pick up the prescription. The pharmacist brings the medicine, and the patient authenticates themselves with their phone by providing a "tokenized" version of their digital identity. Certain that this is the right patient, the pharmacist hands over the prescription, accepts secure payment via the patient's digital wallet (a debit card, we'd like to assume), and uses the patient's tokenized identity to submit the insurance claim for the bulk of the price.

Prescriptions with digital identity



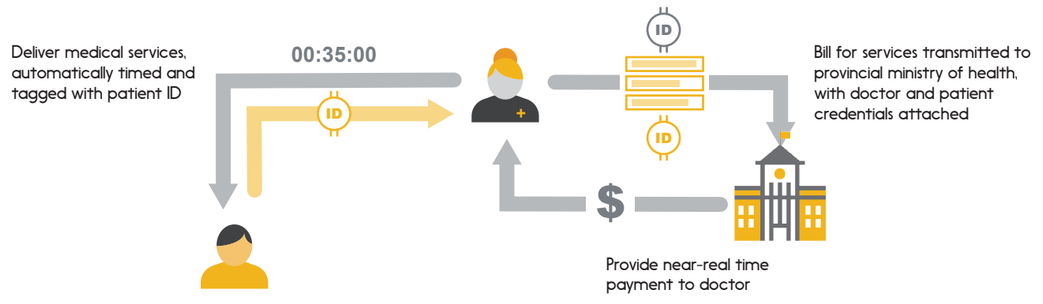
Example 2

Payments

As our patient leaves the doctor, the office automatically submits a services bill to the provincial ministry of health, detailing the services provided, the time required to provide them, and including the patient's identity to fully authenticate the invoice. Authenticated real-time invoices substantially reduce the risk of billing error and billing fraud, reducing overhead for medical practices and for the ministry of health. What's more, without having to allow significant time for billings to be reconciled between the two parties, it may become possible over the longer term for ministries to remit payments to doctors on a near-real-time basis.

Similar benefits would accrue to situations where medical service providers bill private insurance companies – for example, in the provision of physiotherapy services to auto accident victims. Digital identities would enable providers to authenticate each billable session, and the reduction of fraud risk that this entails for the insurance company (which would be far more sure that a bill is tied to a specific, verified patient) would enable them to pay providers more rapidly – while also reducing some of the overhead they currently devote to sniffing out fraud.

Payments with digital identity



Digital identity is not just about "may I?" but about "may you?", as well.

Example 3

Records

Let's say that a patient finds a new job in another province, and moves there with their family. For the first few weeks after arriving, part of their activity will be devoted to registering for government services in their new province – including health services.

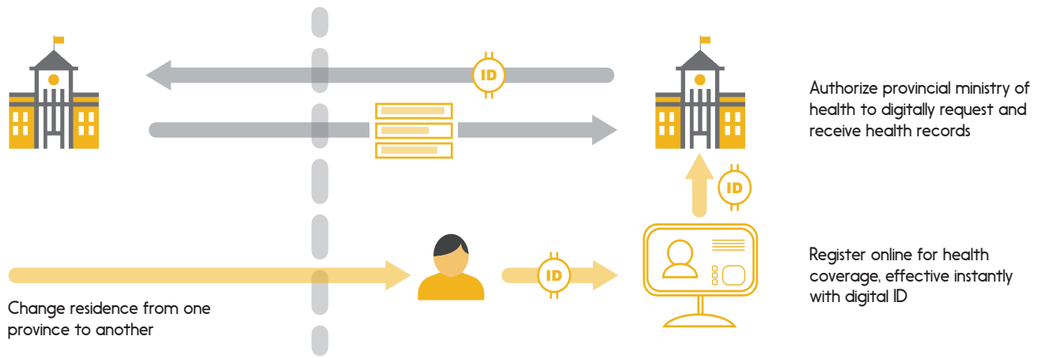
Instead of having to visit a ministry office in person to present their identification documents (birth certificate, driver's licence, etc…) and their various proofs of residency (utility bills or the like), the patient would be able to use their digital identity on a government website, proving both who they are and where they live in one simple, digital action. Even their health card would arrive in digital form (followed by, much later, the physical version); should an illness strike a family member soon after the move, they would be able to access local health services as smoothly as any other provincial residents.

Finally, having found a new family doctor, the patient would be able to use their digital identity to grant access to their medical records from the other province, enabling the doctor to benefit immediately from a comprehensive set of background information on the patient. The patient could also give permission to their doctor to share some or all of their medical records with specialists as required, giving them full control over who their information is shared with, for how long, and why.

In the same way, a digital identity would allow the patient to access their own records online. Personal access to medical records would improve patients' sense of ownership over their own data and health, allowing them to check immunization histories for their families, and with the help of apps, to make certain decisions without necessarily having to book a new doctor's appointment.

In this sense, digital identity is not just about "may I?" but about "may you?", as well. In other words, not only would digital identity make it easier for patients to gain access to healthcare services, but it would also give them the ability to control – in real time – which providers may access their confidential records for the purpose of giving them better-informed medical care.

Records with digital identity



Conclusion

Health care by its nature is often complicated and uncertain, and providing consistent and effective services across a country as big as ours has been a remarkable accomplishment. Digital identity promises to make this system even better:

More efficient, by reducing paperwork, reconciliation effort, and investigative overhead.

More secure, by reliably verifying the identity of each patient at system registration and when accessing services.

More effective, by reducing communication errors and fraudulent access to medicines, and by ensuring instant access to the right information when needed.

The potential is both exciting and close at hand. Digital identity capabilities can be rolled out over time, working with and improving the existing system in incremental steps — and sparking new innovations and services along the way. Following the principle of ubiquity, moreover, a digital identity system that works for health care should also be designed to work equally well for all other government services. We'll take a close look at some of these service categories in upcoming white papers.

"Not only would digital identity make it easier for patients to gain access to services, but it would also give them the ability to control which providers may access their confidential records."

For more information on this topic, visit innovation.interac.ca

Published September 2018