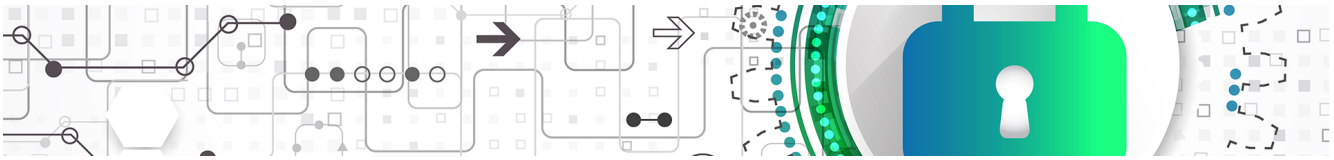

Making More COVID-19 Data Available - Privacy and the Sharing of Patient Data in COVID-19 Healthcare

March 31, 2020

By Noel Courage and Amanda Branch

Canadian institutions and companies are subject to federal and provincial laws relating to the collection, use and disclosure of personal information. Personal information is broadly defined as information about an identifiable individual and could potentially include de-identified information if it could be readily rendered identifiable. These laws are particularly strict for highly sensitive personal health information. It is easy to understand why data is generally kept confidential and privacy is paramount in a health-care context (click here for our earlier article). There are compelling reasons why more data needs to urgently be made publicly available in a pandemic, while respecting individual patient privacy.

Getting more information out to the public

Tracking and predicting the spread of COVID-19 and individuals' responses to it is of crucial importance, and governments and health organizations need all the help they can get. There can understandably be limited resources in compiling and analyzing information when healthcare resources are being overwhelmed by patients in need. The extra effort taken now to collect and analyze information is critical to develop a playbook to counter COVID-19 in the future. -

Hospitals should continue to comprehensively record and, as permitted, share data with public health agencies. Without proper collection and sharing of comprehensive basic health information, health care providers can feel like they are operating with only a partial picture of the virus and how to treat it. It is also helpful for public health agencies to share aggregated or anonymized information with the public so they have a fuller understanding about the extent of community spread of disease. The public release of data is more than simply an exercise in transparency. It provides important public outreach and it is educational. Data is also a basis for local government policy decisions, for example, whether to close businesses or restrict travel. Public compliance with government policy on protective measures and travel restrictions depends in part on their awareness and acceptance of the public health data.

Collection of data

The data must be captured as fully as possible once necessary consents are in place (patient consent may be express, implied or obviated in some cases). It is critical that the backlog of diagnostic testing be resolved to collect as much useful input data as possible. In jurisdictions where there are limited test kits available, and unsuspected mild cases do not qualify for testing (self-isolate instead), the "curve" has been slower to flatten. Here in Ontario, there have been as many as 10,000 pending test results at times, and reports of over a week wait for results in some areas. Testing capacity and through put need to increase to get better input data.

The benefits of collaboratively analyzing collected data

There is no substitute for human analysis. However, everyone recognizes that all tools at our disposal need to be utilized. Technology, such as artificial intelligence ("AI") can step in, particularly in analyzing large amounts of patient data after it has been collected by hospitals. This is an area where healthcare providers may have their own in-house solutions, but often they collaborate with outside companies to access expertise. The shared data in a COVID-19 context could include data about initial patient assessments, comorbidities (underlying health issues), drug treatments, physical treatments (e.g., ventilators), timelines, demographics, geography and patient outcome. For companies developing healthcare AI solutions, large volumes of quality input data are essential to allow the AI to learn quickly and provide useful

output. Read our article here about digital health companies and the power of AI in healthcare.

Any disclosure of collected data must comply with privacy legislation - Privacy Commission Views

Using large volumes of data can be at odds with privacy legislation, however, it need not be an impediment to getting effective data into healthcare software solutions.

Many federal and provincial privacy commissioners have published guidance noting the importance of complete and accurate information flow during a crisis and how this can be permitted through applicable privacy legislation.

For example, in its statement the Office of the Information and Privacy Commissioner of Newfoundland and Labrador urges "do not let privacy considerations put anyone's health at risk." It released a document entitled "*Don't Blame Privacy – What To Do and How To Communicate in an Emergency*" which, among other things, notes that both the *Access to Information and Protection of Privacy Act, 2015* and the *Personal Health Information Act* include provisions that allow for disclosure in emergencies or when the public interest trumps the protection of privacy.

Similarly, the Office of the Privacy Commissioner of Canada has released guidance, *Privacy and the COVID-19 outbreak*, which discusses when personal information may be disclosed by a private or public sector entity without consent.

The Office of the Information and Privacy Commissioner of Alberta released a statement, *Privacy in a Pandemic,* which also stresses the import of ensuring that public bodies, health custodians and private sector organizations know how personal or health information may be shared during a pandemic or emergency situation. Its statement also confirms that all three of its privacy laws include provisions which allow for the sharing of personal or health information in the event of an emergency.

How to prepare health data for sharing - aggregated or de-identified data

Every type of disclosure must comply with privacy laws. For example, a health authority may disclose information to an arm's length research partner or make it publicly available. Organizations may be hesitant to disclose personal or health information because they are unclear about whether the disclosure is permitted under applicable legislation.

A key tool for sharing information is to use de-identified or aggregated data. Data that is truly de-identified, anonymized or aggregated is not within the definition of "personal information" (how to "truly" render data de-identified or anonymous is beyond the scope of this article). Using aggregated and anonymized data can be very useful in identifying trends.

It is important to be mindful of potential re-identification risks and whether the "anonymous" data release could actually lead to identification of an individual. As a hypothetical example, if it is disclosed COVID-19 Patient 500 is female, is in their 30s, lives in Milton, Ontario, traveled to Italy in March, and has diabetes as an underlying condition, then that narrows pool of individuals that could fit that criteria, and privacy issues must be carefully measured.

Sharing collected data with research partners using data sharing agreements

Health care institutions also typically control use and retention of anonymized data through agreements with companies. Data sharing agreements can be used to facilitate the transfer of data between organizations or institutions. These types of agreements identify the parameters which govern, for example, how each party may collect, use, analyze, safeguard, transmit, store, retain and destroy data. Data sharing agreements can also ensure that both parties have considered and are abiding by any obligations that may exist under provincial privacy statutes or various research and ethical guidelines.

These information sharing initiatives can facilitate health care delivery and research projects and can provide valuable data needed for AI systems.

Sharing collected data with the public

Anonymizing data can also facilitate public sharing of data. We have seen governments share daily reports on anonymized patients. Public sharing of anonymized or aggregated information is important for public education, research, and to round out the information that healthcare workers receive from their own institutions.

The importance of properly assessing privacy issues and making data quickly available is apparent. For example, the extent of community transmission can appear to be greatly understated in the absence of up to date health data. Younger demographics seeing only mortality demographics may believe that they are overall low risk if hospitalization and ICU data by age group is not released (death is rare in youth, but hospitalizations or ICU admissions are more common). Powerful AI

software tools may be able to plug some of the gaps in data collection and analysis, but AI does this best when we feed as much information into it as possible. As the scope of data release by health authorities evolves, data releases must be clearly qualified as to the restrictions on the quality of the data released (e.g., number of tests backlogged).

Conclusion

Privacy law balances patient protection with allowing public health authorities to generate and share their best data in aggregate or anonymized form. The collection of the best data and transparent release to research partners and the public are critical for managing the COVID-19 situation.

We appreciate the challenging and important work being done by public health authorities, and this article is provided as a constructive comment to explain how data is shared in compliance with privacy laws.