FAIR Access to Personal Health Information in Private and Public COVID-19 Health Applications

André Carrington[1], Douglas G Manuel[1], and Carol Bennett[1]

[1]Ottawa Hospital Research Institute

October 28, 2020

Abstract

There are an increasing number of consumer smartphone and eHealth applications that are potentially helpful for controlling the COVID-19 pandemic. These applications include contact tracing, proximity tracking, eThermometers and heart rate monitoring. Consumers should have access to their data and the ability to share as much or as little, as they see fit, with public health agencies, healthcare providers or researchers–thereby respecting their privacy and their wishes. One patient's choice or risk does not affect another's. We recommend applying FAIR data principles, supported by changes to laws and governance, to meet these needs.

Introduction: the Need for Access

Open access of de-identified patient data has been an indispensable resource for understanding and controlling the COVID-19 pandemic. The online dashboard hosted by Johns Hopkins and other COVID-19 sites are examples of real-time tracking that aggregate worldwide COVID-19 testing, case and mortality data.(Dong et al., 2020) However, there remain major gaps in available open data such as a lack of sociodemographic information and data on predisposing factors for becoming infected or spreading COVID-19 infection.(Anderson et al., 2020) Additional COVID-19 information is collected by public health contract tracers that could be shared to improve our understanding of COVID-19 spread. As well, COVID-19 information could be shared using data from individual eHealth applications. However, privacy concerns have curtailed more widespread data sharing.

Contact tracing identifies people an infectious person may have had contact with, and possibly infected. Knowing the history of a person's proximity to others, based on cell phone information, can assist contact tracing (Kleinman and Merkel, 2020; Government of Canada). Identifying contacts is challenging and important for COVID-19 because of the large proportion of pre- or asymptomatic infectious transmissions that occur. The challenge is increased during re-opening as people come in contact with more people in public settings. Monitoring temperature, heart rate and respiration has the potential to identify COVID-19 prior to a person being aware of infection or for people with mild symptoms. Monitoring these symptoms can be performed through smartwatches and eThermometers (Chamberlain et al., 2020; Seshadri et al., 2020).

Many proximity tracking applications (O'Neill et al., 2020) and other smart applications either do not allow data sharing with public health or a patient's clinical care team or make sharing overly challenging. Two scenarios are common. In the first scenario, data are on a person's smart application but there are no or limited provisions to share the data, or it is prohibitive to do so. In the second scenario, a person's data are shared with the company that has developed the application, where it is treated as a company asset. People have limited control over how the company uses or shares data with others. Patients cannot easily direct the application developer to share their data with public health agencies or their primary care team. We advocate for data access and sharing and we identify the recent FAIR data principles as the relevant approach.

The FAIR Data Principles

In science research, the ***FAIR data principles*** (Wilkinson et al., 2016; Force11, 2014) have gained recognition— *FAIR* refers to research data being Findable, Accessible, Interoperable and Reusable. That is, we should be able to find where our data resides and have access our data; and, upon access, data should be interoperable with other software and useful (reusable) because it is well-described.

The FAIR principles should also be applied to data held in private or public organizations, supported by individual privacy, for the patient's use, and if/as they direct, for society's **beneficial use** too, e.g., in research or public health management and surveillance. If there are supporting changes to laws and governance, beneficial use can be authorized by the patient's **proactive express consent** that **delegates and mandates access** by a third party on the patient's behalf. This means that people should be allowed to delegate sharing of their data according to FAIR principles in a useful, efficient and timely manner. Patients should be allowed to express and enforce their wishes regarding their data, in alignment with values and strategies that put the patient first (Ministry of Health and Long-Term Care, 2015). After all, the patient or data subject is the *inherent* owner of their data.

While the private sector has some incentives to share data, such as corporate goodwill, they are under no obligation to do so. There are also barriers in access to health data within Canada's public health care system — e.g., barriers to requestors in Canada who are not affiliated with the custodian and are from a different location in Canada. Changes to the law can address these barriers, both in the will to share data and the timeliness of doing so.

Gaps in the Law to Meet Patients' Wishes

In Canada, privacy and access to information laws do not uniformly require private companies and public entities to follow the four FAIR data principles for patients' use of their data. There are gaps in the coverage of each principle, and importantly, the system does not attend to some patients' wishes in an effective and timely manner.

In Ontario, there has been steady progress on several principles. Access to a patient's record is largely required, but web apps were not covered by Ontario's health law — the Personal Health Information Protection Act (PHIPA) (Fabiano, 2020; Ontario Legislature, 2020a). An amendment to address this omission was written into PHIPA this year (March 2020) but has no specified date for when it will come into force. Interoperability (also called data portability) is improving with PHIPA recently requiring an electronic record, which will be useful once the regulations (Ontario Legislature, 2020b) and specifications for the electronic record come into effect in January 2021 and an unspecified date, respectively. To ensure records are reusable, entities are required to provide an explanation of terms and abbreviations, but *only if it is reasonably practical* (Ontario Legislature, 2020a).

A large gap that remains is finding records. One author has found it challenging to navigate government services through multiple web searches and phone calls to find immunization records from years past. Going forward, CANImmunize alleviates this challenge by having patients managing their own immunization records (Houle et al., 2017). However, this solution highlights a systemic problem: the onus is on the patient.

Currently, the patient is at the center of finding, requesting, receiving, resending and negotiating their records. Some patients want that, and that option is always available, but other patients want their ***wishes*** to be at the center, to be respected and carried out. They want public health to have their information from a web app, or their family physician to have a copy of their records, or they want to support research–without having to be proficient with technology, privacy laws, the logistics of government or private entities and the semantics of health care.

Changes to the Law and Supporting Governance

To have patient wishes at the center without the patient themselves carrying the technical and logistical burden requires new capabilities, such as delegation and a trusted governing entity, to support it.

Current laws only require information to be provided directly to the patient—not **delegated** to third parties, such as a health agency or a primary care provider, in accordance with the patient's wishes. In fact, a recent amendment in PHIPA, which has not yet come into force, clarifies that if a provider of a web app seeks access to a patient's record, ***with the patient's authorization and consent***, a health information custodian (government or private) does not have to provide access to the web app provider, but the custodian does have to provide access to the patient directly. This deviation from a patient's wishes (i.e., to delegate access in some cases) occurs because there isn't a system or process by which a health information custodian can trust the validity of such authorizations. However, a governing entity (Fig. 1) empowered by the government could play that role and imbue trust in the system.

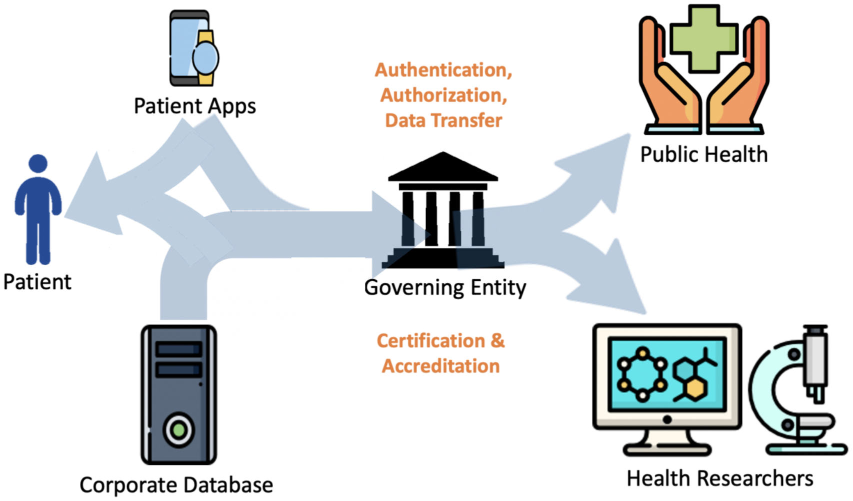

Figure 1: A governing entity can facilitates trust for data sharing and access with proactive delegation.

We recommend that laws and regulations include the right of patients to **delegate** their access to third parties in an **ongoing proactive manner** at the patient's request and direction. The patient may opt for automatic consent and provision, or notification to decide on consent. We also recommend that patients have the right to specify **a group** of third parties **specified by criteria**, to meet the patient's wishes, e.g., using the concept of "layering" (Privacy Commissioner of Canada, 2018).

> Patients can choose if they want to share their data, with whom, and how much or how little they want to share, thereby respecting their privacy and respecting their wishes–and notably, one patient's choice or risk does not affect another's.

Trustworthy proactive delegation does not just meet the patient's wishes it creates a more effective and efficient system for sharing data in matters of public health and research. That is, if proactive delegation creates a legal **mandate** on custodians to share data, then it removes the need to negotiate data-sharing agreements between the data custodian (the company or public entities that either hold or make applications that hold patient data) and third parties. Custodians often hold data hostage in the name of liability and risk causing ***immense delays*** in data sharing.

However, with trustworthy authorization from a patient, and sufficient governance, a custodian is absolved of that risk and they must share data in a timely manner. In other words, it should not be a question of whether or not a custodian trusts the recipient of data, but if a trusted governing entity does instead.

Hence, our proposal requires a governing entity (Fig. 1) that offers trustworthy processes for the patient, custodian and recipient to identify, authenticate and authorize each other. Trusted processes are needed to prevent fraudulent requests, to prevent mistaking one patient for another with the same name. The governing entity would also certify and accredit recipients of data, and collect, manage and enforce patient wishes. Data custodians and application developers may ask patients if they want their information shared, however, patients will be directed to the governing entity to manage their directives and delegation in a trusted manner free of conflicts of interest.

The governing entity, or their agents, could also act as a clearinghouse for access and exchange of data, so that private companies are not required to make connections to or accept connections from multiple requestors, which would be burdensome. In practice, because healthcare is provincially regulated, each province may have its own governing entity and coordination between provinces would be needed.

Finally, all of these concepts would need to be articulated in laws and regulations. We note that, legal mandates can sometimes have unforeseen consequences with private organizations that are custodians of data–e.g., an application provider could choose not to comply with the law, incurring delays during legal wrangling (Zimonjic, 2020) or they could discontinue their service in Canada.

Discussion and Conclusions

We recommend FAIR principles be followed for sharing individuals' COVID-19 and health data. Many aspects of the principles could and should be followed immediately to support efforts to control the pandemic. FAIR principles can be supported by patient charters. However, changes to privacy regulation and oversight are required to robustly support a shift in responsibility for risk and trust to support good data practice among data custodians, individuals and organizations that receive patient data.

For too long we have let data remain in silos of individual data custodians, with unrealized benefits to the individual and society. Current data sharing approaches emphasize the responsibility of data custodians to protect individuals' data. Data custodians and application developers need to allow patients to access their own data and delegate access to their data, according to FAIR principles. Individuals should have the right to share their data with whom they wish.

References

Geoffrey Anderson, John William Frank, C David Naylor, Walter Wodchis, and Patrick Feng. Using socioeconomics to counter health disparities arising from the covid-19 pandemic. *BMJ*, page m2149, jun 2020. doi: 10.1136/bmj.m2149. URL https://doi.org/10.1136%2Fbmj.m2149.

Samuel D Chamberlain, Inder Singh, Carlos A Ariza, Amy L Daitch, Patrick B Philips, and Benjamin D Dalziel. Real-time detection of COVID-19 epicenters within the United States using a network of smart thermometers. *medRxiv*, 2020. doi: 10.1101/2020.04.06.20039909. URL https://www.medrxiv.org/content/early/2020/04/10/2020.04.06.20039909.

Ensheng Dong, Hongru Du, and Lauren Gardner. An interactive web-based dashboard to track COVID-19 in real time. *The Lancet Infectious Diseases*, 20(5):533–534, may 2020. doi: 10.1016/s1473-3099(20)30120-1. URL https://doi.org/10.1016%2Fs1473-3099%2820%2930120-1.

Daniel Fabiano. Significant Changes to Ontario's Health Privacy Law: New Enforcement Powers and Technology Requirements. March 2020. URL https://www.fasken.com/en/knowledge/2020/03/significant-changes-to-ontarios-health-privacy-law/.

Force11. Guiding Principles for Findable, Accessible, Interoperable and Re-usable Data Publishing version B1.0. 2014. URL https://www.force11.org/fairprinciples.

Government of Canada. Download COVID Alert today. URL valuehttps://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert.htmlhere.

Sherilyn KD Houle, Katherine Atkinson, Michelle Paradis, and Kumanan Wilson. CANImmunize: A digital tool to help patients manage their immunizations. *Canadian Pharmacists Journal/Revue des Pharmaciens du Canada*, 150(4):236–238, 2017.

Robert A Kleinman and Colin Merkel. Digital contact tracing for COVID-19. *CMAJ*, 2020.

Ministry of Health and Long-Term Care. *Patients First: a Proposal to Strengthen Patient-centred Health Care in Ontario*. Ontario Long Term Care Association, 2015.

Ontario Legislature. Personal Health Information Protection Act, 2004, SO 2004, c. 3, as amended on July 8, 2020 by the Connecting People to Home and Community Care Act, 2020, S.O. 2020, c. 13 - Bill 175. *Ontario, Canada: Ontario Legislature*, 2020a.

Ontario Legislature. Ontario Regulation 329/04 under Personal Health Information Protection Act, 2004, SO 2004, c. 3, Sched. A, as amended on Oct 1, 2020 by Ontario Regulation 569/20. *Ontario, Canada: Ontario Legislature*, 2020b.

PH O'Neill, T Ryan-Mosley, and B Johnson. A flood of coronavirus apps are tracking us. Now it's time to keep track of them, 2020. URL https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/.

Privacy Commissioner of Canada. Guidelines for obtaining meaningful consent, 2018. URL https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.

Dhruv R. Seshadri, Evan V. Davies, Ethan R. Harlow, Jeffrey J. Hsu, Shanina C. Knighton, Timothy A. Walker, James E. Voos, and Colin K. Drummond. Wearable Sensors for COVID-19: A Call to Action to Harness Our Digital Infrastructure for Remote Patient Monitoring and Virtual Assessments. *Frontiers in Digital Health*, 2:8, 2020. ISSN 2673-253X. doi: 10.3389/fdgth.2020.00008. URL https://www.frontiersin.org/article/10.3389/fdgth.2020.00008.

Mark D Wilkinson, Michel Dumontier, IJsbrand Jan Aalbersberg, Gabrielle Appleton, Myles Axton, Arie Baak, Niklas Blomberg, Jan-Willem Boiten, Luiz Bonino da Silva Santos, Philip E Bourne, et al. The FAIR Guiding Principles for scientific data management and stewardship. *Scientific data*, 3(1):1–9, 2016.

Peter Zimonjic. Privacy commissioner asks federal court to open hearings into Facebook's violation of privacy. https://www.cbc.ca/news/politics/facebook-privacy-commissioner-hearing-1.5454525, February 2020. URL https://www.cbc.ca/news/politics/facebook-privacy-commissioner-hearing-1.5454525.