

Contents lists available at ScienceDirect

### Heliyon

journal homepage: www.cell.com/heliyon



Research article

# Creating standards for Canadian health data protection during health emergency – An analysis of privacy regulations and laws



Jawahitha Sarabdeen <sup>a,\*</sup>, Emna Chikhaoui <sup>b</sup>, Mohamed Mazahir Mohamed Ishak <sup>c</sup>

- <sup>a</sup> College of Law, Prince Sultan University, Riyadh, Saudi Arabia
- <sup>b</sup> Compliance Office, Prince Sultan University, Riyadh, Saudi Arabia
- <sup>c</sup> JS Law Firm, Pickering, ON, Canada

### ARTICLE INFO

### Keywords: Health data Law Protection Limitation Standards

#### ABSTRACT

Health emergencies require unprecedented measures to protect the public from the health disaster. Such measures may require limiting the exercise of personal freedom and other rights like the right to data privacy. The limitation, however, should be temporary and proportionate so that privacy rights are not compromised superfluously. In this aspect, the European Union (EU) implemented better data protection measures and guided the government and various entities on the acceptable ways of handling data during a pandemic, though the measures taken were not very comprehensive. Canadian privacy laws in general are sector driven and not harmonised at the national level and there is no new guidance on the usage of data during emergencies. Hence, this research will analyse laws and regulation in EU and Canada with a view to understanding the necessity of amending privacy laws in Canada to make it relevant, up-to-date and in compliance with EU data protection requirements so data sharing from EU countries could be made easy. It further encapsulates appropriate standards for Canada health data protection for better management of health data privacy.

### 1. Introduction

Collection, use and misuse of personal data are always an important concern to individuals (Singer, 2020; Sarabdeen and Moonesar, 2018; Van Slyke et al., 2006) worried about the insecure storage of data including sensitive information and accidental or intentional errors and disclosures. Governments are being accused of neglecting appropriate safeguards in collecting sensitive data or not investing enough to safeguard those data (Van Slyke et al., 2006). With the collection of massive health data during COVID 19, individuals and privacy advocates have become apprehensive of improper handling of health data, unauthorized access, and transfer of data beyond national boundaries. In Canada, for instance, if someone is tested positive for COVID-19, the data related to infected individuals are collected and the concerned individual and all people who have been in contact with the infected person are notified and advised/instructed to go into self-quarantine to break the chain of infection. In this respect, the health departments in Canada collect and analyse data of infection and implement appropriate measures to contain the spread of the virus. Canada may also share health and travel related data if the infected individuals and the people in contact with them crossed the borders (Canada.ca, 2019).

In controlling the current health emergency, databases of infected individuals are created to contain the spread of the disease. However, such database could potentially expose sensitive data to others if there is lack of appropriate organisational and legislative measures to protect personal data (Van Kolfschooten and De Ruijter, 2020). Additionally, the employment of emerging technologies like artificial intelligence (AI), machine learning, robotic and big data for better data analysis and projections could be a cause of concern. For instance, to maximize the use of AI, huge data input is required. In the current pandemic situation, though collecting of health data in large quantity for analysis and its use are unavoidable, it is expected that reasonable safeguards and standards should be implemented so that a minimum level of protection of health data could be guaranteed.

The delicate interplay between data protection on the one hand, and the protection of public health on the other, presents several challenges. During a crisis like COVID-19, striking a balance between private right to health data privacy and public right to data usage is critical. COVID 19 allowed some of the data controllers (organisations) to coordinate data sharing on a more universal, sustainable, and accountable basis for public good and well-being following a stewardship approach. The stewardship approach facilitates a fiduciary level of responsibility toward the data

<sup>\*</sup> Corresponding author.

E-mail address: jsarabdeen@psu.edu.sa (J. Sarabdeen).

and shares it for public good (The Information Accountability Foundation, 2018). In such an approach, data can benefit the stakeholders beyond the original purpose for which data were collected. Data stewardships consider all parties and use data to create maximum benefits without compromising the rights of individuals and other parties.

This approach is said to be equivalent to corporate social responsibility that encompasses the economic, legal, and ethical expectations. The organizations have a corporate data responsibility regarding the data they collect, create, transfer, and disclose (The Information Accountability Foundation, 2018). These responsibilities form the basis for data stewardship and predominantly depend on values or principles, policies, culture, and technological controls of the organisation. Accountability and responsibility are important elements in the stewardship, and they are the foundation of the General Data Protection Regulation (GDPR), too.

However, the COVID-19 containment initiatives and the possibility of continuous collection of data create concern among Canadians like any other country as some speculate that the governments may be planning to collect and retain the data for longer than required for future unjustifiable surveillance. Even if data may be anonymized, there might be a possibility to link back to the original owner of the data, therefore concerns about government surveillance can not be avoided or contained. For instance, the United Kingdom has planned to retain the data it collects for up to 20 years and the individual right to delete the data may be denied (Murphy et al., 2020). Though the Canadian government has not announced any broader surveillance so far, the ease of collection, use and storage of health data may continue if they are needed for public health emergencies. Hence, analysis of health data privacy laws are needed to enact appropriate and timely standards so that data subjects, collectors, and users will minimise violation to health data privacy (Gerke et al., 2020). The privacy and data protection laws are sector-driven and non-harmonised in Canada. According to the federal system of government, there are different privacy laws for private and public sectors with differing obligations (Bernier and Knoppers, 2020). Thus, the main research question is: can the current data protection regime in Canada ensure data protection of individuals during emergencies like COVID-19?

The objective of the article is to discuss the data protection regime in European Union and Canada and suggest legislative amendment to the Canadian privacy laws. Besides being the leader in providing privacy regulations the EU privacy regulations have cross border implications to other countries including Canada. The relevant EU regulations, decisions and guidelines will be assessed to suggest modifications to the Canadian privacy laws so that the privacy laws in Canada will be applicable, current, and comprehensive. The research will also provide recommendations regarding data protection standards for Canada that could be followed by all those who handle health data during crisis or emergencies like COVID-19. The standards will include data principles and measures in balancing the individual's health data while safeguarding public health.

### 2. Methodology

The research focused on the privacy laws and regulations in Canada that protect health data privacy and drew a comparison with the laws in European Union as they are the pioneers in providing comprehensive data privacy regulation. The comparison will help to suggest recommendations on amendment of privacy law in Canada and its standard in handling health data during emergencies. For the purpose of achieving the research objective, the research analysed the Charter of Fundamental Rights of European Union (CFREU) and the General Data Protection Regulation (EU) 2016/679 (GDPR) to look into the detailed rules on general data protection. The EU Clinical Trial Regulation (Regulation EU No 536/2014), the Toolbox for contact tracing, warning apps (e Health Network, 2020) and the Guidelines regarding acceptable way of processing of data during crisis were also analysed to understand the handling of sensitive data during emergency. Analysis of the CFREU,

GDPR, other related regulations, decisions and guidelines may show the comprehensive nature of data privacy law in EU and the extent of amendment needed to the Canadian Law. The purview of the research also included an analysis on the Canadian federal laws of Privacy (Privacy Act of 1983, the Personal Information Protection and Electronic Documents Act (PIPEDA) 2000) and the provincial laws, with a view to investigating the availability of law to address health data protection in cases of emergency in Canada. The researchers used comparative and content analysis to address the research question. The EU data protection regulations, guidelines, decisions, and the Canadian federal and provincial legislation were considered as primary sources while all other literature on the subject matter were considered as secondary sources. In collecting primary and secondary sources for analysis, the researchers reviewed government websites and research articles from well-known databases. After collecting available literature, laws and regulations on the topic, the researchers extracted, mapped, and reviewed 56 articles, laws, and regulations that were relevant. The information derived was further analysed to suggest appropriate recommendation. This was achieved by developing relevant keywords and phrases like "health data protection", "EU health data regulations", "health data during COVID 19" "standards of data privacy" "Canadian privacy laws", "pandemic measures" "health regulation" and "health data sharing in Canada" in all possible combinations.

### 3. Analysis

### 3.1. Health data protection in the European Union during pandemics

This section analyses the EU regulations, decisions, and guidelines so that appropriate suggestions could be proposed to amend Canadian privacy laws. The Charter of Fundamental Rights of European Union (CFREU) and the General Data Protection Regulation (GDPR) are the major players that regulate privacy protection at the EU level (Watson and Rodrigues, 2018).

The CFREU alludes to the protection of personal data. Article 8(1) states that everyone has the right to the protection of personal data while 8(2) specifically mentions that the data processing shall be conducted fairly for specified purposes. It should be based on consent, or some other legitimate basis laid down by law. It also elaborates that the data subject has the right to access his data, and the right to have it rectified. However, the right to data protection shall be subjected to the control of an independent authority. The GDPR sets out the right and limitation to protection of personal data. According to the GDPR, the principles of data protection should apply to any information concerning an identified or identifiable natural person. It prohibits the processing of special categories of personal data, such as data concerning health and genetic unless certain safeguards are ensured (Article 9(1)).

During pandemics, Articles 9(2) (c), (g) (i) and (j) along with Recital 46, 53, 54, are crucial provisions concerning health data protection. The Recitals are referred in the research as it helps to explain the GDPR provisions though it is not supplementary to GDPR, and the European courts have often relied on the Recitals in interpreting the regulations. Recital 46 states that the health and sensitive data could be lawfully processed for the purpose of vital interest addressed in Article 6 (1) (d). The Recital covers the use of data for protecting someone's life as vital interest and its application is limited to the matters of life and death (Gratton, 2018). However, one cannot use this Recital if protection of life is possible through other less intrusive means. The Recital could possibly be used in emergency care, though it may not be applicable in planned medical care. Article 9(2) also speaks on vital interest, and that data could be used to protect someone's vital interests i.e. necessary for survival. However, the scope of Article 6 (1) (d) and Recital 46 is broader than Article 9(2) (c). Recital 46 allows the processing of health data on humanitarian grounds such as monitoring epidemics, or where there is a natural or man-made disaster causing a humanitarian emergency (Ico.or.uk (n.d.)). Hence, the vital interest excerpt could be utilised if it is demonstrated that the use of health data is for the purpose of vital interest (Ico.or.uk (n.d.)). As a general rule, Article 6 (1) (a) and Article 9 (2) (a) of GDPR require explicit consent for the use and collection of medical data from the data subject as right to personal data could be a fundamental right to physical integrity and human dignity (Van Kolfschooten, 2019, Mariner, 2007). Explicit consent under Article 4(11) of GDPR requires consent be given freely and is specific, informed, and unambiguous (edpb.europa.eu, 2020). Thus, the data subjects must be given adequate information about data processing to allow for an autonomous decision. Explicit consent would indicate that the data subject is voluntarily consenting to disclose personal information while understanding the consequences of their decision (Van Kolfschooten, 2019). However, in some circumstances as elaborated in other provisions of Articles 6 and 9, there are certain alternatives for processing medical data without consent (Jelinek, 2020a, b).

During a pandemic, for instance, to prevent the spread of disease and protect life, Article 9(2) (c), (g), (i) and Recital 46 can possibly be applied without consent. Article 9(2) (i) of GDPR applies to the processing of sensitive data, without the explicit consent of an individual for public interest and public health purposes. Similarly, Recital 53 also allows processing of sensitive health-related data to benefit individuals and the public for the purpose of quality control, managing information and health security, monitoring, alerting, etc. Recital 54 also allows the processing of sensitive data without consent for public interest in the context of public health. The processing should be for public interest only and once the data are processed, they cannot be shared with third parties like insurance companies or employers. The Article and Recitals allow for collection and use of data necessary to study or fight epidemics or to plan a vaccination program. The Recitals clearly allow EU member countries to impose additional processing of sensitive data so that the rights and freedoms of data subjects could be protected. Accordingly, the UK Data Protection Act 2018 in Schedule 1 mentions that processing data in the area of public health shall be carried out under the responsibility of a health professional or another person who owes a duty of confidentiality under enactment or rule of law. In Regulation (EC) No. 1338/2008, public health is explained to include all elements related to health care, health care expenditure, financing, and the causes of mortality.

Article 9(2) (j) allows scientific research during a pandemic or any other related research. However, it requires compliance with Article 89(1) of GDPR even if Articles 6(1) (d), (e) and (f) allow the use of data without consent for the performance of a task that is considered as vital or necessary for public interest or that processing is for the purposes of legitimate interests pursued by the data controller or by a third party. Article 89 requires various safeguards of technical and organisational measures to be placed before processing the data for scientific purpose so that the principle of data minimisation can be ensured. Recital 156 of the GDPR also emphasizes the technical and organisational measures to ensure data minimisation, proportionality, and necessity. Furthermore, when large scales of data collection are carried out by the public authority for research purposes, the exercise could be challenged against GDPR. Such a challenge may require an analysis of robust measures taken and the risk of interference. Section 64 of the UK Digital Economy Act (DEA) 2017 could be considered in meeting the requirements imposed by GDPR (Bell et al., 2019). Though UK exited from the EU, the law passed to meet the requirement of GDPR while UK was still a member country could be relevant in the context of application or interpretation of GDPR requirements by member countries. Section 64 of the DEA requires certain conditions to be met before processing personal data for scientific research and imposes penalties for misuse. Under section 64 of DEA, the information to be used for scientific research should be de-identified information (if the data subject identifies an individual); the processing should be undertaken by the public authority or another body; the person processing data shall take reasonable steps to avoid the accidental or deliberate disclosure of identifiable information; the research purpose must be disclosed by public authority; the research purposes, the processor and the researcher must be accredited by the UK Statistics

Authority Board and each person who processes or discloses the information has to have regard for the Code of Practice published by the UK Statistics Authority Board under Section 70.

Another regulation on research and clinical trial is the EU Clinical Trial Regulation (CTR) (Regulation EU No 536/2014). The main purpose of this Regulation is to have a harmonised rule in relation to clinical trials across EU member countries. CTR as a sectoral law has specific data protection provisions apart from the GDPR. However, CTR in Article 93 mentions that GDPR is applicable in clinical trials. CTR also mentions that processing of health data could be for two distinct purposes and application of data protection principles will differ according to the purpose for which the data is processed. If the collection and use of data are related to reliability and safety of medical products, the CTR and relevant national provisions will regulate the data collection as mentioned in Article 6(1) (c) of GDPR. If the purpose of collection is for research purposes, the activities may either fall under the data subject's explicit consent (Article 6(1) (a) and Article 9(2) (a)) or may fall under public interest (Article 6(1) (e)) exception in conjunction with Article 9(2), (i) or (j) of the GDPR or the legitimate interests of the controller (Article 6(1) (f) and Article 9(2) (j) of GDPR). According to EDPB, a careful assessment of the circumstances of the clinical trial will dictate if consent is necessary or it falls under exceptions (Jelinek, 2019).

During emergencies, CTR allows the researchers in clinical trial to use patients' data and obtain consent at a later period as explained under article 35 of CTR. Critically ill patients or patients whose consent may not be able to obtain during clinical trial can be subjected to clinical trial without getting their consent. Though it has provision for proxy consent, this method of post clinical trial consent could only be used if proxy consent could not be obtained. However, there are no clear guidelines or strategies available on how post clinical trial consent can be obtained. It is to be noted that obtaining informed consent is only an additional safeguard and not the legal basis for processing data. If the processing falls under the public interest under Article 6(1) (e) of the GDPR or the legitimate interest pursued in Article 6(1) (f) of the GDPR, consent could be exempted. Though CTR mentions data processing during emergency situations, what constitutes an "emergency situation" is not explained under Article 35 of CTR.

Besides the GDPR and EU Clinical Trial Regulation, the EU issues other Guidelines and Decisions that are helpful during pandemics. Health Threats Decisions 1082/2013/EU on serious cross-border threats to health was adopted in 2013 as a legislation by the European Parliament and Council (De Ruijter, 2017) and it was intended to support cooperation and coordination between EU member states in the field of serious health threats (Article 1(2)). According to the Decisions, ministers of all the member countries and the EU Commission need to consult the Health Security Committee (HSC) regarding the exchange of information on policy, technical matters, and strategies in relation to cross-boarder health security (Scholz, 2020). The approach taken in the Health Threat Decisions is said to be a good example of the securitization of public health in the EU as it connects EU public health and security policy (Purnhagen et al., 2020). In the context of securitization of public health, the Decisions provides guidelines on using health data for health emergency while safeguarding personal data. It also requires the implementation of appropriate technical and organizational measures to protect personal data (Van Kolfschooten and De Ruijter, 2020; De Ruijter, 2017). For personal data to be shared under the Decisions, it is necessary to establish that data is available, it is in the authority's possession, and that the data may be useful for coordinating the response to a health threat (Decision 1082/2013/EU, Article 9(3)). The Decisions imposes a minimum retention period where it states that personal data are to be automatically removed from the systems after twelve months (Dabrowska-Kłosińska, 2017). It should be noted that the Health Threats Decisions and GDPR are distinct regulations, and the storage requirement is also different. The Decisions is only applicable on data that are collected on serious cross-border threats to health while GDPR has general application on data protection.

However, it failed to specify the proportionality in data collection, use, sharing and retention. It further failed in differentiating various health threats and method of informing the concerned individuals (Van Kolfschooten and De Ruijter, 2020). It could be argued that the new surveillance countermeasures taken to control the COVID-19 pandemic, that allow sharing of health data with EU member states, have the potential to interfere with the right to privacy. The counter measures requirement gives the EU member states power to determine a proportional balance of data protection. However, the approach could be justifiable as it could fall under Articles 6 and 9 of derogation of GDPR. Similarly, the exit screening questionnaire at borders and sharing of confirmed COVID-19 cases for tracing of contacts and sharing of personal information for disease control measures with the World Health Organization (WHO) and third countries could come under the derogation provision of GDPR. The derogations could be applicable even if the patient may not have consented to the sharing of information with other countries or WHO and even, may not have understood the effect of consent and the scope of the data processes.

The European Commission has further published a Toolbox for contact tracing and warning apps (eHealth Network, 2020). The Toolbox states that the contact tracing and warning apps should be fully compliant with the EU data protection and privacy rules, and the apps should be installed voluntarily. It further suggests that data processing by the latest non-invasive privacy-enhancing technological solutions should consider ways to protect personal data and use anonymized data. Though the Toolbox addresses the issues related to contact tracing and warning apps, the provisions could be applied to health monitoring activities and technologies. The Toolbox emphasizes privacy while considering public need for personal data on account of contact tracing. However, what constitutes as 'appreciable balance' in restricting right to data privacy is not elaborated in the Toolbox (Van Kolfschooten and De Ruijter, 2020).

To assist in handling of data protection and data management, the European Data Protection Authority (DPA) most recently published a Guideline regarding the acceptable way of processing data during crisis. The Guideline is said to be pragmatic and coherent in Europe and the world at large. The Guideline helps to charter the crisis without neglecting core data protection principles mentioned in Article 5 of the GDPR. Under the Guideline, data including health data can be processed without consent, if the process is justifiable under public interest particularly in public health, scientific research, or statistical purposes. Though contact tracing needs voluntary adoption, subsequent processing does not require consent. Nonetheless, the European Data Protection Board has advocated implementing core seven GDPR data processing principles mentioned in Article 5, like purpose limitation, data minimization and storage limitation to ensure less intrusion into data protection (Data Protection Board, 2020 and Flamant, 2020). The Guideline has left balancing of public interest and private right to organisations, who are expected to implement appropriate technical and organisational measures. The organisation collecting and processing data including health data should satisfy Articles 10 and 33 of the Regulation where data security of the process shall be ensured following the application of adequate measures. The appropriate technical and organisational measures should include providing access only on a need-to-know-basis, implementing accountability like introducing passwords, and maintaining secure storage. Not to mention, the measures implemented should be audited regularly (European Data Protection Supervisor, 2021).

The analysis of EU regulations along with other health related decisions and guidelines show that the EU has placed some relevant laws and guidelines to help decision makers during pandemics. The GDPR allows health and sensitive data to be lawfully processed for the purpose of vital interest and public health during emergencies, provided appropriate safeguards are in place. Additionally, the EU Clinical Trial Regulation (Regulation EU No 536/2014) regulates clinical trials (European Commission, 2014). Though expressed consent is the requirement for researchers in clinical trial to use patients' data in normal circumstances, the derogations of GDPR allow health data to be used without consent

and obtain consent at a later period. Threat Decisions 1082/2013/EU, 2013 on serious cross-border threats to health, considered public health as part of public safety issue and allowed border control to monitor people's movement for health surveillance. Similarly, Toolbox addresses the issues related to contact tracing and warning apps that could be applied to monitor activities of data subjects and their movement. All the above mentioned measures taken by the EU show that they are better prepared to address health data protection during emergencies like the COVID-19 pandemic, while striking a balance between public interest and private right to data privacy. For instance, the organisation collecting and processing data including health data should satisfy Articles 10 and 33 of the GDPR where data security of the process shall be ensured following the application of the adequate measures in using health data. Conversely, Canada has followed previous EU Data Protection Regulation and the current law in Canada lacks comprehensiveness and is sector driven. In addition, there are no guidelines or directives that provide instructions on balancing public and private rights to data during an emergency.

### 3.2. Data protection and restrictions in Canada

Across the Atlantic in Canada, privacy and data protection laws follow the previous EU Data Protection Directive where privacy laws are sectordriven and non-harmonised. The main theme of this section is to show that Canadian privacy law at this current fragmented state may not be equipped to address an emergency like COVID-19.

There are different privacy laws for private and public sectors with differing obligations. In 1990s many provinces enacted the Freedom of Information and Protection of Privacy Act (FIPPA) to regulate data processing in the public sector. At the federal level, the Privacy Act 1983 regulates personal information regarding collection, use and disclosure by the Government of Canada and it provides protection for identifiable individuals. Additionally, Personal Information Protection and Electronic Documents Act (PIPEDA), 2000 federal law applies to business organizations that are engaged in commercial activities, regardless of their location of business or clients. If the provincial governments enact substantially similar law to PIPEDA to regulate the private sector, then the provincial law will be applied to the private commercial organizations and not the federal laws. Otherwise, PIPEDA regulates commercial organizations that collects, uses, or discloses personal information, including personal health information within a province. PIPEDA would also apply to health care providers who are funded through the public health insurance system. Though PIPEDA does not apply to public hospitals as the core activities are not commercial; non-core activities, such as a pharmacy carrying on a commercial organisation in a hospital space could be subjected to PIPEDA. Quebec, British Columbia, and Alberta have provincial privacy laws substantially similar to PIPEDA and therefore PIPEDA will not be applied in those provinces on private sector commercial activities that occur within the territorial boundaries of the province (Bernier, A & Noppers, M.B., 2020). However, PIPEDA remains applicable in relation to data transfer in cross provincial or national borders. In terms of public sector regulations on privacy, besides the federal laws, each province has passed their privacy law. Ontario, for instance, passed Freedom of Information and Protection of Privacy Act (FIPPA), 1990 and the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), 1990. In regulating the public health records held by public institutions such as hospitals and health boards, the provincial law will be applicable in Ontario.

The sector-driven, federal and provincial laws create some tension in the protection of data privacy regarding interprovincial and international transfer of use of personal data for which the data were collected. There are differences in legislative requirements among the provinces concerning reuse of data for purposes other than the original purpose. The privacy laws differ considerably from one province to the next, and the applicable law varies depending on whether data are used within the borders of a province or interprovincial. Similarly, PIPEDA requires the

J. Sarabdeen et al. Heliyon 8 (2022) e09458

data collectors to collect the data for identified purposes. Therefore, it will be burdensome and risky to use the data for secondary purpose like research if it was not disclosed at the time of data collection. The other issue with differential provincial requirements is retaining the data for longer periods than what is legislatively mandated. Health data related to communicable diseases may require data to be retained for a longer period so that the experts will be able to understand the pattern, nature, and other related information of a particular disease. Though the regulators signaled in favour of providing leeway to have extended retention period and transfer of data for research purposes, there is no legislative measures in this regard (Council of Canadian Academies, 2015). In the absence of legislative amendments, the collection of excessive data to maximise the data pool or retaining the data for longer period may go against the data principles under both federal and provincial laws as there is ambiguity to the allowable duration of storage. Significant variation in privacy laws and data access policies in Canada could cause problems for a comprehensive electronic healthcare record systems that are dependent on various sectoral and jurisdictional flow of personal health care information (Kirby Report, 2002).

As a general rule, the existing federal and some of the provincial laws require explicit consent for collection and processing of data including health data, though alternatives are available. Similarly, PIPEDA in section 6 states that knowledge and consent are necessary requirements for processing of personal information except where the data processing falls within the derogation of Section 7(1). However, industry Canada and the Federal Privacy Commissioner have indicated that in the case of circle of care, implied consent is acceptable under PIPEDA. As health care becomes increasingly specialized and collaborative, a wide range of health care providers may be involved in providing care and the data needs to be shared among them. This range of care providers are called circle of care (Ries, 2006). When technologies are used by the data collectors like hospitals and other organisations, obtaining explicit consent would be a challenge as the data are processed without human factor. Thus, appropriate notice to data subjects in a meaningful, clear, and timely manner is imperative to remain compliant with the privacy laws. During pandemics or any health emergencies, public education may require sharing of aggregated or anonymized information with the public and the data could also be used for public policy purposes (Courage, N., and Branch, A., 2020). Many organisations have employed AI to process large volumes of health data for data analysis and interpretation. Though the sharing of health data during health emergency could fall within the limited exception mentioned under section 7(1) of PEIPDA and the corresponding provincial legislation, there is no guidance available so far on the extent of use and safeguard measures taken to balance public right to data and privacy right of individual.

At the provincial level, Manitoba's Personal Health Information Act 1997 regulates health information, in public and private sector entities, and clearly sets rules for collection, use and disclosure of personal health information. Generally, the Act requires individual consent for processing health data, however, it authorizes trustees (like health care providers of data) to disclose personal health information without consent. A trustee is also allowed to share data with a third party in providing care to the data subject. Like Manitoba, Saskatchewan passed the Health Information Protection Act 1999, and it requires express or implied consent for processing of personal information. Under the statute, implied consent is acceptable for providing care to a patient. The provincial government set up the Saskatchewan Health Information Network (SHIN) to facilitate compilation of personal health information from trustees. At the outset of the Health Information Protection Act 1999, individuals were given the right to object to storage of their specified information on the SHIN. This provision was amended and individual right for objection for storage was removed and consent requirement was also amended (Ries,

Ontario passed the Personal Health Information Protection Act 2004, and it applies to health care providers and facilities who process health related data. The legislation specifies, inter alia, the requirement for

collection, the safeguards against data abuses, and the measures to provide data integrity. The Act also imposes consent requirements as one of the requirements for processing, though it provides for exceptions to privacy like other provincial legislation. It also includes the rights of individuals and the responsibility of their care provider. Alberta's Health Information Act, 2001 regulates health information processing by government departments, health authorities, health care practitioners and all health care providers. The initial version of the statute required consent for disclosure of data. However, the provincial government removed this provision.

Currently, the consent requirement was removed from Alberta's and Saskatchewan's health information privacy laws. However, to have better health care system, sharing of health information requires a coordinated action across the country and amendments by federal and other provincial governments for protecting privacy, while not impeding delivery of care. The Office of the Privacy Commissioner of Canada (OPC) in its annual report to Parliament in 2017 suggested amendments to the Privacy Act on consent requirements along with PIPEDA. The OPC is suggesting Parliament to introduce new exceptions to consent that have societal benefits subject to strict conditions and stronger enforcement. It also suggested to allow pseudonymized information that exempt the need for consent requirements but is still subject to all the other PIPEDA protections. The OPC mentioned that besides the possible legislative amendments, it will also prepare guidelines on big data, artificial intelligence, and robotics use in relation to data protection, among others (OPC, 2017). Similar to the PIPEDA and Privacy Act 1983 proposed amendments, all provincial legislation should also consider amendment to harmonise the law on data protection so that interprovincial transfers could be regulated easily.

In addition, the federal and provincial legislation resemble the old data protection regulation of the EU, thus the amendments could assist them in having compatible laws like EU members and facilitate easy data transfers from EU member countries. For instance, the definition of personal information in PIPEDA and provincial legislation requires amendment so that inference about individuals' personal information using technologies like AI, big data and robotics is included within the definition. This amendment is an important step in protecting personal data as most inferences about an individual are drawn without knowledge or consent of the individuals and that the usage of the inference affects the interests of those individuals, unless the processing of data is justifiable. Considering technology advancement, the right to a meaningful explanation and right to contest should be added so that the concerned individuals whose interests are affected would be able to protect their rights or understand the logic behind the decision. Though the definition of personal data is technology neutral under the Canadian legislation, adding the right to openness will give a chance to the data subject to understand the underlying reasons for the machine-based decision.

The GDPR regarding storage clearly states that the data should be stored for limited period, and that cannot be kept for longer than needed and the data should be kept up to date. Consequently, any apps or systems that are processing data should be accurate and up to date even in case of emergency situations. Possibility of error is potentially high during emergency as many protocols might have been compromised that could lead to wrong diagnoses, medication and may even cause fatal accidents. Although what is reasonable time is not explained in GDPR, the data collector should be able to justify the timescale that they have put in place. However, in three situations, data can be kept for an indefinite period: archiving purposes in the public interest; scientific or historical research purposes; or statistical purposes (5(1) (e)). The regulation also talks about integrity and confidentiality and accountability of data in (5(1) (f). The data collector is responsible for keeping the information systems secure and that the security measures should permit, detect, and respond to security incidents. It also requires that the data collector should review and make appropriate modification to security policies, practices, and procedures on a regular basis as a

reasonable safeguard against loss, unauthorized use, access, modification, disclosure, and other misuses. Amendments to Canadian legislations to reflect storage requirement, due to ambiguity regarding whether data could be stored for limited or long-term period and the exceptions to Article 5, would assist the usage of health data during health emergencies and could encourage scientific research.

There is no provision under the current law for collection of excessive data or retaining of the data. There are also no provisions to regulate technology usage in processing of health data for analysis and interpretation. An introduction of further provisions like Articles 6, 9 and 89 will facilitate the scientific research using de-identified large scale health data. Right to explanation is adopted in Article 15(1) (h) of the GDPR which is linked to openness, access and accuracy and allows individuals to understand the nature, element and principal characteristics of the decisions and inferences about them. Article 22(3) of the GDPR introduced right to contest so that risk of algorithmic discrimination or other unfair treatment could be reduced or eliminated. The right to contest is distinct from right to withdraw consent. Such rights should be added to PIPEDA as well as provincial legislation. The right to explanation and contestation necessitates the organizations to keep log and trace the collection and use of personal information so that complex processing involved in AI and other technologies are documented. Any inspectors or investigators could understand the personal information that have been processed by technological means. It also helps to ensure broader legal compliance relating to data protection.

The Canadian government has taken a major step to amend PIPEDA. It introduced the Bill C-11 in the House of Commons in late 2020 to amend the existing law so that the data protection law in Canada can be comprehensive and current (Scassa, T., 2019). If the Bill is passed, it will create the Consumer Privacy Protection Act (CPPA) and the Personal Information and Data Protection Tribunal Act (PIDPTA). The amendments are not only expected to boost data privacy but also create deterrence against data breaches as violators could be penalized with a hefty fine of \$10 million and class actions for damages. The Bill proposes more liberty to the data subjects to control their personal information. It requires the organisation to provide privacy in plain and clear language under mandatory privacy management programs. In addition to correcting and supplementing with correct data, the new Bill also introduces a right to portability of data from an organisation to another within the "data mobility framework." It also provides right to request for the disposal of personal information which the organisation needs to comply with, unless it can show that disposal will affect another individual's data, or law requires the retention of the data or contractual terms does not allow disposal (Karn, B., 2020). Before the proposed Bill, the 10 fair information principles were enshrined under Schedule 1 of PIPEDA and are implicit in Alberta, British Columbia and Quebec's respective laws. Based on fair information principles, the organizations are expected to establish privacy management for handling and protecting the personal information of individuals (OPC, 2012). The current Bill, however, formalised the requirement of privacy management program with added responsibilities.

Under the proposed Bill, the Privacy Commissioner is given greater oversight and enforcement powers. The bar on requirement of consent was also raised, consent should be expressed not implied. Implied consent is only justifiable if it is shown by the data collector that collection of data is within reasonable expectation of data subjects and the data falls within low sensitive data. To receive informed consent, the organisation collecting information is required to provide details of the purpose, the description of data, and its usage in addition to possible consequences. If the organisation is working with a third party, it must disclose the name of the third party. Nonetheless, the exception of "legitimate interest" will allow the organisation to collect daily business-related information without express consent.

The creation of Personal Information and Data Protection Tribunal (the "Tribunal") under the Bill, will be an important element in the proposed amendment. The Tribunal will hear appeals from decisions made

by the Privacy Commissioner of Canada (the "Commissioner"). It will function informally and expeditiously in accordance with fairness and natural justice without following the rules of evidence. The Tribunal is also vested with power to impose various penalties up to \$10,000,000. The new amendment will give way for the data subject to claim damages for use and misuse of personal data if such use caused injury or loss (Buffett PLC Inc., 2021).

Within Canada, Ontario amended the *Personal Health Information Protection Act, 2004* (PHIPA) and introduced through *Bill 188, the Economic and Fiscal Update Act, 2020.* The amendment intended to give individuals the right to access personal records in different forms. The access also covers data in electronic format and introduced the right to data portability. Contravening this provision would warrant administrative and financial penalties (section 61). Ontario is moving towards the requirement of keeping electronic audit logs. Personal Health Information Protection Act 2004 amendments mandate the maintenance of an electronic audit log of electronic personal health information (Fabiano and MacRae, 2020). This information needs to be shared with the Ontario Information and Privacy Commissioner if the Commissioner requests so.

The existing data protection or privacy legislation of few provinces have been amended to introduce more alternatives to the consent requirement, and a proposal for amendment to PIPEDA is underway. The regulators should introduce provisions in clarifying the storage period and introducing rights like right to a meaningful explanation and right to contest so that the Canadian privacy law can stand out to address the challenging technology driven environment. The legislative changes could harmonize federal and provincial laws so that any hindrance in terms of interprovincial transfer of data including the health or sensitive data to facilitate research or commerce could be made easy. Additionally, such amendment will also assist in meeting the requirement of the EU data protection regulation (GDPR) on receiving data from EU member countries. The GDPR has stringent requirements in transferring data to a third country which does not have compatible law or agreement as mentioned under A.46 of the GDPR.

The analysis of this section shows that the Canadian privacy law in its current form is fragmented and incomprehensive to address emergencies efficiently. The federal government and many provincial governments are taking initiatives to amend the law to suit the changing and challenging environment and address data protection issues in a comprehensive manner. Further, the amendments to the existing law will bring it in par with GDPR, considered as one of the comprehensive legislations in terms of data protection, as EU requires compatible law for data transfer from EU member countries to a third country. A uniform privacy law across Canadian provinces will improve efficiency in handling privacy issues, and that could increase public trust on privacy and data handling. All the provinces could work together to minimize the differences in their laws and work on having similar privacy laws. This will help to address privacy concerns and pave ways for central data management repositories that could be overseen by designated privacy commissioners. Central data management will prevent the replication of data processing procedures and could expedite handling of data for research, testing, and vaccine development. The central data management initiatives should be audited by the Privacy Commissioners of all the provinces and the federal Privacy Commissioner on a regular basis. Mobilizing accurate, adequate, and relevant data through central data management system across various provinces and beyond will ensure equitable access to scientific research and findings (Bernier and Knoppers, 2020).

## 4. Suggestions on creating standards for health data protection in Canada

By considering the GDPR and other literature on data protection and privacy, the following should be considered by data collectors or organisations to establish appropriate standards for health data protection during pandemics and beyond so that the data subjects could be assured appropriate level of data protection while waiting for the updating of existing laws in Canada.

Where possible, the data subjects should be informed of the collection of data and the purpose of data collection. Nonetheless, the authorities may opt not to inform the data subject of collection, use or retention of data if they think that such a disclosure will affect the national security, health, or other justifiable purposes (ass v. Germany, 1978). In such a case, applying proportionality should be the mantra and excessive governmental or organisational intrusion and improper use of personal information should be avoided where feasible. The data collection measure for national health, security and other related purposes should be temporary until the public health situation is alleviated and when the need for the data ceases, the data collection also is expected to cease.

The current EU Guideline regarding privacy comes within the exception mentioned in Articles 6 and 9 of the GDPR. According to the EU Guideline, it is preferable to follow the data protection principles where appropriate even if the data processing falls within the exceptions. Complying with the data principles could allow to build community trust on the governmental and organisational measures. Similarly, the COVID-19 outbreak initiatives published by the Office of the Canadian Privacy Commissioner indicated that the derogating of data protection law in federal and provincial level legislation could be used in case of emergency and all the relevant parties could conduct a coordinated afford to address current health emergency situations. In this context, British Columbia temporarily rescinded its data localization requirements. However, there is no guideline issued by the Privacy Commissioner, as such the health service provider only has to resort to the provisions of the existing federal and state privacy legislation in addressing the unprecedented emergency cases like COVID-19 (OPC, 2020, Murphy et al. 2020 and Eck and Hatz, 2020).

The retention period may vary depending on the circumstances; the EU Health Threat Decision provides for 12 months retention period. The retention period should be reasonable, and the organisation should justify the retention of data beyond the specified period. Retention periods should be proportionate to the type of personal data and their usefulness (Segerstedt-Wiberg and Others v. Sweden, 2006). This will help to decide the appropriate retention period based on objective criteria (Digital Rights Ireland, 2014).

The data controller or processer whenever possible, should place emphasis on transparency and take steps to inform about the processing of data. The disclosure should include the usage of their data in simple, clear language. The data controller or processer should provide identity, contact details of the organisation, purposes of the processing, recipients of such data, information regarding international transfers of the data, period for which the data will be stored, and information on further processing. The data must be sufficiently protected both technically against cyber risk and organizationally against unauthorized sharing (Mikkelsen et al., 2020). In processing data for secondary purposes such as scientific research, appropriate security measures should be imposed so that the data is not used for non compatibility purposes. The security measures should only allow access to individuals who are trained on confidentiality. The organisation should create an accountability measure with regards to data access and the data should be encrypted. It is recommended that a full data life cycle analysis is to be mandated so that weak spots and operational risks could be identified (European Data Protection Supervisor, 2021). Attention should be given to true anonymization and pseudonymization to control the risk to data subjects (Taranto et al., 2020).

There should be different retention period based on categories of data and it should be dependent on the specific health threat. For proportional implementation of contact tracing, it must be ensured that health data is not processed for purposes other than the specific health threat and is only shared through the selective communication channel. An opportunity should be created to have a meaningful explanation and contest the processing of information or the output of data (Fabiano and MacRae, 2020). There is a need to appoint a data-privacy leader in the

organization's COVID-19 response team to ensure early evaluation and discussion of possible measures affecting data privacy (Mikkelsen et al., 2020).

The data subjects should be given opportunity to inspect, rectify, delete the stored personal data in all the member countries where the data, including sensitive data are kept and this will promote some sense of control (Ducato, 2020; Rotaru v. Romania, 2000). Creation of data hubs like COVID-19 Open Research Data set (CORD-19) of Allen Institute of AI and MiPasa of World Health Organization, facilitates collection of health-related data, analysis of data through software to control spread of the disease, expatiates the vaccine and vaccine related research. Health related data can also be integrated with location and other datasets to understand the spread of the disease. When Canadian health data is being shared with the data hub, various parties involved in these hubs need to be regulated through contractual terms so that the research should not hinder beneficial use of the data hub. They may use block chain technology to facilitate different licenses to support collaboration among different participants and meet the legal requirement in the absence of appropriate law in the country where data hubs are located.

The guidance by the European Data Protection Board (EDPB) on data transfer measures involving third country whose data protection laws are not compatible with EU level of data protection, could be an assistance in dealing with data transfer from Canada to other countries. According to the Guidelines, the organisations that use standard contractual clauses ("SCCs"), or other transfer tools under Article 46 GDPR to transfer data, are required to put in place additional safeguards in the SCCs. The data exporters are expected to take appropriate steps as supplementary measures to close the gap in data protection in the third country as follows:

- a. The organisation exporting personal data to a third country needs to know the transferee and keep a written record. The record should include onward transfers if further transfers to any other third country are involved.
- b. Identifying appropriate transfer tools that an organisation relies on is necessary. If there is a need for supplementary measures to protect data in a third country where data are being transferred, the supplementary measure should show that the processing of the data needs to be clear, precise, and accessible. The measures are proportionate to the purpose, and objective of the transfer. Proportionate measures should have independent oversight and it should also have effective remedies.
- c. The supplementary measures may be technical (e.g.encryption), organisational (e.g. adoption of policies and best practices) or contractual in nature (e.g. report data access requests).
- d. All the necessary procedural steps should be set so that supplementary measures could be implemented.
- e. Ongoing evaluation should be done as part of accountability so that
  the exporters can update any regulator developments that could
  impact data transfer requirements (Paulley and Kim, 2020).

The countries involved in sharing data could create an executive structure to coordinate emergency responses. They can draw measures and implement balanced policies so that a resilient system could be created as they work collectively for a greater good (Renda and Castro, 2020).

### 5. Conclusion

Though providing protection for data is an arduous task for various parties collecting, storing, and using data including health data, appropriate protection for health data is necessary since health data is a lifetime history of every patient. Various studies have suggested that with the adoption of technology in healthcare, the public concern for misuse of health data is high since it could be easily collected and used or misused without their consent (Van Kolfschooten, 2019). The public loss of confidence in data protection is even greater in a crisis where the

J. Sarabdeen et al. Heliyon 8 (2022) e09458

government establishes health data bank for broad reuse for approved purposes that could override the requirement of subsequent consent to collect, use, or disclose data for public wellbeing. However, the success of the implementation measures to utilise health and other sensitive data depends on the availability of balancing of public interest to use the data and private right to protect the same data.

The analysis of health data protection regulations and guidelines in EU and the data privacy laws in Canada shows that the EU regulations and guidelines are current and relevant as compared to Canada. The Canadian laws lack comprehensiveness, and they are not up to date to address issues of crisis management and technology development. While the Canadian public and organisations are waiting for updated laws after introduction of Bill C-11 in the Parliament, data collectors, or controllers (organisations) should take initiatives to adopt standards to ensure compliance to data principles and to honor the data subjects' rights where practicable. Amendment to provincial legislation will also allow to streamline the law in relation to handling of data that could greatly benefit various stakeholders. The standards the researchers discussed have incorporated principles of accountability, minimization, proportionality, and necessity following the literature, stewardship/corporate governance concept, and will guide all the stakeholders including the data subjects in the protection of health data privacy.

### **Declarations**

### Author contribution statement

Dr. Jawahitha Sarabdeen:Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Wrote the paper.

Dr. Emna Chikhaoui & Mohamed Mazahir Mohamed Ishak; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data

### Funding statement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

### Data availability statement

Data will be made available on request.

### Declaration of interests statement

The authors declare no conflict of interest.

### Additional information

No additional information is available for this paper.

### Acknowledgements

The authors would like to acknowledge all the support provided by Prince Sultan University (PSU) and Governance and Policy Design Research Lab, PSU.

### References

- Bell, J., Aidinlis, S., Smith, H., Mourby, M., Gowans, H., Wallace, S.E., Kaye, J., 2019.
  Balancing data subjects' rights and public interest research. Eur. Data Protect. Law Rev. (EDPL) 5 (1), 43–53.
- Bernier, A., Knoppers, M.B., 2020. Pandemics, privacy, and public health research. Can. J. Public Health 111, 457, 457.
- Canada.ca, 2019. Coronavirus Disease (COVID-19): Canada's Response. Available at:  ${\tt https://www.canada.ca/en/public-health}$ 
  - /services/diseases/2019-novel-coronavirus-infection/canadas-reponse.html#ta.

Council of Canadian Academics, 2015. Accessing Health and Health-Related Data in Canada, Ottawa, Canada. Available at: https://www.researchgate.net/publication/274920946\_Accessing\_Health\_and\_Health-related\_Data\_in\_Canada.

- Dąbrowska-Kłosińska, P., 2017. Tracing individuals under the EU regime on serious, cross-border health threats: an appraisal of the system of personal data protection Eur. J. Risk Regul. 8 (4), 700–722.
- De Ruijter, A., 2017. Mixing EU security and public health in the health threats decision.
  In: de Ruijter, A., Weimer, M. (Eds.), EU Risk Regulation, Expert and Executive
  Power. Hart Publishing, pp. 101–120.
- Digital Rights Ireland Ltd v Minister for Communications. Marine and natural resources and others and kärntner landesregierung and others. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293.
- Ducato, R., 2020. Data protection, scientific research, and the role of information. Comput. Law Secur. Rep. 37, 1–16.
- Eck, K., Hatz, S., 2020. State surveillance and the COVID-19 crisis. J. Hum. Right. 19 (5), 603–612.
- eHealth Network, 2020. Mobile Applications to Support Contact Tracing in the EU's Fight against COVID-19 Common EU Toolbox for Member States Version. Available at: https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-19 apps en.pdf.
- European Data Protection Supervisor, 2021. EDPS Orientations on Manual Contact
  Tracing by EU Institutions in the Context of the COVID-19 Crisis, pp. 1–10. Available
  at. https://edps.europa.eu/system/files/2021-02/21-02 02\_orientations\_on\_manual\_
  contact\_tracing\_euis\_en\_0.pdf.
- Fabiano, D., MacRae, S., 2020. Significant changes to ontario's health privacy law: new enforcement powers and technology requirements. Health/Priv. Cybersec. Bull. Available at: https://www.mondaq.com/canada/privacy-protection/917894/signific ant-changes-to-ontario39s-health-privacy-law-new-enforcement-powers-and-techno logy-requirements.
- Flamant, J., 2020. Regulatory privacy guidance for a pandemic the story so far in COVID-19 Exit Strategy. In: A Global Privacy and Cybersecurity Guide. Hogan Lovells. USA.
- Gerke, S., Shachar, C., Chai, P.R., 2020. Regulatory, safety, and privacy concerns of home monitoring technologies during COVID-19. Nat. Med. 26, 1176–1182.
- Gratton, L.-P., 2018. Article 9. Processing of special categories of personal data. Available at. https://gdpr-text.com/read/article-9/#comment\_gdpr-a-09\_2i.
- Ico.or.uk (n.d.). Vital interest. In: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/vital-interests/.
- Jelinek, A., 2020a. Guidelines 05/2020 on Consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020. Available at: https://edpb.europa.eu/sites/ default/files/files/file1/edpb guidelines 202005 consent en. pdf.
- Jelinek, A., 2020b. Guidelines 03/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the COVID-19 Outbreak. Available at. https://edpb.europa.eu/sites/default/files/files/file1/edpb\_guidelines\_ 202003 healthdatascientificresearchcovid19\_en.pdf.
- Jelinek, A., 2019. Opinion 3/2019 Concerning the Questions and Answers on the Interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR) (art. 70.1.b)). Available at: https://edpb.europa.eu/ sites/default/files/files/file1/edpb\_opinionctrq\_a\_final\_en.pdf.
- Mariner, W., 2007. Medicine and public health: crossing legal boundaries. J. Health Care Law Pol. 10, 121.
- Mikkelsen, D., Soller, H., Strandell-Jansson, M., 2020. Privacy, Security and Public Health in a Pandemic Year available at: https://www.mckinsey.com/business-functions/risk/our-insigh
  - ts/privacy-security-and-public-health-in-a-pandemic-year#
- Murphy, S., Sabbagh, D., Hern, A., 2020. Piloted in May, Ditched in June: the Failure of England's Covid-19 App. The Guardian, UK.
- OPC, 2012. Getting Accountability Right with a Privacy Management Program. Available at: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl\_acc\_201204/.
- OPC, 2017. 16-17 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act. Available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar\_in dex/201617/ar\_201617/#heading-0-0-3-1.
- Paulley, S.J., Kim, K.H.A., 2020. Why the Guidance on International Transfer of Data Post Schrems II Doesn't Offer as Much Comfort as We'd Hoped. Available at: https://www .mondaq.com/canada/privacy-protection/1016664/why-the-guidance-on-internatio nal-transfer-of-data-post-schrems-ii-doesn39t-offer-as-much-comfort-as-we39d-ho ned.
- Purnhagen, P.K., De Ruijter, A., Flear, L.M., Hervey, K.T., Herwig, A., 2020. More competences than you knew? The web of health competence for European union action in response to the COVID-19 outbreak. Eur. J. Risk Regul. 11 (2), 297–306.
- Renda, A., Castro, R., 2020. Towards stronger EU governance of health threats after the COVID-19 pandemic. Eur. J. Risk Regul. 11, 273–282.
- Kirby Report, 2002. Caada standing senate committee on social affairs, science and technology, the health of Canadians. In: Recommendations for Reform, Ottawa: Standing Senate Committee on Social Affairs, Science and Technology, 6. Available at: www.hc-sc.gc/ca/hcs-sss/com/kirby/index\_e.hlml.
- Ries, M., 2006. Patient privacy in a wired (and wireless) world: approaches to consent in the context of electronic health records. Alberta Law Rev. Available at: https://canlii. ca/t/2d5f retrieved on 2022-01-11.
- Rotaru v. Romania, 2000. ECHR, 4 May.
- Sarabdeen, J., Moonesar, A.I., 2018. Privacy protection laws and public perception of data privacy: the case of Dubai e-health care services. Benchmark Int. J. 25 (6), 1883–1902.

- Scholz, N., 2020. Cross-border Threats to Health EU Action on Preparedness and Response. Available at:h
  - ttps://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646123/EPRS\_BRI(2020)646123\_EN.pdf
- Segerstedt-Wiberg and ors v Sweden, 2007. Merits and just satisfaction, App no 62332/00, ECHR 2006-VII. In: 44 EHRR 2, IHRL 3288 (ECHR 2006), 6th June 2006, European Court of Human Rights [ECHR].
- Singer, W., 2020. Balancing Public Health and Data Privacy: where Does COVID-19 Meet Cybersecurity? Available at: https://www.forbes.com/sites/startupnationcent ral/people/wendysinger1/?sh=9b3c7e121441.
- Taranto, L., De Ampuero, S., Navarro, P., Wenzel, A., 2020. Key privacy considerations for COVID-19clinical trials. In: COVID-19 Exit Strategy. A Global Privacy and Cybersecurity Guide. Hogan Lovells, USA.
- The Charter of Fundamental Rights of European Union (CFREU), 2012. The General Data Protection Regulation (GDPR), 2018.
- The Information Accountability Foundation, 2018. Evolving Accountability to Ethical Data Stewardship A Key Part of Wave Four Privacy Laws. Available at: https://informationaccountability.org/2018/10/evolving-accountability-to-ethical-data-stewardship-a-key-part-of-wave-four-privacy-laws/.
- Van Kolfschooten, H., 2019. EU coordination of serious cross-border threats to health: the implications for protection of informed consent in national pandemic policies. Eur. J. Risk Regul. 10, 635–651.
- Van Kolfschooten, H., De Ruijter, A., 2020. EU data protection laws and health data COVID-19 and privacy in the European union: a legal perspective on contact tracing. Contemp. Secur. Pol. 41 (3), 478–491.
- Van Slyke, C., Shim, J., Johnson, R., Jiang, J., 2006. Concern for information privacy and online consumer purchasing. J. Assoc. Inf. Syst. Online 7 (6), 415–444.
- Watson, H., Rodrigues, R., 2018. Considerations for the use of social media in crisis management. J. Contingencies Crisis Manag. 26 (1), 89–98.