The Need for a National Digital Identity Infrastructure

Andre Boysen

Cyber security for health-care data has never been more important nor more vexing than it is today. Across the Group of Twenty countries, health-care spending consumes upward of 50 percent of government revenue, and its share continues to climb. In many places around the world, online access to health-care services is being held back, due to the highly sensitive nature of the data and our collective inability to provide viable protection for online service delivery. As a result, many things that could be done online with greater efficiency, such as seeing our health-care records or getting a new bank account, are instead delivered in person, at a much higher cost. Only the most basic and low-risk services are online today, and even those are beset by the huge overhead cost of data breaches and password resets. This is a global issue that plays out in communities everywhere.

Consider some of the other dynamics at play that contribute to the challenge. Some patients access health care every day; others access services every few years. Some patients are very internet savvy, while others don't want anything to do with online services that require a perpetual mindset of vigilance and active suspicion, as well as evergreen technical acumen.

The topology of health care is one of the most diffuse sectors of the economy, with no organizing force between government, hospitals, doctors, labs, researchers, patients, medical device makers and health-care foundations and registries (such as Canadian Blood Services and the Canadian Cancer Society). In fact, considering the problem as one of topology rather than one of security might provide some good insight as to the path forward.

It is clear that pushing more and more "point solution" security controls out in response to breaches has not solved the problem — it is chasing the symptoms rather than addressing the issue. In fact, this continuous change in access and control mechanisms has increased the attack surface. 2FA, or two-factor authentication, which uses a device to generate one-time codes, for example, has evolved to real-time intercepts of passcodes by criminals. So, too, have spoofing templates evolved to overcome on-device biometrics.

The current strategies have failed. Pulling back from online service delivery is not possible either — economics and patient safety require innovation. A different approach is needed — one where the security model is strong but hidden from end-users. Such a model could provide simplified access for patients while better mitigating the cyber threats. Hiding the security model improves the patient experience while maintaining proper controls for access.

Are Digital Health Cards the Answer?

Every Canadian has a health-care card, which enables them to access medical care when needed. Importantly, this same card can be used to convey their sharing wishes as regards organ and tissue donation; by registering as an organ and tissue donor, citizens also have the opportunity to save another person's life.

However, as sophisticated as the health-care system is today, there is a clear opportunity being missed. One of the issues currently plaguing the economy is the privacy and security surrounding digital identity. While digital identity and health care may seem unconnected, digital identity has the potential to change the health-care landscape and the way medical data is shared in Canada.

Canadians are able to give the gift of life through organ donation by registering their consent, but they have no way to share their health-care data — a massive resource that goes untapped, held captive because of its highly personal and sensitive nature. With the right tools and controls, giving patients control of their data will allow them to share it with researchers. We can also transform health-care delivery at the same time.

If a health card can indicate an individual's willingness to donate their organs, why can't it also allow individuals to access and donate health-care data? With adequate privacy and security measures in place, sharing that data is something that can be done every day. Data is a gift that keeps on giving.

Data Is the Fuel That Drives Health-care Innovation

Data is the fuel that drives health-care innovation through medical trials — the source for new drugs, devices and therapies and vital to improving health-care outcomes in

Andre Boysen is the chief identity officer at SecureKey. Andre has led the pioneering privacy-engineering in his work at SecureKey in the evolution of its services, including the Verified.Me service, the SecureKey Concierge service and the BC Services Card. He consults with SecureKey's public sector customers around the world on how to transform service delivery to offer citizens more choice, control and convenience while increasing business integrity and lowering costs. Recognized as a global leader on identity, privacy, digital transformation and blockchain, Andre is also a regular speaker, contributing author and media commentator.

Health-care spending consumes upward of 50 percent of government revenue, and its share continues to climb.

The duty of care with health-care data is high, because if data is leaked, there is no way to "refund" privacy. The data safety issue is preventing the health-care industry from delivering crucial services online; a solution needs to be found.
(Photo: Alexander Gatsenko/Shutterstock.com)

Canada. Connecting patients to doctors, and researchers to drug companies, is complex and expensive. Throughout the process, it's critical to manage consent, ensure privacy and protect access to patient health-care data.

Various studies allow for health-care data to be captured and gathered. From there, the data cannot be used without explicit knowledge and consent from the patient, yet no digital infrastructure is in place to ask individuals to consent to the use of their data. As a result, medical trials toil on, gathering data one study at a time.

According to Toronto University Health Network's Dr. Joe Cafazzo, setting up one medical trial for a new drug with 200 to 300 patients costs over $1 million, and requires enrolling patients, doctors, nurses and researchers into an online portal to gather and share data over the life of the study.[1] To secure the data, administrators distribute paper forms, gather signatures, confirm participant consent and issue passwords for everyone involved. All of the information-sharing infrastructure is set up, then taken down for each trial to manage protocols around data sensitivity, privacy and consent. While the protocols are necessary, there is no process in place for patients to opt in to participate in subsequent studies or to make data available only as a control sample.

This boils down to one issue that is impacting digital identity today: passwords. Regardless of whether passwords are long, changed several times per minute or composed of random characters, they are not secure enough to keep health-care data private. The data safety issue is preventing the health-care industry from delivering crucial services online — despite provinces spending 40 to 50 percent of budgets on health care today. If health-care data is leaked, there is no way to "refund" privacy, and the consequences may be that an individual is uninsurable or unemployable.

The duty of care with health-care data is high, but finding a solution to enable data sharing needs to be found.

Health-care Cost Implications of Password Misuse

Searching for a solution for password issues in health care, Dr. Aviv Gladman — chief medical information officer and emergency physician at Mackenzie Health and a trained electrical engineer — conducted a study to analyze how much password friction was costing the health-care sector. Dr. Gladman concluded that three percent of all health-care spending was on inefficient authentication due to doctors and nurses mistyping passwords, resetting passwords or losing password fobs (Gladman 2015).

In 2017, the Canadian Institute for Health Information estimated that total health spending in Canada was expected to reach $242 billion (Canadian Institute for Health Information 2017). According to Dr. Gladman's findings, that means that upward of $7.3 billion is being spent on password frustrations that are slowing down health-care delivery. This could be easily streamlined, resulting in additional savings and improved patient experience, if individuals could book appointments online or review lab results from a mobile device.

The wave of internet-connected devices that experience a similar password problem is getting worse. Many devices that Canadians are purchasing (stereos, cars, activity trackers, TVs, fridges and so on) are connected to the internet and run with connected apps with passwords. For example, some cars now come with an app that allows the owner to lock the doors, sound the horn or locate it from their phone. There have been cases where the vehicle location feature is still active and shows a past owner where the car is located even after it has been sold to someone else. Better controls are needed for health-care devices.

By contrast, Apple has a strong digital identity scheme for its devices. This gives consumers

comfort in sharing, for example, the heartbeat and movement data the Apple Watch produces throughout the day. This data is shared with Apple, but there is no way for patients to add this data to their health-care record or share it with their doctor.

Digital identity is bigger than health care — it's needed right across the economy. But there are crooks — they are out to cause harm, and they are good at it. In 2017 alone, there were 7.8 billion identity records stolen, according to a recent report (Risk Based Security 2018). Today, passwords are the only barrier to accessing sensitive systems and data; however, a good digital identity system will move us beyond this limitation so that consumers can do more online. Health care needs digital identity, and the rest of the economy does, too.

The World before the Electrical Grid

The state of digital identity today can be compared to that of electricity in 1869. Prior to the introduction of the standardized electrical grid in 1870, only the biggest factories had their own electrical generators, which were used to power light bulbs so that factories could run two shifts and increase productivity and output. After the electrical grid was introduced, there were massive efforts to convince businesses to join. There were two groups of businesses that said yes to joining the grid and two groups that said no.

Of those that said yes, the first group consisted of smaller businesses that did not yet have a generator due to their complexity and cost. They could join the grid at a reasonable cost, enabling them to run two shifts and compete with bigger players. The second group consisted of businesses that had a generator but disliked the distraction it represented from the core business of making products. These businesses used a generator because they needed light, but it was not core to the business, and joining the grid allowed them to focus on making products.

Among those that said no, the first group included businesses that were interested in the electrical grid but had recently invested in a new generator. They saw the appeal but took a wait-and-see approach while using the new generator they had already invested in. The second group of businesses believed their generator was core to the business and were worried about relying on a third party for a resource that was key to production.

What is interesting is that in the end, everyone joined the grid. From the standpoint of economics and simplicity, the offering was so compelling that businesses eventually found running their own generators every day to be too inefficient and taxing on the business. At that point, the number of use cases for electricity grew very quickly. Electricity was no longer solely about powering the light bulb — it expanded to many different uses that ultimately transformed the economy.

What Is the Parallel with Accessing Services Online?

Digital identity is a lot like the electrical grid. Every online service delivery organization on the internet is running its own digital identity generator. Facebook, Amazon, Netflix, Google, governments, schools, hospitals, financial institutions and telecommunications providers are all running their own fiefdoms of identity services. Today, the first digital identity grids are starting to emerge, meaning that service delivery organizations no longer have to run their own digital identity generators. Organizations can get out of managing the risky password services that they own and manage.

SecureKey, a leading identity and authentication provider, makes trusted access to online services easier and more private for Canadians, with better integrity and lower costs for business. SecureKey is in the process of developing the digital identity grid in Canada to solve the problems associated with today's online service delivery organizations. The current system is too difficult for consumers to use, and the costs are unsustainable. Businesses, governments, educational institutions and health-care organizations around the world are regularly experiencing data breaches, because no single organization can afford the massive investments required to make digital identity safe, convenient and private. It takes a village to make digital identity work.

In 2012, Canadian financial institutions partnered and launched the first version of this digital identity grid — a service allowing Canadians to reach Government of Canada

In 2017 alone, there were 7.8 billion identity records stolen, according to a recent report.

Good digital identity is something you can hold in your hands, simple to use and accepted everywhere, much like a credit card or mobile phone.

websites by using their banking credentials. Since the launch, more Canadians are making government transactions online, and business confidence in transaction integrity has increased substantially, because banking credentials are not often forgotten and are managed carefully. This has resulted in costs for government reducing by 80 percent over the prior generation of service, equating to close to $750 million in savings (Office of the Auditor General of Canada 2013, chap. 2).

Yet, as powerful and compelling as it was, the system did not solve the entire digital identity problem. The first generation of service was a safe replacement for multiple passwords. Now, what is needed is an easy, trustworthy and private way for consumers to prove who they are when signing up to access online services, such as health care. We need to book appointments, see our lab results, consult with our doctor, confer with a specialist, bring in our Apple Watch electrocardiogram and enable our families to exercise power-of-attorney decisions.

The Digital Identity Grid

What is good digital identity? Good digital identity is something you can hold in your hands, simple to use and accepted everywhere, much like a credit card or mobile phone. It is trustworthy and cost-effective for businesses and will provide Canadians with more choice, control and convenience. Through the emerging Canadian model, consumers will be able to combine their financial institution account with their mobile phone and government-issued ID to create a digital identity that is still physical (with the SIM card in their mobile device) and simple to use and can be used everywhere. Digital health cards will be added to this mix.

The new digital identity grid is launching in Canada in 2019. It will provide better business confidence for identity registration, use less data and lower costs. It will give consumers the control and convenience to manage their online life, and it will mean that possession of user data will no longer be enough to allow imposters to masquerade as someone that they are not. It will leverage blockchain technology, allowing for transparent, secure data tracking across devices. And it will support the global principles of privacy and security by design developed by Ann Cavoukian, former information and privacy commissioner for Ontario and current distinguished expert-in-residence at Ryerson University's Privacy by Design Centre of Excellence, who is providing privacy expertise for organizations working in this area.

Finally, it will meet the criteria of Canada's identity standards organization, the Digital ID and Authentication Council of Canada (DIACC). DIACC is composed of members from across Canada, from governments, financial institutions, telecommunications companies and more, alongside SecureKey, striving to make digital identity work for Canadians across the economy.

Creating the Digital Circle of Care for Patients

Modern medicine best practice holds that the health-care system empowers the patient by putting them in the centre of their own health-care story; each individual creates their own circle of care. We do not yet have the tools to allow patients to do this.

National digital identity infrastructure is what is required to solve the problem. Here in Canada, we are on the cusp of having a world-leading digital identity scheme. It is designed by Canadians for Canadians. And it is designed to work across the economy, so that businesses and consumers can conduct transactions online with trust, confidence and privacy.

It is not a technology problem (the technology exists); it is not a skills problem (we know how to do it); it is not a money problem (health-care costs would come down significantly). It is a problem of focusing national will.

Sharing health-care data is needed, achievable and worthwhile. Digital identity is required to make this happen. Consumers will be able to see and donate their data, allowing them to become health-care heroes every day.

Works Cited

Canadian Institute for Health Information. 2017. "Total health spending in Canada reaches $242 billion." November 7. www.cihi.ca/en/total-health-spending-in-canada-reaches-242-billion.

Gladman, Aviv S. 2015. "Identity, Context, and the Digital Clinical Moment." Presentation at IdentityNorth summit, May 7.

Office of the Auditor General of Canada. 2013. "2013 Fall Report of the Auditor General of Canada." www.oag-bvg.gc.ca/internet/English/parl_oag_201311_02_e_38796.html.

Risk Based Security. 2018. "Data Breach QuickView Report." January. https://pages.riskbasedsecurity.com/2017-ye-breach-quickview-report.

Endnotes

1 See http://ehealthinnovation.org/shedding-light-dark-side-digital-health-healthto-october-edition/.