A Legal Framework for Healthcare: Personal Data Protection for Health Law in Turkey

Veli Durmuş, Mert Uydacı

Marmara University Healthcare Management Department, Istanbul, Turkey

ABSTRACT

Personal Health Data are generated at every encounter between an individual and health-care providers: doctors, hospitals, pharmacies, laboratories, and home-care providers. Data protection refers to the set of privacy-motivated laws, policies and procedures that aim to minimise intrusion into respondents' privacy caused by the collection, storage and dissemination of personal data. The Regulation on Processing and Ensuring Privacy of Personal Health Data (dated 2016) is an instrument that allows protecting privacy for health-related data in Turkey. This article aims to provide a holistic general overview of the data protection regime in Turkey. Furthermore, this paper presents the principle rights of data protection and transmission in health law and latent ethical concerns by specifying decisions of Supreme Court in Turkey and European Court of Human Rights on using personal data. The research is descriptive on data protection law for healthcare setting in Turkey. Primary as well as secondary data has been used for the study. The primary data includes the information collected with current national and international regulations or law. Secondary data include publications, books, journals, empirical legal studies. Privacy and data protection regimes in health law shows there are some obligations, principles and procedures which shall be binding upon natural or legal persons who process health related personal data. A comparative approach presents there are significant differences in some EU member states due to different legal competencies, policies, and cultural factors.

Keywords: Personal Data, Health Data, Data Protection, Data Privacy, Healthcare, Health Law

1. INTRODUCTION

Every patient who needs to get a medical treatment should share health related personal data with healthcare providers. Therefore, personal health data plays an important role to make health decisions and identify health threats during every encounter between a patient and caregivers. In other words, health data can be defined as privacy and sensitive information which is protected by various health laws and regulations. In many cases, the data are an outcome of the confidential relationship between patients and their health care providers.

Health data usually consist of individual, personal health and other related information. The European Group on Ethics in Science and New Technologies (EGE), in the Opinion No 13 Ethical Issues of Health Care in Information Society defines "health data" as including "a wide range of information about an individual, which all touch upon an individual's private life (OECD, 2015).

Globally, almost all nations have own laws, regulations or rules in order to protect personal health data. Several countries state that difficulties negotiating data sharing arrangements among public authorities. Especially, legal regulations and a lack of interagency co-operation limits data sharing among public authorities in Turkey. In the same way, Norway, which has the strongest health information system with the greatest data availability, do not permit Ministry of Health to share data with any other legal entity. (OECD, 2015).

There is a variety of instruments that allow authorities to use the health data or to set the barriers data sharing across international borders. In Turkey, for example, the protection of personal data mainly depends on "the Law on Personal Data Protection". This legislation numbered 6698 published at the Official Gazette dated April 7, 2016 has entered into force at the date of its publication. On the other hand, the General Data Protection Regulation (GDPR), however, came into force on April 27, 2016 in EU after 6698 numbered law in Turkey. Law on personal data in Turkey, hence, is largely based on the EU Data Protection Directive (Directive 95/46/EC) instead of GDPR (Akıncı, 2017). GDPR adresses the protection of fundamental rights and

freedoms of natural persons and in particular their right to the protection of personal data. Similarly, the Law on Personal Data Protection Law (LPDP) presents set forth obligations, principles and procedures for privacy of personal data such as health related data.

In fact, a law on the protection of personal data was a step taken towards harmonising the Turkish legislation with EU legislation. The Data Protection Law was prepared based on Directive 95/46/EC on data protection. The Data Protection law is very similar to EU Data Protection Directive, however, it is not entirely same and the differences in the Data Protection Law are deficiencies rather than improvements.

This study deals with general aspects of the Personal Data Protection for Health Law in terms of the principle rights of data protection and transmission in health law and latent ethical concerns by specifying decisions of Supreme Court in Turkey and the European Court of Human Rights. Turkey has been linked to the European Court of Human Rights by Association Agreement since 1990. This research, therefore, not only focus mainly on data protection regulations for healthcare setting at national and international level, but it also provides how the protection of personal data for health care is implemented and experienced by health employees in the light of Supreme Court decisions in Turkey and the European Court of Human Rights decisions.

2. BACKGROUND OF THE STUDY

Health systems must focus on improvements in care quality and co-ordination; and efficient care delivery and on finding new ways to make systems more productive and sustainable. The need to more actively manage health system outcomes will drive health systems toward greater use of clinical and administrative data to assess the comparative effectiveness of therapies and services. These data will also be needed to support re-designing and evaluating new models of health care service delivery and to contribute to the discovery and evaluation of new treatments.

While all countries are investing in health data infrastructure, there are significant cross-country differences in data availability and use, with some countries standing out with significant progress and innovative practices enabling privacy-protective data use; and others falling behind with insufficient data and restrictions that limit access to and use of data, even by government itself. Countries that develop a data governance framework that enables privacy-protective data use will not only have the information needed to promote quality, efficiency and performance in their health systems, they will become a more attractive centre for medical research and will have opportunities to build public-private partnerships (OECD, 2015).

It is no doubt that every health related data is highly related to research on health outcomes for providing some factors that affect the live of community and a big picture on health care system in public. Despite of all these benefits, working with the health data on which the research is based can be challenging. Some challenges are technical, such as the use of different standards in different jurisdictions to record important data. Others are related to privacy concerns: access to health data for research carries the risk that personal data could be released, whether inadvertently or intentionally. To deal with the data flow, organizations are increasingly formalizing their data management and use practices. This results from legal requirements, recognition of the importance of public trust, and opportunities to improve service through the effective use of data.

To support improving health data and privacy governance frameworks, health ministry and policy makers in Turkey making decisions on health data governance including the development and use of personal health data and the legal frameworks, policies and practices that are in place to protect the privacy of data subjects when data are being processed and analysed. In this perspective, examining the current situation from different points of view can help to define legal framework of personal health data by stating what is the main purpose of law on data protection and how to deal with complicated issues on personal health data in Turkey.

3. OBJECTIVES OF THE STUDY

This study has tried to present the principle rights of data protection and transmission in health law and ethical concerns by specifying decisions of Supreme Court in Turkey and European Court of Human Rights on using personal data. In short, it has been tried to respond to the following questions in the study:

- What is known about health related data from various sources and across jurisdictions?
- What are the ethical, legal, and social concern of access to data?
- What are the benefits and challenges to access to health data for public and jurisdiction?

4. SIGNIFICANCE OF THE STUDY

As part of Turkey's accession process to the European Union, enactment of specific legislation relating to the protection of health data is an important step in this road. While European Union's data protection regulations date as far back as to 1995, Turkey enacted the "the Law on the Protection of Personal Data" and the "Regulation on Processing and Ensuring Privacy of Personal Health Data" in 2016. Although the data protection regime in Turkey has been governed by other legislation such as the Turkish Criminal Code, the Turkish Civil Code, the Banking Law as well as the Labour Law, the general framework of the health data protection and processing regime shall be governed by the Regulation on Processing and Ensuring Privacy of Personal Health Data as well as the Turkish Law on the Protection of Personal Data.

At international level, countries begin to address effective practices in the protection of privacy in the use of personal health data to facilitate the mechanisms of supporting privacy-protective data use. In this regard, this study is new, which draw a legal framework to strengthen the essential elements of the health data protection and to assist developing strong legislative reform in Turkey under the international health data practices such as the European Data Protection Directive (95-46-EC) and EU Data Protection Regulation.

5. ACCESSING HEALTH DATA: BENEFITS, RISKS, AND BARRIERS

Health data allows researchers to get a more complete picture of the disparate factors that contribute to the physical and mental health of a population. Moreover, by enabling researchers to access larger samples, population-wide health and health-related data enable the study of rare events such as rare diseases or rare adverse reactions to treatments (Jutte et al., 2011).

During the digitalization of critical health data, electronic health records became one of the hot topics in medical informatics. In addition, proliferation of new monitoring and health-care instruments have led to dramatic growth in individual-level data on factors that affect individual health, social well-being, and the provision of health care.

Although routinely collected health data has been used for health research and system innovation for decades, the rapidly expanding scope of electronic data provides new opportunities. These data enable the study of serious diseases, comparison of incidence rate or measure of overall potantial factors on well-being. Research using these data can improve health outcomes and patient safety, better inform a range of health and social policies, enable beneficial innovations, reduce health-care practices of little or no benefit, and slow the growth in health-care costs (Roos et al., 2008; Lewis, 2011).

Beside benefits of accessing health data, in allowing the use of these data, one risk is that private information will be revealed. There are four main risks of using health data (Council of Canadian Academies, 2015): First, it is a possible that the data is accidentally release if data handling procedures are not appropriate. Health data, for example, can be stolen by mobile devices such as laptops and USB keys. Second, illegal access to databeses leads to misuse by intruders such as hacking of health care database. Third, inadvertent access can cause to recognize someone's privacy data. For example, an employee of the data custodian doing statistical analysis on a data set could inadvertently recognize a neighbour or relative in the database. Finally, anonymized data (de-identification) that prevents individual identities from being revealed in the information provided to the external researcher is contain risk. If anonymized is done poorly, the data could still contain sufficient information that individuals could be identified and their sensitive information revealed. Turkey restrict non-profit and university based researchers from access to the majority of national de-identified health micro datasets (OECD, 2015). In addition, Duly processed data must be deleted or anonymized if and when the processing is no longer needed. Anonymization is the process of taking out all personally identifiable data so that the data cannot be associated with any specific or identifiable person. Data is deleted or anonymized by the data controller *ex officio* or upon request by the data subject. The Law does not provide the details of the request process.

Barriers to accessing health data is another factor to get into account during health data process. While some barriers can affect timely access to available data, others can limit potential or interest to use data to generate research and innovation. There are many barriers related to access in health field. Cost, for example, is a factor in enabling access to data. Adequate and stable funding is needed to set up a sound infrastructure, attract and retain skilled staff members, and support the continued success of an organization (Marchessault, 2011). In addition, The access process may be unclear for researchers, and they may lack the skills or time to determine how they should proceed (Academy of Medical Sciences, 2006).

6. LEGAL FRAMEWORK FOR HEALTH DATA PRIVACY AT THE NATIONAL LEVEL

A large amount of health related information flows between patient and care providers when receiving health care. This raises a delicate issue that is mainly related to the collection, storing, and transmission of health data, which is considered by European and Turkish health law as "*sensitive data*", thus requiring reinforced protection. In the LPDP, health data is a particular category of data that is described as a sensitive data. This sensitive data means, according to (art. 6/1):

> *Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data are deemed to be personal data of special nature.*

Also and that the processing of such data is generally prohibited. This prohibition is established in article 6(2):

> *It is prohibited to process the personal data of special nature without explicit consent of the data subject*.

However, article 6(3) permits processing in some cases the personal data when:

> *Excluding those relating to health and sexual life such as the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing may be processed without seeking explicit consent of the data subject, in the cases provided for by laws.*
>
> *Personal data relating to health and sexual life may only be processed, without seeking explicit consent of the data subject, by any person or authorised public institutions and organizations that have confidentiality obligation, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.*

In short, the article claims that the data, except for the health and sexual life, may be processed without consent of a person. On the other hand, the health and sexual life data may only be processed as long as based on public benefit issues. In fact, the article provision is open to debate in terms of "Article 8 –Right to respect for private and family" of European Convention on Human Rights which is recognised by Turkey Republic.

Most countries have more than one national legislation that governs aspects of health data privacy protections (OECD, 2015). In Turkey, on the other hand, there is both general data privacy legislation applying to all personal data and health-sector specific legislation providing greater clarity regarding the collection and use of personal health data. Furthermore, enabling access to personal health data about individuals rests on legal and ethical norms. In Turkey, respect for privacy and confidentiality of personal health is protected by laws, rules and ethical principles. Hence, the government has a legislation governing the use and sharing of health information.

The Law on the Protection of Personal Data predominantly determine the legal framework for rights and obligations of persons whose data are collected and processed (data subjects) and for companies and governments that collect and process these personal data. The actual protection, on the other hand, does not only depend on the legal framework, but also the ways in which it is enforced by courts. Although the LPDP is rather new and there are no enforcement actions, the Personal Data Protection Board, the national supervisory authority in Turkey, has published the draft versions of the secondary legislation, as well as some booklets providing guidance on the implementation of the LPDP, allowing us to have somewhat of an understanding on how the brand-new data protection legislation will work. The Board is authorized to supervise personal data processing by entities to ensure protection of fundamental rights and freedoms, maintain the Data Controllers' Registry, set out the regulatory framework for personal data protection, impose administrative sanctions and publish a white list of countries where sufficient data protection measures are in place for a safe data export.

Under the LPDP in Turkey, personal data may only be processed in compliance with the procedures and principles set forth in this Law and other laws. Moreover, the following principles shall be complied within the processing of personal data:

1) Lawfulness and conformity with rules of *bona fides*.
2) Accuracy and being up to date, where necessary.
3) Being processed for specific, explicit and legitimate purposes.
4) Being relevant with, limited to and proportionate to the purposes for which they are processed.
5) Being retained for the period of time stipulated by relevant legislation or the purpose for which they are processed.

Internationally, most industrialized nations have laws protecting personal information or health information. However, there is large variation in the regulations, their objectives, and their restrictions on data sharing across international borders. In Turkey, for example, data protection and confidentiality is treated as a fundamental right in Constitution and sub-regulations. Personal data relating to health and sexual life may only be processed, without seeking explicit consent of the data subject, by any person or authorised public institutions and organizations that have confidentiality obligation, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing (Article 6(3) of the LPDP). Data confidentiality, however, is not conceived as a right in several other jurisdictions, such as the United States (European Union, 2000).

In addition, some national laws, such as Turkish Criminal Code numbered 5237, Turkish Civil Code numbered 4721, Turkish Code of Obligations numbered 6098, Labour Law numbered 4857, regulate the collection and use of personal data. All these legislations provide certain protections for personal rights that are indirectly related to personal data. The Turkish Constitution dated 1982, for example, provides the highest legislative authority for the regulation of personal data by setting fundamental principles. According to Article 20 of Constitution:

> "*Everyone has the right to request the protection of his/her personal data. This right includes being informed of, having access to and requesting the correction and deletion of his/her personal data, and to be informed whether these are used in consistency with envisaged objectives. Personal data can be processed only in cases envisaged by law or by the person's explicit consent. The principles and procedures regarding the protection of personal data shall be laid down in law*".

Turkish legislation strives to both protect health information privacy and facilitate information sharing as long as the personal data of special nature with explicit consent of the data subject. Personal data, on the other hand, excluding those relating to health and sexual life may be processed without seeking explicit consent of the data subject, in the cases provided for by laws. At the national level, key legislation includes the *Turkish Constitution (1982)*, the *Protection of Personal Data Act (2016)*, the *Regulation on Processing and Ensuring Privacy of Personal Health Data (2016)* and the *Patient's Rights Directive (1998)*. *The Regulation on Processing and Ensuring Privacy of Personal Health Data (2016)*, which set forth provisions concerning (i) health service providers, (ii) individuals whose personal health data has been processed, (iii) individuals and entities who provide hardware, software and filing system services to health service providers, and (iv) public institutions, organizations, individuals and other entities who process personal health data pursuant to the relevant regulations.

The *Patient's Rights Directive (1998)*, on the other hand, primarily covers; utilizing health services according to the principles of justice and equity, right to request information, right to request determination of priority, right to receive medical attention, right to receive general information, right to examine records, right to request record correction, right of privacy, right to not being exposed to any medical procedure without informed consent, right to have informed consent prior to organ or tissue transplantation or other medical research, right of the volunteers to be protected and informed, right to security, right to request respect to humanitarian values.

Furthermore, at the international level, the European Court of Human Rights, which is recognised by Turkey, guarantees the right to respect for private and family life, home and correspondence (Article 8). The court also stated that the importance of the protection of medical data to a person's enjoyment of the right to respect for private life (European Court of Justice, 2014). The European Court of Human Rights has stated in several instances that access to relevant health information can be seen as a component of the fundamental right to the protection of private and family life (Lemmens, 2013).

Regarding with processing of personal health data, Ministry of Health of Turkey put into practice a new information system that called "*E-Pulse*", which is an personal health record system that Turkish Ministry of Health integrated all the information systems of all health institutions. Thanks to e-Pulse, people can access their lab results, medical images, prescription and medication details, emergency information, diagnosis details, reports and health records that contains all the details concerning the examinations via desktop and mobile platforms. People can also share their medical records with their doctor(s) and relatives within specific regulations. This personal health record system, however, has been criticized by decision and policy makers in many ways such as protection of privacy, ensuring the safety of health data, the consent with respect to the processing of personal health data issues. All these criticism subjects needed to be discussed under the national and international regulations.

7. COURT DECISIONS ON HEALTH DATA

The protection of personal data, including medical information, is a fundamental feature of the right to respect for private life. Health data are considered sensitive by both the General Data Protection Regulation for European Union and the Regulation

on Processing and Ensuring Privacy of Personal Health Data for Turkey, are subject to stricter rules of processing. Respecting the confidentiality of health data is crucial not only for the protection of a patient's privacy but also for the maintenance of that person's confidence in the medical profession and in the health services in general. Without such protection, those in need of medical assistance may be deterred from seeking appropriate treatment, thereby endangering their own health (Council of Europe, 2015).

There is a decision about particular health data collection in the European Court of Human Rights. The main subject of judgement is the applicant alleged in particular that the collection of her personal medical data by a state agency in Latvia without her consent. The court emphasized that the importance of the protection of medical data to a person's enjoyment of the right to respect for private life. As a result, the court held in 2014 that there had been a violation of Article 8 of the Convention in the applicant's case (European Court of Justice, 2014).

In Finland, once a decision has been taken, the applicant's HIV infection data was shared with the national court during the proceeding of ex-husband convicted of manslaughter as an evidence despite her disapproval. The applicant's medical data had become part of the criminal proceedings against her ex-husband without her consent. As a result, the European Court of Human Rights found that a violation of Article 8 of the Convention (the European Court of Human Rights, 1997). In an Australian High Court case (High Court of Australia, 1996), on the other hand, it was held that medical records remain the property of the healthcare professionals (High Court of Australia, 1992), and patients have no right of access to their medical records. In some jurisdictions such as New Zealand, United Kingdom, United States, legislations have been enacted to allow patients the right of access to their medical records under certain conditions.

Under the Directive 95/46/EC principles, according to the European Court of Justice, the notion of "data concerning health" must be considred a broad interpretation to include information concerning all aspects (both physical and mental) of an individual's health (European Court of Justice, 2003; Costa et al., 2017).

General Assembly of the Supreme Court in Turkey has held that personal data is not required to be confidential (Decision dated, 17.06.2014, E.2012/12-510, K.2014/331). With this decision, the Supreme Court distinguishes between the concepts of privacy and confidentially. Because confidentially refers to the duties and practices of people and organizations to ensure that individuals' personal information. However, privacy broadly encompasses protection of one's physical self, protection of one's private physical space, and protection of information about oneself and one's activities. Therefore, privacy law to determine whether privacy is respected.

The LPDP numbered 6698 authorizes the Personal Data Protection Board to make the necessary examination in the matters falling within its scope of work upon complaint or ex officio, where it learnt about the alleged violation. The primary duties and powers of the Board are to ensure that the personal data are processed in compliance with fundamental rights and freedoms and to determine the adequate measures which are necessary for the processing of the data of special nature. In addition, The board can examine whether the personal data are processed in compliance with the laws, upon complaint, or *ex officio* where it learnt about the alleged violation, and to take temporary measures, if necessary.

The Board anonunced a decision (dated 21.12.2017 and numbered 2017/62) at the begining of 2018 that health care service providers must ensure that they have taken all technical and administrative measures to prevent presence of unauthorized persons at the tables, gates or benches and to prevent the recipients of services hearing, seeing, learning or reaching out each other's data. In Turkey, however, vast majority private and public health organizations provide a service that ensure personal data (i.e. patient's name and ID number) to call the patient. During a routine medical examination, for example, the patient's full name/ID number is displayed on the overhead patient call screen in the waiting room in most health care insitutions. Apperently, this practice does not protect patient's privacy. In this respect, according to the Board's decision, hospital or other healthcare institutions are obliged to take all necessary technical and administrative measures to provide a sufficient level of patient privacy. This practice, however, does not effectively and efficiently performing in most health services. The Board held that those who do not comply with the decision will be subject to administrative fines as per the Law.

8. CONLUSIONS

Some suggest that the right to control future use of health information is part of privacy protection, while others believe it is part of personal autonomy (Pritts, 2008). Regardless of the nature of the interest, approaches to this right to control vary from more restrictive to more flexible.

A very restrictive view is that people should provide consent for every specific future use of data for which they did not originally give their explicit informed consent. A more flexible view is that autonomy is respected when data are used for research related purposes in line with the type of research for which people originally provided consent.

The personal health data protection has become crucial, especially in the context of the patient confidentiality and the privacy of information. Medical information is one of the most sensitive personal data. Patients share information related to their disease to receive a better treatment. Because there is a large amount of health data flowing through the health care systems, the issues of privacy and data protection are not trivial nor easy to implement or enforce.

The protection of personal data, particularly health data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as well as patient confidentiality and the privacy of information. Respecting the confidentiality of health data is a vital principle in Turkish legal system. However, implementation of the data protection legislation, especially health data privacy, into national regulations are very new and transparency on personal data processing practices is low. Although the protection of personal health data is harmonized within the EU by Directive 95/46/EC, many differences still exist in the actual protection of personal data.

Finally, it is very important to regularly review the relevant policy to make sure it is still compatible with the practices of the workplace and the data it maintains and processes in Turkey.

9. LIMITATIONS

Limitations of this study are acknowledged since policy settings are also the result of other factors such as political, social, cultural, and historical, which are beyond the scope of this paper.

REFRENCES

Academy of Medical Sciences (AMS), (2006). *Personal Data for Public Good: Using Health Information in Medical Research*. London, United Kingdom: AMS.

Akıncı, A.N. (2017), Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi [*Evulation of General Data Protection Regulation in aspect of Turkish Law and Regulations*]. Paperwork Number-6, Kalkınma Bakanlığı, Yayın No:2968, 2.

Costa, A., Yelshyna, A., Moriera, T.C., Andrade, F., Julian, V., Novais, P. (2017), A legal framework for an elderly healthcare platform: A privacy and data protection overview, *Computer law & Security Review*, 33: 647-658.

Council of Canadian Academies (2015), *Accessing health and health-related data in Canada. The expert panel on timely access to health and social data for health research and health system innovation.* Ottowa, Canada, p.55-65.

Council of Europe (2015), Health-related issues in the case-law of the European Court of Human Rights, *Thematic Report*, 2015, p.4-27.

EU-European Union (2000), *Charter of Fundamental Rights of the European Union*, Online version available at: http://www.europarl.europa.eu/charter/pdf/text_en.pdf (viewed on 24th April 2018)

European Court of Human Rights (1997), the Court's case-law No.22009/93, Z. v. Finland, 25 February 1997, Online version available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-9432%22]} (viewed on 17th May 2018).

European Court of Justice (2003), Judgment of 6 November 2003, Case C-101/01 – Bodil Lindqvist, 50 and 51.

European Court of Justice (2014), Judgment of 29 April 2014, Case No. 52019/07 – L.H. v. Latvia.

High Court of Australia (1996), the Court's case-law No. 186 CLR 71, Breen v. Williams, 6 September 1996, Online version available at: http://www.julieclarke.info/publications/1998breen.pdf (viewed on 25th May 2018).

High Court of Australia (1992), the Court's case-law No. 2 SCR 138., Mclnerney v. MacDonald, 11 June 1992, Online version available at: https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/884/index.do (viewed on 20th April 2018).

Jutte, D. P., Roos, L. L., & Brownell, M. D. (2011). Administrative record linkage as a tool for public health research. *Annual Review of Public Health*, 32, 91-108.

Lemmens, T. (2013). Pharmaceutical knowledge governance: A human rights perspective. *Journal of Law, Medicine & Ethics*, 41(1), 163-184.

Lewis, S. (2011). How has health services research made a difference? *Healthcare Policy*, 6(Special Issue), 74-79.

Marchessault, G. (2011). The Manitoba Centre for Health Policy: A case study. *Health Policy,* 6(Special Issue), 29-43.

OECD (2015), Health Data Governance: Privacy, Monitoring and Research, *OECD Health Policy Studies*, OECD Publishing, Paris, p.11-110.

Roos, L. L., Brownell, M., Lix, L., Roos, N. P., Walld, R., & MacWilliam, L. (2008). From health research to social research: Privacy, methods, approaches. S*ocial Science & Medicine*, 66(1), 117-129.