# PANDEMICS IN A CONNECTED WORLD: INTEGRATING PRIVACY WITH PUBLIC HEALTH SURVEILLANCE

**Chantal Bernier, Liane Fong, and Timothy M. Banks***

*The tragedy of the Ebola pandemic illustrates and confirms the need for information sharing in a coordinated pandemic response. However, high-profile cases reported in the news media, videos of sick, dying, or orphaned individuals in highly intimate and tragic situations as well as public health news conferences and hospital statements have brought to light the privacy implications of pandemic news reporting and public health intervention measures. This article contributes to the ongoing legal, ethical, and social debate regarding the role, if any, to afford to personal privacy in an effective, globalized, and electronic public health surveillance system and pandemic response. Our working assumption is that there should be a role. However, privacy governance frameworks are, at best, incomplete in ensuring effective and protective use of personal information in pandemics response.*

## 1. Context

In the 21st century, public health policies and interventions must contend with high human mobility, cross-border data sharing, and unprecedented data analytics capability, all while expectations of privacy continue to evolve. Data surveillance has become a key component of pandemic response plans. Experts predict that the future of public health data surveillance will involve the automatic collection of patient data from electronic health records, which may include the patient's name, address, risk factors, previous immunizations, and treatment.[1] Data collection for pandemics intervention would therefore become a by-product of electronic health record systems used in clinical care. One can imagine the pressure to share information across state borders for even more effective global surveillance.

While public health objectives are imperative during a pandemic, patients and suspected patients will be quick to highlight the privacy risks of pandemic response measures such as the public and institutional dissemination of personal information. At the individual level, these risks include ostracism, stigmatization, exposure of

---

* Chantal Bernier is a Counsel, Liane Fong is an Associate, and Timothy M Banks is a Partner, each at Dentons Canada LLP. The views expressed in this paper are the authors' alone as of the date of writing this paper. They do not represent those of our clients or firm, and our views are subject to change in this highly dynamic area of law. We are grateful for the research assistance of Aiwen Xu, Student-at-Law, in the preparation of this paper.

[1] See e.g. Office of the Privacy Commissioner of Canada, "Use of Data from the Electronic Health Record for Health Research: current governance challenges and potential approaches", by Donald J Willison (Ottawa: OPC, March 2009) at para 1.2.3, online: <https://www.priv.gc.ca/information/research-recherche/2009/ehr_200903_e.asp> ("[w]ith the advent of the common interoperable [electronic health records], gleaning of data for public health reporting is likely to become automated")."

lifestyle, and restriction of freedom. At the collective level, intrusive measures may lead to discrimination, the erosion of medical support through the alienation of potential workers, and the subversion of containment efforts due to the reluctance of patients to seek treatment for fear of the consequences**.**

Therefore, in the context of electronic global information sharing and analysis, the full realization of public health surveillance goals to prevent and control pandemics requires commensurate safeguards to protect individual privacy and information security. Policy makers must aim to develop a framework that balances individual and collective interests. As discussed below, this will require both technological and administrative safeguards that are commensurate with the serious risks.

## 2. A few facts to ground our legal analysis

A pandemic is defined as the global outbreak of a disease, entailing, by definition, cross-border manifestations.[2] Public health surveillance is described as the "continuous, systematic collection, analysis and interpretation of health-related data needed for the planning, implementation, and evaluation of public health practice."[3] The information exchange is ideally multi-institutional and multi-disciplinary. Personal health information relates to the individual, while aggregate health data is population-level data reflecting collective trends. Some interventions require personal record-level data, while others require merely population-level data.[4] In addition to personal health data, public health surveillance may also need to rely on other personal information such as cell phone data or other geographical location systems. Mobile phone data (in the form of call data records) are viewed as important mechanisms for providing researchers with the ability to map outbreaks and track population flows so as to anticipate future areas of outbreaks and implement preventative measures.[5] In Mexico, for example, analysis of call data records has

---

[2] World Health Organization bulletins have referred to the classic definition of "pandemic," which is "an epidemic occurring worldwide, or over a very wide reach, crossing international boundaries and usually affecting a large number of people". See Heath Kelly, "The classical definition of a pandemic is not elusive" (2011) 89:9 Bulletin of the World Health Organization 540, online: <www.who.int/bulletin/volumes/89/7/11-088815/en/>, citing JM Last, *A Dictionary of Epidemiology*, 4th ed (New York, Oxford University Press, 2001).

[3] World Health Organization, "Public health surveillance" (2014), online: WHO <www.who.int/topics/public_health_surveillance/en/>.

[4] For example, certain pandemic response measures such as contact tracing or "other investigations that require public health to communicate directly with patients" require personal information. See Khaled El Emam et al, "Physician Privacy Concerns When Disclosing Patient Data for Public Health Purposes During a Pandemic Influenza Outbreak" (2011) 11:454 BMC Public Health, online: BMC <www.biomedcentral.com/1471-2458/11/454>.

[5] "Call for Help", *The Economist* (25 October 2014), online: <www.economist.com/news/leaders/21627623-mobile-phone-records-are-invaluable-tool-combat-ebola-they-should-be-made-available>. See also Pierre Deville et al, "Dynamic Population Mapping Using Mobile Phone Data", (2014) 111:45 Proceedings of the National Academic of Sciences of the United States of America 15888, online: <www.pnas.org/content/111/45/15888.full>. Non-profit

helped to measure how effective government mobility restrictions on citizens were in controlling the spread of the H1N1 flu epidemic.[6] In many cases, population-level data may simply be insufficient when dealing with serious virulent diseases that may require contact tracing and isolation measures to control spread of the illness.

Personal health information can be eponymous (where the individual's name is included), pseudonymous (where the name is replaced by a code number), or anonymous, de-identified, or anonymized (where the identifiers have been removed from the health information).[7] Technologists remind us regularly that even anonymized information can be linked back to identifiers with lesser or greater effort depending on numerous factors, such as the size of the sample and the nature of the information that is not de-identified.[8] However, a practical approach would favour the deployment of anonymization where the process to re-identify would be so arduous to make it remote and unlikely.

Intervention in pandemics includes several forms of personal health data collection, dissemination, and analysis. For example, pandemic response plans will call for reporting the identity of ill or suspected ill individuals to front line health workers and to multi-jurisdictional and multi-disciplinary authorities. These plans may also enable authorities to employ such methods as active surveillance of symptoms, isolation, quarantine, and contact tracing – including "aggressive contact tracing," i.e., tracing persons who have been in contact with the ill individual.[9]

---

organization Flowminder uses "anonymized mobile phone network data, household surveys, and remote sensing data to improve planning and operational decision making in a range of areas including disaster response and climate impacts, disease outbreak prevention, and poverty reduction." They only work with anonymized data at cell tower resolution or lower. Moreover, they sign MOUS/NDAs with participating telecom operators and store data in accordance with the industry's standard security guidelines. See Flowminder, "For Telecom Operators", online: Flowminer.org <www.flowminder.org/about/telecom-operators/>.

[6] United Nations Global Pulse, "Mobile Phone Network Data for Development" (October 2013) at 5, online: UN Global Pulse <www.unglobalpulse.org/sites/default/files/Mobile%20Data%20for%20Development%20Primer_Oct2013.pdf>.

[7] Canada Health Infoway & Pan-Canadian Health Information Privacy Group, *Privacy and EHR Information Flows in Canada, Version 2.0* (31 July 2012) at 41, online: Canada Health Infoway <https://www.infoway-inforoute.ca/index.php/resources/reports/privacy/doc_download/626-privacy-and-ehr-information-flows-in-canada-version-2-0>.

[8] Adam Tanner, "Harvard Professor Re-Identifies Anonymous Volunteers In DNA Study", *Forbes* (25 April 2013), online: Forbes.com <www.forbes.com/sites/adamtanner/2013/04/25/harvard-professor-re-identifies-anonymous-volunteers-in-dna-study/>. For a discussion and analysis of academic articles that critique the effectiveness of de-identification as well as a discussion of effective de-identification standards, see Information and Privacy Commissioner of Ontario & Information Technology and Innovation Foundation, "Big Data and Innovation, Setting the Record Straight: De-identification Does Work", by Ann Cavoukian and Daniel Castro (Toronto: IPC, 16 June 2014), online: <www.privacybydesign.ca/content/uploads/2014/06/pbd-de-identification_ITIF1.pdf>.

[9] Public Health Agency of Canada, "The Canadian Pandemic Influenza Plan for the Health Sector" (Ottawa: PHAC, 2006) at Annex M, online: <www.phac-aspc.gc.ca/cpip-pclcpi/pdf-e/annex_m-eng.pdf>; World Health Organization, Department of Communicable Disease Surveillance and Response, *WHO Consultation on Priority Public Health Interventions Before and During an Influenza Pandemic* (Geneva: WHO, 2004) at 26, online: WHO Regional Office for Africa

In the event that human-to-human transmission of the disease is possible, privacy issues affect not only the person who is directly affected by a pandemic illness but also his or her contacts. In these cases, many individuals may be swept up into the public health care surveillance system prior to diagnosis. Serious illnesses that are easily transmitted may require isolation for a lengthy period of time until the likelihood that the person is a carrier can be ruled out or eliminated. Even if the person is not a carrier, the mere fact of isolation will most certainly involve revealing intimate details and sensitive information to friends, neighbours, family, employers, and social and religious affinity groups. Certainly, circumstances may require efforts such as isolation. However, mere knowledge that the person has come into contact with the illness may result in social isolation and stigmatization.

Without question, clinical care and pandemics control require a certain degree of collection, disclosure, and analysis of personal information. The test for legitimacy of this use of personal information is one of proportionality and security. Privacy and security challenges arise from the difficulties around consent, the possible duty to disclose, the scope of dissemination – including across borders – the vulnerability of electronic platforms, the determination of consistent use, and balancing respect for individual privacy with the collective benefits of data analytics.

## 3. Privacy Implications

### (A) Duty to Disclose

Whether patients suffering from an illness in a state of pandemic have a freestanding duty to disclose their infection or suspected infection has not been widely tested on a general basis in Canada. However, disclosure obligations can be imposed through legislation. Certain provincial health acts require persons who suspect that they are infected with a specified communicable disease to place themselves under the care of a medical practitioner or direction of a public health official.[10]

In relation to pandemics, the closest situation to the duty to disclose is the legislative designation of reportable illnesses. During the 2003 SARS outbreak in Toronto, public health authorities took the voluntary quarantine and compliance approach. When the Ontario government designated SARS as a reportable, communicable, and virulent disease under the Ontario *Health Protection Promotion Act* ("*HPPA*"), public health authorities received the legislative authority to issue orders to detain and isolate individuals.[11] During the outbreak, almost all patients who

<www.afro.who.int/fr/downloads/doc_download/5116-who-consultation-on-priority-public-health-interventions-before-and-during-an-influenza-pandemic.html>.

[10] See e.g. Nunavut's *Communicable Diseases Regulations*, RRNWT 1990 c P-13, s 2, as duplicated for Nunavut by s 29 of the *Nunavut Act*, SC 1993, c 28; Saskatchewan's *Public Health Act, 1994*, SS 1994, c P-37.1, s 33; Yukon's *Communicable Disease Regulations*, YCO 1961/048, s 3; Prince Edward Island's *Notifiable Diseases and Conditions and Communicable Diseases Regulations*, PEI Reg EC560/13, s 4.

[11] For example, the Ontario *Health Protection Promotion Act*, RSO 1990, c H.7, s 22 [*HPPA*], authorizes a medical officer of health to issue an order under prescribed conditions in order to control the risk of the

were asked accepted the request for quarantine voluntarily. Only 27 written orders mandating quarantine under the Ontario *HPPA* were issued.[12]

The federal *Quarantine Act*, which is intended to restrict the spread of communicable disease in Canada, also imposes a duty to disclose in certain circumstances.[13] The Act imposes a requirement on travelers to disclose to a border screening officer or quarantine officer if they have "reasonable grounds" to believe they have been exposed to specific communicable diseases or have been in close proximity to a person who is likely to have a specified communicable disease.[14] Following a medical examination by a quarantine officer, a traveler may be required to comply with treatment or any other measure for preventing the introduction and spread of the communicable disease.[15] When the *Quarantine Act* was introduced in 2005 to repeal and update the previous version of the Act, the Office of the Privacy Commissioner of Canada ("OPC") generally supported its introduction, finding that the Act struck a balance between public health and privacy rights.[16]

Beyond the immediate pandemic crisis, restrictions upon privacy may linger even where the disease or disorder becomes a chronic, manageable illness that nevertheless remains potentially infectious. We see this distinctly with HIV/AIDS. Although initially nearly unmanageable and frequently deadly, HIV is becoming increasingly manageable, yet it continues to carry significant stigma and disclosure obligations. These disclosure obligations can continue even when the risk of transmission is nearly scientifically negligible but is, in the view of the law, still realistically possible. In *R v Cuerrier*, the Supreme Court of Canada ("SCC") held that failure to disclose an HIV positive status to a sexual partner is fraud, thus vitiating consent to a sexual activity and constituting aggravated assault.[17] Subsequent cases used this analysis to form the elements of aggravated assault or aggravated sexual assault.[18] Over a decade later, in *R v Mabior*, the SCC further clarified this standard when it set out that consent is vitiated if there is a "realistic possibility that HIV will

---

outbreak of a communicable disease. These orders can require individuals and groups to be placed in isolation or to place themselves under the care and treatment of a medical professional.

[12] Mark A Rothstein et al, "Quarantine and Isolation: Lessons Learned from SARS" (November 2003) at 58, online: Law, Science and Public Health Program Site <biotech.law.lsu.edu/blaw/cdc/SARS_REPORT.pdf>. http://biotech.law.lsu.edu/blaw/cdc/SARS_REPORT.pdf

[13] SC 2005, c 20 [*Quarantine Act*].

[14] *Ibid*, s 15(2).

[15] *Ibid*, s 26.

[16] Raymond D'Aoust, "Bill C-12, the *Quarantine Act*" (Ottawa: 18 November 2004), online: <https://www.priv.gc.ca/media/sp-d/2004/sp-d_041118_e.asp> (statement delivered to the House Standing Committee on Health).

[17] [1998] 2 SCR 371 at para 66, McLachlin J [*Cuerrier*]..

[18] Isabel Grant, "Prosecution of Non-disclosure of HIV in Canada: Time to Re-think *Cuerrier*" (2011) 5:1 MJLH 7 at 9, online: <mjlh.mcgill.ca/pdfs/vol5-1/mjlh_vol5-1.pdf>.

be transmitted."[19] Where the person uses a condom and has a low viral load, the realistic possibility of transmission is negated.[20]

In *Mabior*, the SCC declined to consider whether other sexually transmitted diseases would constitute "serious bodily harm" to meet the requirement for aggravated sexual assault, and stated: "where the line should be drawn with respect to diseases other than HIV is not before us."[21] However, Canadian jurisprudence has had occasion to consider whether other communicable diseases, including herpes, also carry with it a duty to disclose.[22] The trend among these cases shows that there is a duty to disclose where the behaviour about to be engaged in with another person puts that person at significant risk of serious bodily harm.

Whether non-disclosure of a communicable disease will attract penalties will depend on whether there is a statutory requirement applicable in the circumstances, or whether it is viewed to meet the standards of a criminal offense, such as for aggravated assault in "endanger[ing] the life of [a] complainant."[23] Countries such as Liberia have made it an offence to "knowingly, intentionally, or willfully" infect another person or group of persons with specified communicable diseases, which could criminalize the concealing of information by persons with communicable diseases.[24] The significance of Liberia in the Ebola crisis may give precedents to other countries to follow suit.

From these legislative provisions and case law emerges the fundamental rule that the right to privacy may only be infringed upon where the imperatives of public health are demonstrated. This has effects both at the collective level – say, in relation to quarantine measures or disclosure at the border – and at the individual level, where knowingly putting a person at risk of contracting an illness has been deemed to constitute criminal negligence and even sexual assault. In essence, the privacy interest in non-disclosure is weighed against the collective interest in disclosure. Until disclosure weighs in favour of the collective interest, the individual right to privacy must prevail.

### (B) The Notion of Consent in the Face of a Pandemic

[19] 2012 SCC 47 at paras 4, 91,104 [*Mabior*].

[20] *Ibid* at paras 94-104. In a companion case, *R v DC,* 2012 SCC 48, the SCC applied the standard in *Mabior* that a significant risk of serious bodily harm is found in the presence of a realistic possibility of transmission and is negated by both low viral load and condom protection.

[21] *Supra* note 19 at para 92.

[22] For example, in *R v JH,* 2012 ONCJ 753, the offender pled guilty to sexual assault in failing to inform the complainant that he was likely infected with HSV-2 (herpes). In this case, the disease was transmitted to the complainant.

[23] *Criminal Code*, RSC 1985, c C-46, s 268, which states: "Every one commits an aggravated assault who wounds, maims, disfigures or endangers the life of the complainant."

[24] Legisature of Liberia, News Release, "House Passes Law to Criminalize the Concealing of Information of Persons with Communicable or Contiguous Infectious Diseases" (2 October 2014), online: Legislature of Liberia <legislature.gov.lr/house/news/2014/10/house-passes-law-criminalize-concealing-information-persons-communicable-or-conti>.

The basic rule across Canada regarding personal health information is that it cannot be collected, used, or disclosed without consent, except as authorized or required by law.[25] In the face of a pandemic, where more is at stake than the individual's interests, consent becomes an issue. This begs the question regarding what the law authorizes in that context.

In *McInerney v McDonald*, the SCC reiterated that no disclosure of personal health information is allowed unless disclosure is necessary in relation to paramount public interest such as the safety of individuals or the public.[26] The parameters for applying this public interest test can be drawn from the Fair Information Principles as well as judicial interpretation of section 8 of the *Canadian Charter of Rights and Freedoms*.[27] At a minimum, they require that the collection, use, or disclosure of personal health information be subject to consent unless: (1) express consent cannot be given but can be reasonably inferred from the actions or inactions of the patient seeking medical care when the effectiveness of the care depends upon the collection,

---

[25] See e.g. the Ontario *Personal Health Information Protection Act, 2004*, SO 2004, c 3, Schedule A [Ontario *PHIPA*]. If the disclosure is made for the purpose of s 39(2) of the Ontario *HPPA*, *supra* note 11, the Ontario *PHIPA* permits health information custodians to disclose personal health information to a number of parties, including the Chief Medical Officer of Health, the Ontario Agency for Health Protection and Promotion, a medical officer for health, and a public health authority (in the same or another jurisdiction). The Ontario *PHIPA* also allows a health information custodian to disclose personal health information where permitted or required by law (s 29(3)). It also permits disclosure where the health information custodian believes on reasonable grounds that it is necessary in order to eliminate or reduce a significant risk of serious bodily harm to a person or group of persons (s 40(1)). For additional information on permitted disclosures in Ontario, see the Information and Privacy Commissioner of Ontario, "Fact Sheet: Disclosure of Information Permitted in Emergency or Other Circumstances" (Toronto: IPC, 2005), online: <www.ipc.on.ca/images/Resources/fact-07-e.pdf>. In addition, federal legislation – such as the *Privacy Act*, RSC 1985, c P-21, s 8(2)(m) – establish disclosure permissions for public interest reasons. The federal *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, s 7(3)(e) [*PIPEDA*], also establishes exceptions to consent, including where disclosure is required in an emergency that threatens the health or security of an individual, subject to written notification requirements to the person to whom the information relates. In addition, an organization may disclose to a government institution if (1) the institution has made a request for the information, (2) the institution has identified its lawful authority to obtain the information, and (3) the disclosure is requested for the purpose of administering any law of Canada or a province (*PIPEDA*, s 7(3)(c.1)(iii)). Provincial legislation such as Ontario's *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31 [*FIPPA*], and *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c M.56 [*MFIPPA*], require a head of an institution to disclose a record if there are reasonable and probable grounds to believe that it is in the public interest to do so and that the record reveals a grave environmental, health, or safety hazard to the public. Such legislation also requires the head of an institution to provide notice to the affected individual upon such disclosure (*FIPPA*, s 11; *MFIPPA*, s 5). In compelling circumstances affecting the health or safety of an individual, an institution *may* disclose personal information without consent; however, it must notify the affected individual (*FIPPA*, ss 21(1)(b), 42(h); *MFIPPA*, ss 14(b), 32(h)). In the context of pandemic scenarios, these exceptions could be invoked where the personal information is used in the public interest in order to combat the spread of a communicable disease.

[26] [1992] 2 SCR 138 at 154, citing *Halls v Mitchell*, [1928] SCR 125 at 136, where Duff J held that "reasons connected with the safety of individuals or of the public, physical or moral" would be sufficient to override a patient's right to confidentiality.

[27] *PIPEDA*, *supra* note 25, Schedule I; *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Charter]*.

use, or disclosure of the information;[28] or (2) public interest imperatives demonstrably displace individual rights to privacy.[29]

Clinical care creates a very specific context for the requirement of consent. The health services which clinical patients seek are generally necessary. They therefore generally do not have a choice about the collection, use, or disclosure required for the provision of these services.[30] While this fact may lower the requirements in relation to documenting and formalizing consent, it increases obligations in relation to safeguards and accountability as a corollary to the effectively diminished control of individuals over their personal health information. This imposes commensurate governance frameworks, safeguards, access to personal information, and recourse in relation to accuracy and protection of the information.

However, it may be more appropriate in the initial high-risk, urgent-response phase of a pandemic to regulate privacy interests by focusing on legitimate *uses* and *disclosures* of personal health information in the name of public interest rather than to focus on consent. One schematic could be to regulate uses and disclosures through the following governance framework in the initial phase:

(i) No consent would be required for direct or indirect collection if the collection was manifestly for and limited to a pandemic response;
(ii) The demonstrated need for personal health information for the initial pandemic response would need to be supported by scientific evidence if transmission routes are known, or by peer-reviewed hypotheses if transmission routes are not known; and
(iii) Any re-purposing of personal information – including for treatment in subsequent phases of the pandemic, non-pandemic research, and other purposes – would be subject to express consent unless the information was anonymized.[31] The threshold risk of re-identification would need to

[28] In *R v Dyment*, [1988] 2 SCR 417 at para 27 [*Dyment*], the SCC emphasized the sensitivity of health records and stated that "the use of a person's body without his consent to obtain information about him, invades an area of personal privacy essential to the maintenance of his human dignity." The Court found that a doctor may take blood samples from an unconscious individual where it is used for medical treatment purposes. However, the Court held that unless the law otherwise requires, the blood samples may not be provided to a third party for non-medical purposes. Accordingly, law enforcement breached the individual's privacy interest when it took the blood sample for evidence, which was an unreasonable "seizure" for the purposes of Section 8 of the *Charter*. See *Dyment* at para 31.

[29] S*upra* note 26.

[30] See e.g. Ontario *PHIPA*, *supra* note 25, s 38, which permits health information custodians to disclose personal health information to other health information custodians where (1) the disclosure is reasonably necessary for the provision of health care, (2) it is not reasonably possible to obtain the individual's consent in a timely manner, and (3) the individual has not expressly instructed the custodian not to make the disclosure. See also the Ontario *PHIPA*, s 39(d), which permits the disclosure to certain health information custodians who have previously provided health care, where the disclosure is for the purpose of improving or maintaining the quality of care the receiving custodian provides to the individual or to individuals provided with similar healthcare.

[31] The authors acknowledge that, currently, provincial health privacy legislation set out exceptions that permit health information custodians to disclose personal health information without consent for research

> be established by consensus and be commensurate to the context and the purposes for which the information would be used.

This or a similar framework would govern the ethical and lawful use of personal information in pandemic prevention or response. It would do so in a manner respectful of the individual right to privacy, yet which still serves the collective benefit of public health.

### (C) Privacy in the Scope of Information Dissemination in Pandemic Response

While the potential uses for personal health information are broad, the rule to determine permissible use is narrow. For instance, in the federal public sector, use of personal health information is permissible if such use is consistent ("compatible" in French) with the initial purpose for collection. In the private sector, the use of such information is permissible only if it is used for the purpose for which it was collected.[32] In general, these rules would entail continued recognition that personal health information cannot be used without express consent for any other use than to treat the patient, unless otherwise permitted by law. However, should the public interest in the use of information "clearly outweigh any invasion of privacy," non-consensual use would be allowed in the paramount public interest. Still, it is subject to a demonstration based on scientific evidence of the necessity for the personal health information of a specific patient.[33]

---

purposes provided specific requirements and strict conditions are met. See e.g. the Ontario *PHIPA*, supra note 25, s 44.

[32] *Privacy Act*, *supra* note 25, s 7; *PIPEDA*, *supra* note 25, s 5(3), Principle 4.5; Alberta's *Personal Information Protection Act*, SA 2003, c P-6.5, s 16; British Columbia's *Personal Information Protection Act*, SBC 2003, c 63, s 14; Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector*, CQLR c P-39.1, s 5.

[33] See e.g. *Privacy Act*, supra note 25, s 7(b). See also Ontario *PHIPA*, *supra* note 25, s 40, which permits disclosure of personal health information for public interest and public health purposes, and also permits health information custodians to disclose where they believe on reasonable grounds that disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or a group of persons. In *Canadian AIDS Society v. Ontario* (1995), 25 OR (3d) 388 (Ct J (GD)), aff'd [1996] OJ No 4184 (CA), the Court found that the mandatory reporting of HIV-positive statuses under the Ontario *HPPA* triggered *Charter* rights under ss 7 and 8. A Red Cross laboratory had tested some blood samples it had collected ten years prior and discovered that they were HIV positive. However, at the time of collection, the Red Cross did not inform the donors that their blood would be tested for the HIV virus. In the circumstances of the case, the Court found that disclosure of the statuses did not represent a violation of those rights; it accorded with the principles of fundamental justice and was reasonable, having regard to the importance given to the public health interest (at paras 131 and 158). Even if such mandatory reporting requirements violated ss 7 and 8 *Charter* rights, they would be justified under the *Oakes* test in s 1 as being rationally connected to the objective of protecting public health. While less intrusive measures were considered, the Court concluded that there were no viable options short of full compliance with the full reporting requirements. In discussing the Ontario *HPPA* as a whole, the Court stated (at para 168) that the "provisions are reasonable, and infringe rights as little as possible. As well, the effects of enforcement are not harmful in relation to the benefits of compliance with the reporting requirements of the *HPPA*" at para 168. Importantly, the Court highlighted the high mortality rates that existed at the time and emphasized the public health benefits of reporting, and noted (at paras 100, 102) that "a reporting of HIV positive status pursuant to the Acts cannot control the spread of the disease. It is

Pandemic response plans typically consist of several phases, which have different requirements for information sharing at each phase. Use of personal health information must be strictly necessary for the required public health intervention. In other words, personal health information cannot be disclosed unless for consistent use or as dictated by necessary intervention. Privacy legislation attempts to balance the individual's privacy of personal health information rights with the collective's need for disclosure and reporting by health care providers for public health or other public interest reasons. Sharing personal health information without consent is recognized as discretionary or mandatory in limited public health and public interest circumstances, particularly where the individual harm of disclosure fades before the collective harm of non-disclosure.

It follows that when the potential for a pandemic threat has not reached a level of emergency or when that threat has subsided – i.e., the least-risk phase – only population-level information is required. Therefore, where the population health risk is low, no personal information can legally be collected, used, or disclosed without consent. In other instances where only indicator-based surveillance efforts are required to monitor a potential pandemic and direct contact with a patient is unnecessary, any personal health information that is disclosed should merely be de-identified. However, where aggregate data – meaning data that is severed from identifiers and merged into one series of trends – indicates the potential for a pandemic outbreak, state authorities could then use technology that allows for re-identification of the data to make the link back to the original data. De-identified or general information – such as statistical, aggregate, and anonymous epidemiological results – does not trigger the same privacy legislation considerations, subject to ensuring that information cannot be re-identified. However, in a high-risk phase, personal health information may be needed for tracing and monitoring individuals. In these scenarios information regarding these indicators would be shared only with pre-determined responsible authorities such as hospitals and health ministries.

In Canada and the United States, legislation broadens the scope for dissemination in situations where it is required to protect the interests of public health. Canadian provincial health privacy legislation generally permits – and in some cases requires – regulated entities to report personal health information to public health authorities without consent for certain public health purposes.[34] The US *Health*

---

the counselling, education and cooperation by members of high risk groups and those infected that will have an impact on changing behavior and stemming the spread of the disease."

[34] See e.g. *supra* note 25. In light of provincial mandatory notification requirements, certain medical practitioners and laboratories – and, in some cases, institutions and school authorities – might be required to provide the relevant public health authority with information about certain reportable communicable diseases. The information required to be reported varies by province but depending on the disease may include details about the affected individual, including contacts, places visited, and more. See e.g. Ontario's *Reports*, RRO 1990, Reg 569; Alberta's *Communicable Diseases Regulation*, Alta Reg 238/1985; Prince Edward Island's *Notifiable Diseases and Conditions and Communicable Diseases Regulations*, PEI Reg EC560/1; New Brunswick's *Reporting and Diseases Regulation*, NB Reg 2009-136; Nova Scotia's *Communicable Diseases Regulation* NS Reg 196/2005; Quebec's *Minister's Regulation under the Public Health Act*, CQLR c S-2.2, r 2.

*Insurance Portability and Accountability Act* ("*HIPAA*") Privacy Rule is another legislative attempt at striking the appropriate balance between individual privacy interests and public health concerns.[35] *HIPAA*'s Privacy Rule permits certain health care providers, health plans, and health care clearinghouses – i.e., "covered entities" – to disclose personal health information to authorized public health authorities and their authorized representatives for public health surveillance, investigations, and interventions.[36] While *HIPAA* permits public health disclosures without consent of the patient, it does not require it. However, applicable US federal or state laws may require reporting of specified communicable diseases. Canadian provincial health laws also contain mandatory notification requirements with respect to certain communicable diseases.[37] In any case, where disclosure is made to public health authorities, the fundamental right to privacy, as universally recognized, dictates that only the minimum amount of personal information necessary to meet the public health need should be disclosed.[38]

The scope for dissemination broadens again where pandemic emergencies threaten to become uncontrollable. In the face of such a threat, personal health information could be shared with additional authorities such as law enforcement and customs authorities. At each point, the collection, use, and disclosure of personal information must be based on scientific evidence of necessity in order to prevent and control the pandemic spread. Here, again, concern for the collective harm of non-disclosure re-surfaces.

---

[35] 45 CFR §§ 160, 162, and 164 [*HIPAA*].

[36] *Ibid*, § 165.501 and §164.512(b)(1)(i). At the direction of a public health authority, a covered entity may also disclose protected health information to a foreign government agency that is acting in collaboration with a public health authority (§164.512(b)(1)(i)). A covered health care provider may also disclose protected health information in order to notify a person that he or she has been exposed to a communicable disease, provided that the law authorizes the covered entity to do so in order to prevent or control the spread of the disease during a public health intervention or investigation (§164.512(b)(1)(iv)). For more information on *HIPAA* in emergency situations, see generally, US Department of Health & Human Services, Office of Civil Rights, *Bulletin: HIPAA Privacy in Emergency Situations* (Washington DC: US HHS, 2014), online: <www.hhs.gov/ocr/privacy/hipaa/understanding/special/emergency/emergencysituations.pdf> [*Bulletin*].

[37] *Supra* note 34. For example, the Ontario *HPPA*, supra note 11, ss 25–28, contain requirements for various individuals – including physicians, medical practitioners, hospital administrators, superintendents of institutions, school principals, operators of laboratories, and more – to report to the local medical officer of health of the health unit instances of specific reportable and /or communicable diseases. See also *Specification of Reportable Diseases Regulation*, O Reg 559/91. The content of required reports are set out by regulation and require the reporting of personal information including name, address, sex, and other details. For example, reports related to Ebola by a physician or practitioner must also include the date of diagnosis, travel history outside Canada and places of travel within Canada in the week prior to and since onset of the illness, clinical history, and more (*Reports*, RRO 1990, Reg 569, ss 1 and 5(4)).

[38] Under *HIPAA*, when disclosing personal health information to a public health authority, covered entities may reasonably rely on the determination made by the public health authority that the minimum amount of information has been requested for the stated purpose. See *HIPAA*, *supra* note 35, §164.514(d)(3)(iii)(A). Where public health disclosures are routine or recurring, covered entities must develop standard protocols that address the types and amount of protected health information that may be disclosed for such purposes to ensure that they disclose only the minimum amount of personal information required to achieve the purpose is disclosed. See *HIPAA*, *supra* note 35, §164.514(d)(3)(i).

Where there has been a request for information about a named patient, *HIPAA* permits a hospital or other health care facility to acknowledge an individual is a patient at the facility and provide basic information about the patient's condition in general terms, subject to certain conditions.[39] The patient or their legally authorized representative must provide written authorization before the facility can make more detailed disclosures. Such disclosures include affirmative reporting to the media about an identifiable patient and about their specific treatment information, such as specific tests.[40] The disclosure of patient names and information to the media has been more prevalent in the US than in Canada. In the US, the source of the disclosure to media may originate from a non-covered *HIPAA* entity – such as a family member or friend – or through the investigative efforts of journalists.[41]

Finally, the OPC has published "best practice" guidelines for protecting privacy before, during, and after an emergency.[42] These publications provide guidance regarding how to implement privacy practices to ensure that individual's privacy is protected even during a pandemic emergency. The OPC's publications also establish standards to ensure that such protections do not pose barriers to appropriate information sharing. Sensitive information, such as personal health information, should be treated with additional precautions such as strictly limiting the purposes of its use as well as specific storage and security requirements.[43]

Before an emergency, organizations should establish information-sharing protocols that protect an individual's privacy. For instance, such protocols should require an organization disclosing information to clearly establish the reasons for seeking the information. They should ensure that the organization shares only information that relate directly to the emergency, and share only the minimum personal information data elements required for the purposes at each stage of any authorization. The protocols might also require that the shared information remain separate from the receiving organization's existing system. The protocols must also clearly establish the

---

[39] *Supra* note 35, §164.510(a). Such disclosure is only permitted where the patient has not objected to or restricted the release of this information. If the patient is incapacitated, there must be a belief that the disclosure is in the best interest of the patient and is consistent with any prior expressed preferences of the patient.

[40] *Bulletin*, *supra* note 36 at 2. While *HIPAA* remains active during a public health emergency, once a public healthy emergency is declared certain provisions may be waived, including requirements to honour a request to opt out of the facility directory or adhere to a patient's right to request privacy restrictions.

[41] See William Maruca, "Ebola in the News: Is Too Much PHI Being Revealed and by Whom?" (October 15, 2014), *HIPAA, HITECH & HIT* (blog), online: <hipaahealthlaw.foxrothschild.com/2014/10/articles/privacy/ebola-in-the-news-is-too-much-phi-being-revealed-and-by-whom/>. Maruca highlights the intense media scrutiny of certain Ebola patients in the US. It has been reported that the name of the nurse who contracted Ebola while treating a patient, which was widely reported in media, was determined by cross-referencing an address with public records and a state nursing database.

[42] Office of the Privacy Commissioner of Canada, "Privacy Emergency Kit" (Ottawa: OPC, 2013), online: <https://www.priv.gc.ca/information/pub/gd_em_201305_e.asp>. This guidance is applicable to organizations subject to federal privacy legislation, but its general principles may also be applied more broadly.

[43] *Ibid* at 6.

security of the information in transit and in storage as well as the start and end dates for the sharing. Other important privacy elements that should be addressed include access and correction rights, retention and destruction obligations, and appointing an individual responsible for addressing questions and complaints.[44]

In an emergency situation where no information protocols are established, the OPC's guidance suggests that the requesting organization should be required to explain its reasons for seeking personal information, and the information should similarly be the minimum necessary to achieve its purposes. Disclosures should be documented (e.g., personal information disclosed, when it was provided and to whom, for what purposes, the legislative authority for which it was provided). Unless otherwise required by law, an organization should notify individuals, where possible, about personal information that was disclosed for emergency purposes.[45]

### (D) Monitoring Cross-border Privacy Compliance in the Context of a Pandemic

In an interconnected global context, pandemics will have broad implications that extend beyond borders. In Canada, authority to share information across borders can emerge from Canada's international obligations and from provincial legislation. Canada is a signatory to the World Health Organization's ("WHO") International Health Regulations, which are legally binding regulations adopted by most countries to contain the rapid international spread of communicable diseases. The Regulations recognize the cross-border implications of a pandemic response and provide a framework for sharing, monitoring, and evaluating information from the sources of infections. The Regulations also require signatories to notify the WHO of events that may constitute a public health emergency of international concern according to defined criteria.[46] Additionally, certain Canadian provincial public health acts include specific acknowledgement that public health and safety may require information sharing with other jurisdictions, including internationally.[47]

---

[44] *Ibid* at 6-8.

[45] *Ibid* at 9-10.

[46] Signatories are required to notify the WHO of any event within its territory that may constitute a public health emergency of international concern, in accordance with established decision instruments. See World Health Organization, *International Health Regulations (2005)*, 2d ed (Geneva: WHO, 2005) at Article 6, online: <whqlibdoc.who.int/publications/2008/9789241580410_eng.pdf?ua=1> [*WHO IHR*]. Signatories are also required to furnish to the WHO relevant data concerning the sources of infection or contamination – including vectors and reservoirs at its point of entry – which could result in international spread of disease. In accordance with the *WHO IHR*, when a state party collects or receives personal information pursuant to the *WHO IHR* from another state party or from the WHO, the former state party is required to keep the personal information confidential and to process it anonymously as required by national law. States parties may disclose and process personal information where it is essential for the purposes of assessing and managing a public health risk, subject to certain conditions. The information should be processed in accordance with national law; it should not be further processed in excess of the purpose; it should be accurate and up to date; and it should not be retained longer than necessary. See *WHO IHR*, Articles 19, 45, and 45.2.

[47] See e.g. Quebec's *Public Health Act*, CQLR, c S-2.2., s 133; Manitoba's *Public Health Act*, CCSM, c P210, s 80.

Cross-border information sharing creates higher risks for individual privacy due to the fact that once personal health information enters another jurisdiction, it then becomes subject to the privacy laws of that jurisdiction. The jurisdiction may have certain laws – notably anti-terrorism legislation – that could override existing requirements on the recipient country regarding permissible use and disclosure.[48] If the recipient country does not have privacy protection laws – nor laws that recognize and protect human rights and/or civil liberties – it would be challenging to ensure that the information is used in a manner that meets the standards of Canada's constitutional rights.[49] Moreover, in cross-jurisdictional legal contexts, a further complication comes from the respective states' territorial sovereignty in relation to enforcement of cooperation agreements and the continued control, protection, and access to information in the other jurisdiction.[50] This greatly restricts the disclosing country's ability to control the use of information in the recipient country.

The consequences of cross-border personal health information sharing may also vary between states. In some states, such sharing can trigger significant restrictions on protected individual freedoms. A recent report by the Ontario Information Privacy Commissioner ("IPC") underscores the adverse impact that cross-border disclosure can have on Canadian citizens where sensitive information is shared with foreign government entities.

The IPC's investigation stemmed from reports that US Customs and Border Protection Officials were denying Canadians entry into the US on the basis of mental health issues. US Customs and Border Protection Officials accessed information recorded on the Canadian Police Information Centre ("CPIC") database, where police in Ontario recorded, among other things, sensitive information about attempted suicides by Ontarians.[51] In her findings, the Commissioner determined that the recording or uploading of information relating to suicide attempts or threats of suicide to CPIC is a disclosure under the *MFIPPA* and the *FIPPA*. While certain Ontario police services exercised some degree of discretion in determining whether to include such information on the CPIC, others automatically recorded such information into the

---

[48] Canada, Chief Information Officer Branch, "Guidance on Preparing Information Sharing Agreements Involving Personal Information" (Ottawa: Treasury Board of Canada Secretariat, 2010) at 2.7.3, online: <www.tbs-sct.gc.ca/atip-aiprp/isa-eer/isa-eerpr-eng.asp?format=print> [*Guidance on Preparing*].

[49] *Ibid* at 6.9.4.

[50] Institute for Citizen-Centred Service, "Government-to-Government Personal Information Sharing Agreements: Guidelines for Best Practice" at 30, online: <www.iccs-isac.org/en/pubs/Personal%20Information%20Sharing%20Agreements%20Guidelines%20for%20Best%20Practice.pdf> [*Government-to-Government*].

[51] A Memorandum of Cooperation between the RCMP and the US Federal Bureau of Investigation ("FBI") provides the FBI with access to CPIC. FBI grants access to the CPIC database to the US Department of Homeland Security, which includes US border officials. See Information and Privacy Commissioner of Ontario, "Crossing the Line: The Indiscriminate Disclosure of Attempted Suicide Information to US Border Officials via CPIC: A Special Investigation Report" (Toronto: IPC, 2014) at 2, online: <www.ipc.on.ca/images/Resources/indiscriminate_disclosure.pdf>.

database. The Commissioner considered the automatic recording to be in non-compliance with these Acts.[52]

Particularly compelling in the Commissioner's view – and highly applicable in the context of information sharing in connection with pandemics – was that sensitive mental health information was disclosed. In the context, this disclosure posed barriers to those seeking travel to the US.[53] This experience highlights the fact that where personal information or personal health information is made accessible to foreign government entities – such as in the context of communicable disease surveillance – adverse consequences can have deep impact on Canadians. Any cross-border information sharing should be scrutinized closely to ensure that the disclosure is limited and justifiable in the circumstances precisely taking into account the gravity of potential consequences.

While cross-border sharing of personal health information is essential for pandemic responses in order to trace patients and contacts, the risks and consequences discussed above show that such sharing must be framed within strict safeguards.[54]

---

[52] *Ibid* at 3. In addition to setting out other measures such as a process to seek removal of suicide or attempted suicide information on CPIC, the Commissioner established that information may be recorded in specified and limited circumstances, including where the information links more closely to potential harm. For example, the information may be recorded on CPIC where the person has a history of serious violence or where the suicide attempt involved the threat of serious violence or harm directed at other individuals.

[53] *Ibid* at 12.

[54] Although outside the scope of this paper, cross-jurisdictional sharing of information within Canada also has its challenges due to the inconsistency in the express provisions in provincial public health statutes that provide for inter-jurisdictional information-sharing. The provinces currently share information with the federal government in order to monitor infectious diseases and identify emerging health events. Since these arrangements are largely built on informal relationships with few formal agreements in place, they present the risk of having data arrangements with few detailed parameters. See Public Health Agency of Canada, *Overview of the Multi-Lateral Information Sharing Agreement (MLISA) to Support Public Health Information Sharing among Federal, Provincial and Territorial (F/P/T) Governments in Canada* (Ottawa: PHAC, 2014) at slides 4-5, online: <carpha.org/Portals/0/docs/MEETINGS/Epid_LabDir/Kroop_MLISA%20Overview_PHAC_%202014.pdf>. The provinces and federal government agreed in principle in 2009 to a memorandum of understanding ("MOU") that establishes a general framework for information sharing during a Public Health Emergency. This MOU does not contain operational details, but key elements address privacy on a general basis, including requiring that the collection, use, and disclosure of personal information – including personal health information – be carried out in the most limited manner necessary as authorized by law or an individual's consent, on a need-to-know basis, and with the highest degree of anonymity possible in the circumstances and using the least invasive means. See Pan-Canadian Public Health Network, "Federal/Provincial/Territorial Memorandum of Understanding (MOU) on the Sharing of Information During a Public Health Emergency" (Ottawa: Pan-Canadian Public Health Network, 2012) at s 5.2, online: <www.phn-rsp.ca/pubs/mou-is-pe-pr/index-eng.php>. In cooperation with the provinces and territories as well as the Public Health Network, a Multi-lateral Information Sharing Agreement has been developed to replace the MOU. This Agreement also sets out the surveillance information to be shared, its use, disclosure, and protection in the context of infectious diseases and other public health events. Its aim is to mitigate potential privacy risks by having a clear purpose for the collection, use and disclosure of information. As of 8 October 2014, British Columbia, Nova Scotia, Nunavut, the Northwest Territories, and the Public Health Agency of Canada have signed the agreement. See Nova Scotia, News Release, "Province to Sign Information Sharing Agreement" (8 October 2014), online: Government of Nova Scotia <novascotia.ca/news/release/?id=20141008003>.

Information sharing agreements ("ISAs") should be in place to impose limitations upon use and disclosure of personal health information as well as obligations of safeguarding, retention rules, access, and remedies for breaches. Key guidance on developing information sharing agreements include Canada's Treasury Board Secretariat's *Guidance on Preparing Information Sharing Agreements Involving Personal Information* and the *Public Sector CIO Council's Government-to-Government Personal Information Sharing Agreements Guidelines for Best Practice*.[55] Although these guidance materials focus on ISAs generally as well as in specified circumstances, they highlight that ISAs cover sensitive data in the exchange of personal health information and that such information must receive the proportionate level of protection.[56]

Principles set out in the ISA guidance documents are particularly important when contemplating a pandemic response. For example, personal information should only be shared where there is legal authority and a clearly justifiable need for a specified and current period of time, and it should be shared only in the most limited manner possible and with the highest degree of anonymity possible.[57] Legislation may also apply. For instance, the *Quarantine Act* permits the sharing of information with other states in certain circumstances, and it specifically allows personal information obtained under the Act to be shared with foreign governments where the Minister has reasonable grounds to believe that the disclosure is necessary to prevent the spread of a communicable disease or to enable Canada to fulfill its international obligations.[58] The Act further states that the individual to whom the information relates must be notified of the disclosure.[59]

A key component of an ISA will be the inclusion of specific security measures that safeguard sensitive personal health information and should include "high standards for privacy and security, including encryption, secure storage, retention schedules, and requirements for secure disposal of personal information."[60]

---

[55] *Guidance on Preparing*, *supra* note 48; *Government-to-Government*, *supra* note 50. *Guidance on Preparing* is intended to be consulted by institutions subject to the federal *Privacy Act*, *supra* note 25. *Government-to-Government* sets out six "best practices" which form the life-cycle of the decision-making process for ISAs between governments within Canada: (1) identify and determine risk factors; (2) explore alternative strategies; (3) conduct risk assessments; (4) document the ISA decision; (5) create an ISA; and (6) monitor and follow-up on ISA effectiveness.

[56] *Ibid* at 15.

[57] *Ibid* at 12.

[58] *Supra* note 13, s 56. Personal information obtained under the Act may be disclosed to other government agencies and health organizations, whether domestic or foreign, if the Minister has reasonable grounds to believe that the disclosure is necessary to prevent the spread of a communicable disease or to enable Canada to fulfill its international obligations.

[59] *Ibid*, s 56(3).

[60] See Information and Privacy Commissioner of British Columbia, *Investigation Report F10-02 Review of the Electronic Health Information System at Vancouver Coastal Health Authority Known as the Primary Access Regional Information System ("PARIS")* (Victoria: Office of the Information and Privacy Commissioner for British Columbia, 2010) at para 120 (addressing personal health information sharing by a public body).

The sending organization should "push" the information to the recipient organization in the other jurisdiction in the manner and times provided for in the agreement, since the alternative of having the other party "pull" the information would require giving them broad access to a database.[61] The ISAs should also include robust prohibitions on secondary use and disclosure. Such prohibitions should consider any applicable access and other privacy laws that could apply in the recipient jurisdiction, and should additionally establish a consultation procedure for such circumstances.[62] In the context of cross-border transfers, the receiving jurisdiction's laws – including applicable anti-terrorism laws – may determine the enforceability of clauses that restrict the purposes for which information can be used. Accordingly, ISAs should include protective clauses to address this.[63] The guidance document also suggests additional requirements such as segregating shared data from its records or notifying when the information is disclosed under foreign law.

Accordingly, while cross-border information sharing is necessary when faced with the threat of a pandemic emergency, cross-border sharing presents unique risks to individual privacy. Once information is shared with another jurisdiction, it becomes subject to the laws of that jurisdiction respecting the collection, use, and disclosure of personal health information, and the disclosing jurisdiction can do little to ensure compliance with its privacy standards. In turn, cross-border information sharing must be framed within strict safeguards such as ISAs.

### (E) Safeguards in the Context of Multi-Sectorial Information Sharing on Vulnerable Platforms

In relation to privacy, protective pandemic intervention would integrate both specific and generic safeguards. Safeguards should specifically ensure that patient data are de-identified unless identification is demonstrably necessary, and that no personal information be collected, used, or shared if non-personal information meets public health needs. Such data-minimization efforts must be supported by either destruction or segregation of identifying data, along with clear data linkage rules and a separately held patient linkage index (i.e., central repository assigning meaningless numbers to records in an anonymized manner). In broad strokes, the governance framework would be built on three main categories of data:

(i) Anonymized data, which is data completely severed from identifiers in a manner that would make re-identification so arduous to be remote. This data could be used and shared without the restrictions of privacy protection since the privacy interest has been practically eliminated.
(ii) Pseudonymized data, which is data where the real identifiers have been replaced by artificial identifiers, such as a bar code, to protect privacy but

[61] *Government-to-Government*, *supra* note 50 at 16.

[62] *Guidance on Preparing*, *supra* note 48 at 6.5.

[63] *Government-to-Government*, *supra* note 50 at 30. See also *Guidance on Preparing*, *supra* note 48 at 6.9.3.

also allow tracking back to the original identifiers when identification becomes necessary. Rules must be developed in each case to state when tracing back to the original data may be justified and how the pseudonymized data must be held to ensure there is no re-identification other than as allowed.

(iii) Identifiable data, which, of course, means data that contains identifiers. This data receives full protection of privacy law.

In addition to the governance framework, de-identification methods must be further developed and must properly balance private and public interests.[64] Limiting access to de-identified personal health information and ensuring that data-sharing agreements are in place can reduce the risks of re-identification.[65] A retention schedule would ensure the timely destruction of personal health information and of de-identified or aggregate information is done as soon as it is no longer relevant.

Specific technological and administrative safeguards must also be developed. Technological safeguards should be calibrated by threat and risk assessments in order to protect sensitive personal health information. These safeguards must be in place prior to the adoption of new technology and must integrate commensurate protection into technological infrastructure.[66] Moreover, the staff who use this technology must also be digitally literate. Administrative safeguards – such as clear privacy practices supported by training and appropriate disciplinary measures – must also be in place.

It is established that general safeguards must reflect the sensitivity of personal health information and the high level of trust that the patient places in the health system. The importance of each factor calls for commensurate protective measures. The

---

[64] For example, under the Ontario *PHIPA*, supra note 25, s 4(1)–(2), "personal health information" is defined as "identifying information" that "identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual." Under the US *HIPAA*, supra note 35, § 165.514(a), de-identified information is not personal health information and therefore is not protected by the Privacy Rule. See generally US Department of Health & Human Services, "Guidelines Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule" (Washington, DC: US Department of Health & Human Service, 2010), online: <www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance .html>. For a discussion on risk-management approaches to de-identification of personal health information, see Khaled El Emam, "De-identifying Health Data for Secondary Use: A Framework" (22 October 2008), online: Electronic Health Information Laboratory <www.ehealthinformation.ca/wp-content/uploads/2014/07/2008-A-framework.pdf>.

[65] Information and Privacy Commissioner of Ontario, "Looking Forward: De-identification Developments: New Tools, New Challenges", by Ann Cavoukian (Toronto: IPC, May 2013) at 12, online: <www.privacybydesign.ca/content/uploads/2013/05/de-identifcation-developments.pdf>.

[66] See e.g. Communications Security Establishment & Royal Canadian Mounted Police, *Harmonized Threat and Risk Assessment (TRA) Methodology*, TRA-1 (Ottawa: CSE, 23 October 2007); eHealth Ontario, "Guide to Information Security for the HealthCare Sector" (Toronto: eHealth Ontario, 2010), online: eHealth Ontario <www.ehealthontario.on.ca/images/uploads/pages/documents/InfoSecGuide _Complex.pdf>. In the US, *HIPAA*'s Security Management Process requires organizations to "implement policies and procedures to prevent, detect, contain, and correct security violations" and to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity". See *HIPAA*, *supra* note 35, §164.308(a)(1).

implementation of such general safeguards rests upon a robust and clear governance framework that ensures privacy impact assessments for any measure that has privacy implications, and an accountability framework to ensure compliance.

## 4. Moving Forward: Respecting Data Minimization and Achieving Data Optimization in Pandemic Response

The ethical dilemma at the heart of this discussion relates to balancing between two factors: namely, the individual harms of disclosure and stigmatization, on the one hand, and the collective harm of non-disclosure, on the other. In the background, many believe that data analytics – including analytics regarding personal information – should be allowed to advance scientific knowledge of pandemic diseases. Indeed, treasures of scientifically relevant information should not lie unused or be destroyed if they can be used in a privacy-protective manner.

This dilemma calls for both legal and technological solutions. Legally, the challenge calls for a framework moving from a static notion of personal information to a dynamic notion that takes into account how the collection, use, and disclosure of information would impact the individual. A static notion of personal information is rigid in the sense that personal information is described in law and governed by clear rules, without full consideration of context embedded in its application. A dynamic notion, on the other hand, is founded in human rights law, balancing individual rights and collective rights. The optimization of data requires this balancing in order to allow an effective response to pandemics. This would not preclude refining the framework for regulating "uses" and "disclosures" in certain phases of pandemics, while entrenching the concept of "consent" for non-critical phases of pandemic responses. An ethical and pragmatic governance framework would allow or prohibit use of personal information according to the demonstrable cost and benefit of its disclosure. This notion would take into account the essential considerations that must guide the protection of privacy through a pandemic.

Technologically, we should continue to investigate with greater urgency anonymization or de-identification techniques that prevent identification in cases where identity is not necessary, but which allow for the use of the connecting information where it is necessary.[67] In particular, we must develop a richer understanding of anonymization and de-identification as a risk-based inquiry rather than as a binary analysis of what is personal (and therefore protected) and what is not personal (and therefore available). .

The objective is to arrive at a privacy protection framework for pandemic prevention and response that that serves both individual privacy interests and

[67] Information and Privacy Commissioner of Ontario & Electronic Health Information, University of Ottawa, "De-identification Protocols: Essential for Protecting Privacy", by Ann Cavoukian and Khaled El Emam (Toronto: IPC, June 2014), online: <www.privacybydesign.ca/content/uploads/2014/06/pbd-de-identifcation_essential.pdf>.

collective interests in public health. In summary, this framework must be of international scope and contain:

(i) A specific set of rules for collection, use, and disclosure of personal information in the context of the imperatives of preventing and responding to pandemics;
(ii) Regimes for the management and safeguard of anonymized, pseudonymized, and identifiable data;
(iii) Definitions of individual rights and obligations in the context of pandemics, in relation to consent, access, and duty to disclose personal health information in the public interest; and
(iv) Monitoring mechanisms to ensure the compliance of all states concerned.

This framework is essential to regulate the use of personal health information in the international context of pandemic prevention and response. The framework must balance individual and collective rights. In relation to individual rights, a specific set of rules must clearly define the circumstances in which a duty to disclose would apply and the circumstances that would require meaningful consent. In relation to collective rights, the dissemination of information, which is key to coordinate response and manage outbreak, must be unambiguously allowed where necessary, but must also be explicitly prohibited to the extent that the disclosure is not justified by exacting scientific standards. This international framework would support pandemic response by governing all states involved in relation to common norms and mechanisms. In this way, the individual harms of personal health information disclosure may be balanced against the collective harms of non-disclosure and we ensure the greater good, in full respect of individual rights.