
Report prepared for the Data Futures Partnership

The Sharing of Personal Health Data – A Review of the Literature

David Moore and Malin Niemi

29 June 2016



This work is licensed under the Creative Commons Attribution-NonCommercial 4.0 International License. To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc/4.0/>.

About Sapere Research Group Limited

Sapere Research Group is one of the largest expert consulting firms in Australasia and a leader in provision of independent economic, forensic accounting and public policy services. Sapere provides independent expert testimony, strategic advisory services, data analytics and other advice to Australasia's private sector corporate clients, major law firms, government agencies, and regulatory bodies.

Wellington Level 9, 1 Willeston St PO Box 587 Wellington 6140 Ph: +64 4 915 7590 Fax: +64 4 915 7596	Auckland Level 8, 203 Queen St PO Box 2475 Auckland 1140 Ph: +64 9 909 5810 Fax: +64 9 909 5828	
Sydney Level 14, 68 Pitt St GPO Box 220 NSW 2001 Ph: +61 2 9234 0200 Fax: +61 2 9234 0201	Canberra Unit 3, 97 Northbourne Ave Turner ACT 2612 GPO Box 252 Canberra City, ACT 2601 Ph: +61 2 6267 2700 Fax: +61 2 6267 2710	Melbourne Level 2, 65 Southbank Boulevard GPO Box 3179 Melbourne, VIC 3001 Ph: +61 3 9626 4333 Fax: +61 3 9626 4231

For information on this report please contact:

Name: David Moore
 Telephone: +64 4 915 5355
 Mobile: +64 21 518 002
 Email: dmoore@srgexpert.com

Contents

1.	Introduction	1
1.1	Purpose of this report	1
1.2	Our approach.....	1
2.	The sharing of personal health data and social licence issues	2
2.1	We are leaving digital footprints behind us every day.....	2
2.2	Gaining social licence relies on an organisation fulfilling implicit norms	2
2.2.1	Elements of a social licence in a personal health data context	3
2.3	What motivates people to share their personal health data varies between individuals and contexts	6
2.3.1	New Zealanders are relatively reluctant to share their personal health data with government agencies	8
3.	Data types and uses	9
3.1	Personal health data is wider than medical records	9
3.2	The range of stakeholders and uses of health data go far beyond the area of health care	10
4.	Benefits and concerns	13
4.1	Publicly available health data has significant individual and societal benefits.....	13
4.2	Concerns about individual harm make people less willing to share their health data.....	15
4.2.1	A distinction between subjective and objective harm	16
5.	Cross-cutting issues	18
5.1	Areas for further research.....	19
6.	References	20

Tables

Table 1	Examples of uses across stakeholder groups	11
Table 2	Examples of benefits from sharing personal health data	14

Figures

Figure 1	Elements of a social licence in a personal health data context	4
----------	--	---

1. Introduction

1.1 Purpose of this report

The Data Futures Partnership Working Group commissioned a review of issues and questions raised across New Zealand and internationally on the sharing of personal health data in general, and in particular the factors that influence people’s acceptance and approval of sharing the data – i.e. social licence issues.

1.2 Our approach

Our approach has been to synthesise existing information related to the sharing of personal health data by drawing on academic journals, media coverage and political debates – in New Zealand and internationally. The emphasis has been on finding and documenting key themes, rather than giving a more exhaustive review of the literature.

Our search strategy included using Boolean operators, searching across various sources including: Ebsco Business Premier, ABI/Inform Global, ProQuest Research Library, Google Scholar, Google Books, Web of Science, Elsevier’s Scopus, and Google ((using “intitle” (for keywords) and “inurl” (for domains) commands)). The search included using free text and keywords, as well as using commands for specific fields such as Subject, Abstract, Title and Descriptor. In addition, “New Zealand”, “NZ” and “govt.nz” were used as keyword and inurl: terms.

Our search terms included using a combination of terms from the left column below, with one or more of the phrases listed in the right column below.

- | | |
|--|---|
| <ul style="list-style-type: none">• Social licence• Social contract• Social contract theory• Trust• Ethics• Privacy• Security• Confidentiality• Corporate social responsibility• Economics of Privacy | <ul style="list-style-type: none">• Health information• Personal/individual health data• Personal/individual information• Big data• Big health data• Data governance• Data mining• Data sharing• Information sharing• Analytics• Access to information• Electronic health informatics• Electronic health records• Ethical health informatics• Personal information privacy• Quantified city/community• Genomics |
|--|---|

2. The sharing of personal health data and social licence issues

2.1 We are leaving digital footprints behind us every day

By using our mobile phones, credit cards, tracking devices, search engines and websites –bits of data containing information about ourselves are being generated every day and these digital footprints can in many instances be used to find out about both our mental and physical health. Examples of data generating activities include (Sarasohn-Kahn 2014):

- Googling health related terms or using online tools for health information;
- Using mobile phone apps, digital health and medical devices such as fitbits, weight scales, and blood pressure monitors;
- Purchasing health and medical products using a credit card or consumer loyalty cards;
- Passively communicating personal information such as location and retail store preferences through GPS sensors integrated into smartphones; and
- Buying fast food, cigarettes, and anything else that might have an impact on health.

By linking and aggregating this kind of behavioural data with individuals' records from genetic, medical and genealogical data, a detailed health profile of individuals, communities, cities, and countries can be created and used for many purposes – including preventing spread of epidemics, promoting healthy behaviours, and increasing the quality of health services (Sedenberg and Mulligan 2015, Sarasohn-Kahn 2014).

However, these uses require a critical mass of data at a sufficiently granular (individual) level, which raises issues such as personal privacy, lack of control of data ownership and trust. In turn, these issues act as major barriers to gaining detailed personal health information at a larger scale, which then limit the individual and societal benefits that can be drawn from the personal health data (Kostkova, et al. 2016, Nature Biotechnology 2015).

Consequently, sharing personal health data means that a trade-off arises where individuals need to give up some amount of privacy and control, in order to obtain benefits – either directly (personal) or indirectly (societal) (Brack and Castillo 2015, Conge, Pratt and Loch 2013).

2.2 Gaining social licence relies on an organisation fulfilling implicit norms

What makes people share (or not share) their health information can be analysed from the concept of social licence. The premise of social licence builds upon trust and credibility between an individual and a certain organisation – be it the national government, the local government, a company or a research institute – and throughout the literature it is usually defined as a “community’s acceptance or approval of the presence of an organisation’s

operations in their area”, and it has been increasingly recognised by various agencies as a prerequisite to development (Data Futures Partnership 2016, Yates and Horvath 2013).

The concept of a social licence applied to the sharing of personal health data is somewhat analogous to participation as a subject in a research study – where previous research suggests that an individual’s cooperation depends on a belief of voluntary participation and that the study is governed by values of reciprocity, non-exploitation, and service for the public good. If these conditions are not believed to be met, threats to the social licence of the research project may emerge – which may limit the number of voluntary participants (Carter, Laurie and Dixon-Woods 2015).

Moreover, general issues that are taking part in the social licence conversation today include issues of data ownership and control (including protecting any cultural value of data), finding suitable methods of benefit sharing, and communicating societal and individual benefits that might be gained from sharing personal health data (Gluckman 2015).

Social contract – an alternative concept used within the literature

Social licence is a relatively new concept throughout academia, dating back to 2007 (Data Futures Partnership 2016). Similar to social licence is the concept of “social contract”, which has also been used within the literature of data sharing and individuals’ acceptance of organisations’ activities within a community. It has been defined as consisting of “shared norms or understanding about the rights and responsibilities between two parties in an exchange relationship” (Li, et al. 2014).

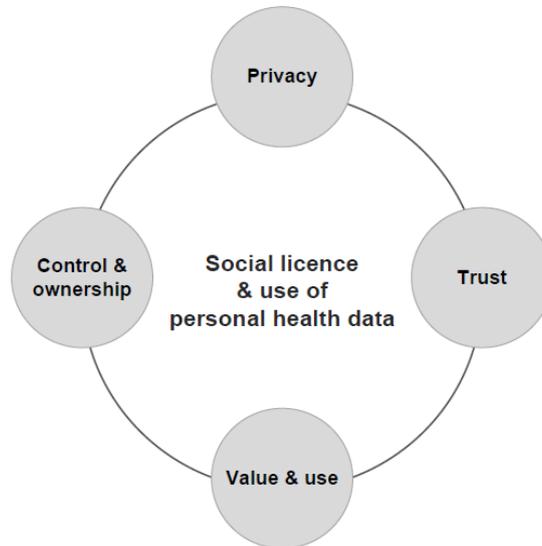
Like social licence, trust is an essential element of a social contract. Without trust, the social contract may not form, as individuals are less likely to believe that an agent will respect the rights and responsibilities in the social contract. Instead, they are more likely to believe that the agency will undertake opportunistic behaviours. In the case of data exchange and social contracts, some basic norms identified in prior studies are organisations’ social obligations to respect individual’s information privacy (Li, et al. 2014).

One difference between the above definitions of social licence and social contract implies that while a social contract can be seen as an implicit contract between two parties – where the norms work *both ways* – gaining social licence relies solely on the organisation fulfilling the implicit norms. In other words, from a social contract point of view – an individual may be considered having a duty to inform the rest of the society if their health directly implicates the well-being of others (Sedenberg and Mulligan 2015). This has not been explicitly raised as an issue within a social licence context.

2.2.1 Elements of a social licence in a personal health data context

The elements of a social licence are the conditions (implicit norms) that attach to the provision of personal health data from individuals to an agent. Figure 1 illustrates key elements within an individual health data context, as identified from the current literature, which should be addressed in order for agencies to increase the probability of gaining social licence.

Figure 1 Elements of a social licence in a personal health data context



Privacy

Individual privacy is an important factor affecting willingness to share personal health data (Vithiatharan 2014, Calit2 2014). In this context, privacy refers to who has access to the data and how identifiable a person is from that data. Overseas studies have found a strong preference among individuals for their data to be anonymised (Calit2 2014, IPSOS MORI 2014).

Trust

The issue of trust is closely linked to that of privacy. For example, the Health Data Exploration project¹ found that the dominant condition attached to the release of individuals' personal health data for research was an *assurance* of privacy (Calit2 2014). Demand for privacy increases in response to adverse data events (such as data breaches) which diminish trust in such assurances.

The trust factor is also closely linked to the question of what the data is used for (IPSOS MORI 2014). Research by IPSOS, carried out among over 2000 Britons, found a “data-trust deficit” whereby trust in institutions to use data appropriately was lower than trust in those institutions generally. The research indicates that trust is higher when data sharing has a clear public benefit and when there are safeguards in place. The addition of safeguards such as anonymisation of data, or punishment for data misuse, significantly improved the level of support for data sharing from 33 percent to around 51 percent (IPSOS MORI 2014).

¹ The Health Data Exploration project conducted a study within the U.S to better understand the barriers to using personal health data in research from the individuals who track the data about their own personal health, the companies that market self-tracking devices, apps or services and aggregate and manage that data, and the researchers who might use the data as part of their research (Calit2 2014).

Value & use

Willingness of individuals to share personal health data has been demonstrated to be strongly linked to the question of what that data will be used for, and in particular to the value of that use (Calit2 2014, IPSOS MORI 2014, Gluckman 2015). As we will explain below (section 4.1), the value from sharing personal health data can be direct to the individual and/or of wider benefit to society. Research has shown that while some individuals are more willing to share their data if it will directly benefit them, others are willing to share for altruistic reasons (Kostkova, et al. 2016). Moreover, if people believe that agencies will use the data for their own benefit and not for the common good, individuals have been found to be less willing to share their data (IPSOS MORI 2014). This finding is closely linked to the element of trust.

Control & ownership

Closely related to privacy is the need for consent, which is a way of giving individuals control and ownership over their own data (Calit2 2014). Research suggests that sharing is more likely to occur when individuals have the power to select the conditions under which they share their data (Pickard and Swan 2014). The concept of consent refers to the person's right and ability to control information about themselves, and to impose limitations on its use and reuse by entities such as researchers and health care organisations (Roski, Bo-Linn and Andrews 2014).

Research has shown that people are generally less concerned about privacy when fair information practices (FIPs) are implemented. FIPs are defined as “procedures that provide individuals with control over the disclosure and subsequent use of their personal information and govern the interpersonal treatment that consumers receive” (Li, et al. 2014).

In terms of sharing personal health data, three general approaches to consent have been identified (Vayena, Mastroianni and Kahn 2013):

1. Opt-in to information sharing;
2. Opt-out of information sharing,² and
3. Information sharing as a condition of use of a particular site/device/mobile application.

The third approach refers to a website's terms of use, terms of service, or privacy statements, implying they maintain the right to use the data they collect. By virtue of using the site, the user agrees to share the data generated. This third category sometimes includes “inferred consent” by people who (potentially unknowingly) share their data by using websites, mobile phone applications, tracking devices etc. As people are increasingly sharing their information online, concerns regarding this third option will become more pointed (Kostkova, et al. 2016, The Economist 2016, Vayena, Mastroianni and Kahn 2013).

² While offering options for individuals to “opt-in” or “opt-out” of research will help mitigate concerns, this may also increase the risk of bias in the data (Bipartisan Policy Center 2013).

2.3 What motivates people to share their personal health data varies between individuals and contexts

The motivations behind disclosing personal health information has been recognised to be more complex than in other areas where similar privacy concerns exist (for instance the sharing of financial data) (IPSOS MORI 2014, Pickard and Swan 2014). So far, we have established the issues that are important for an agency to address – in order to increase the chances of gaining social licence – involves addressing aspects of privacy, trust, value and use, and control and ownership. Uncertainties regarding these concerns have long made individuals reluctant to share their personal health data. However, a few recent studies have found that people are becoming increasingly willing to share their data (Pickard and Swan 2014, Calit2 2014).

For instance, on websites such as PatientsLikeMe.com, individuals share their personal health data with peers with similar medical conditions with the motivation to learn as much as possible about mutual health concerns, and the recent development of data sharing communities such as the “Quantified Self” movement (see Case study 1 below) and datadonors.org show that people are becoming more willing to trade some of their privacy and control over their data, for its value and use. While the “Quantified Self” movement consists of advocates for self-tracking with the ultimate desire to enhance their personal lives, datadonors.org is urging people to actively link and share their personal data with the ultimate purpose of saving lives. The latter’s mission is to provide a database to researchers, scientists and physicians within the global health community – to help enhance their research and better the prospects of healthier people and communities (Kostkova, et al. 2016, DataDonors n.d., Hoffman 2015, Calit2 2014).

The “Quantified Self” movement and datadonors.org demonstrates that people who are willing to actively share their data, are motivated by different factors. While the former are motivated by personal gain – the latter are motivated by societal gain and altruism. These examples further illustrate that people are increasingly noticing the possible values and areas of use that their health data may bring – both directly to the individual and to society. Whether the underlying reason behind the growth of these communities is an increased feeling of trust and/or a growing awareness of the possible values and benefits of health data, or whether it is due to other factors, requires further research.

Moreover, a U.S. survey study of 128 participants, investigating people’s willingness to share their personal health data, found that approximately 63 percent were willing to share their health data in some instances. The type of data they would be willing to share included data related to: diet (88 percent), exercise (88 percent), traits (85 percent), diseases and conditions (81 percent), genomic data (80 percent), fitness tracking information (80 percent), medications (79 percent), and electronic medical records (72 percent) (Pickard and Swan 2014).

The main motivation for sharing was the possibility of making new health discoveries (88 percent), followed by the incentive of learning more about personal health risks (82 percent). 73 percent felt motivated to share personal health information due to a desire of changing the current system. Only 15 percent wanted something in return (Pickard and Swan 2014).

Case study 1 : The Quantified Self Movement

The Quantified Self (QS) movement's mission is to "support new discoveries about ourselves and our communities that are grounded in accurate observation and enlivened by a spirit of friendship". Thus, QS brings together people who share an interest in gaining self-knowledge through self-tracking, and want to take ownership of and reap the value of their own data (QuantifiedSelf n.d.). The movement originated in San Francisco, where Gary Wolf, a journalist and author, co-founded the "Quantified Self" blog in 2007. This has now spread to multiple countries around the world where people – at conferences, meetings and online – share experiences of self-tracking techniques using devices such as Fitbit or Nike Fuelband (Watson 2013, The Economist 2012).

For instance, at a conference held in 2011, people highlighted many beneficial uses of their health data, which has helped to enhance their lives. Examples included an iPhone app which helps determine the best drug combination to control a person's Parkinson's Disease and a device called "Zeo", which tracks sleep quantity and quality by measuring brainwave activity to determine how long the wearer spends in light, deep, and rapid-eye-movement (REM) sleep. In 2012, Zeo had generated the largest-ever database on sleep stages, which revealed differences between men and women in REM-sleep quantity. Another device mentioned was "Spiroscout". This device has a sensor that attaches to an asthma inhaler and uses satellite-positioning data to enable patients and researchers to work out which environments make their condition worse (such as proximity to a particular type of crop) (The Economist 2012).

As a result of the movement's significant spread across the world, self-quantifying has been thought to give a glimpse of the future of health care in which a greater emphasis is placed on monitoring (using a variety of devices) to prevent disease, prolong lives, and reduce medical costs (The Economist 2012).

The movement has also arrived at workplaces. Each day, more tools are being developed to help employers monitor, track, and better understand the activity of workers. These tools are real-time, often anonymous and usually invisible. Many of the startups in Human Resources (HR) believe that bringing the QS to HR is the next big thing. While some argue that this is a great development (for instance as it is believed to lead to more transparency and efficiencies), these devices will raise many issues about data ownership and workplace privacy (Watson 2013, Bersin 2014).

Others point out that it is the corporations that ultimately will benefit from these data-gathering practices. Moreover, another problem is that self-quantification experiments lack the rigorous controls of pharmaceutical trials, and that the results generated could purely be due to placebo effects (Kennedy, Poell and Dijck 2015, The Economist 2012).

2.3.1 New Zealanders are relatively reluctant to share their personal health data with government agencies

With respect to sharing electronic health records (EHR), key factors that have been shown to influence the willingness of New Zealanders to share their personal health information include (The Palliative Care Council of New Zealand 2010)³:

- The role of the person requesting the information;
- The content of the information requested, and
- The level of individual identification.

Māori have also expressed concern about rights of access to, and use of, personal health information.⁴

In regards to the role of the person requesting the information, findings from a 2006 New Zealand survey of 200 respondents found that the respondents were:

- Willing to share all of their information with health professionals, especially if they were consulted first;
- Willing to share their information with health administrators and researchers, if they were consulted first, and
- Less willing to share information with other organisations (such a government agencies or private health insurers) (Whiddett, et al. 2006).

This is consistent with findings from another, more recent paper, which found that while many New Zealanders are happy with general practitioners and hospitals receiving their personal information, only 17 percent were happy to share their personal health data with the Ministry of Health (Scoop Media 2015).

A key conclusion from the report by the The Palliative Care Council is that New Zealanders feel their health data belongs to them, which means a level of trust must be formed between the individual and the users of the data. In addition, New Zealanders want to know how their personal health information is going to be used and they want to be given the opportunity to give their consent (or not) to these uses (The Palliative Care Council of New Zealand 2010). Thus, in order for New Zealanders to be more willing to share their health data and give up privacy, the elements of trust, value and use, and control and ownership need to be addressed.

³ This is drawing on conclusions found by a 2009 survey of 1,828 respondents carried out throughout New Zealand. The survey aimed to examine attitudes towards sharing confidential personal health information held in EHRs (Hunter, et al. 2009).

⁴ The principle of rangatiratanga, whereby Māori are guaranteed the right of ownership over their taonga, or knowledge, has been interpreted as meaning health-related data about an individual belongs to an individual, especially when it is used as grouped data (The Palliative Care Council of New Zealand 2010).

3. Data types and uses

3.1 Personal health data is wider than medical records

Today, healthcare data come in many formats, including structured and unstructured free-text data captured by EHR and data streaming from social media and mobile applications.⁵ Within health care, much attention has been given to big data⁶, which covers a whole range of data types, including (Bipartisan Policy Center 2013):

- Clinical data derived from EHR within physician offices, hospitals, imaging centres, laboratories, pharmacies, and other settings in which care and services are delivered;
- Claims and cost data derived from those who pay for and manage care;
- Biometric data derived from devices and other remote tools that monitor such things as weight, blood pressure, blood glucose levels, etc.;
- Data input by individuals, including preferences, satisfaction levels, health status, and self-tracking information on food intake, exercise, sleep, etc.;
- Genomic information;
- Data on other determinants of health, such as those related to socioeconomic factors and the environment, and
- Social media data.

Different types of health data can further be divided into three broad categories of data and level of access (Heitmueller, et al. 2014, Groves, et al. 2013):

1. **Personal and proprietary data.** This type of data is controlled by individuals and non-governmental bodies, including commercial entities, pharmaceutical companies, academia or non-government organisations. Typically, the individual or commercial entity has the desire, and often the legal right, to restrict access to and use of the data. Examples of this data are information on people’s clinical trials, personal health records, and cell phone and credit card information.
2. **Government-controlled data.** The second type is data to which a government can restrict access. These data include census data and, in some countries, personal health records. The advent of big data in health care may dramatically expand the depth and breadth of this data to include data on individual behaviour.

⁵ Much of the information collected is not put to use to improve health or health care. For example, studies have shown that less than 15 percent of health data in EHR are entered in structured data fields that allow those data to be analysed using traditional retrieval and analysis methods (Roski, Bo-Linn and Andrews 2014, Bipartisan Policy Center 2013). Due to the significant amount of data that is being collected by an ever increasing use of self-tracking devices, new ways of storing, analysing and re-using this “big-data” are currently being developed (Calit2 2014).

⁶ To date, there is no single widely accepted definition of big data. However, a common way of describing it is through the three Vs; volume, variety and velocity (Roski, Bo-Linn and Andrews 2014).

3. **Open data commons.** This data is available to all and it may be private, commercial, or government controlled. In contrast to open data, open data commons are usually kept up-to-date and provided in accessible format – enabling the immediate use of information.

A key presumption is that data is worth more when shared: previously unconnected data such as personal health records from different health and social care providers can be linked and analysed to provide new insights that can inform improvements in sectors of the economy such as health care. This data can be both real-time and unprecedented in their level of detail because they can rely on data already produced as a side effect of daily life, such as location data tracked by GPS sensors in mobile devices.

3.2 The range of stakeholders and uses of health data go far beyond the area of health care

Research has suggested that health care services, such as visits to the doctors, contribute to only about 10 percent of health outcomes. Individual behaviour and lifestyle choice, on the other hand, determine as much as one-half of health status – which is why behaviour change has been called by some ‘the Holy Grail of health care’ (Sarasohn-Kahn 2014, Roski, Bo-Linn and Andrews 2014).

Much of the personal data collected from consumers today would not be considered “health information”, yet it is used for a health purpose. Even consumer footprints that are not expressly about health can, through algorithms, be used to help determine a person’s physical or mental health. How we shop, the magazines we subscribe to, our “likes” on Facebook, where we spend our weekends – this information can relatively easily be purchased by third parties, as discovered by investigative reporters in 2014 (Kroft 2014, Sarasohn-Kahn 2014, Kshetri 2014). This also implies that the range of stakeholders and the range of potential uses of health data go way beyond the area of health care.

The primary stakeholders on the pathway from the collection and sharing of personal health data to improve outcomes for individuals and public good can be divided into the following groups (Calit2 2014, Heath Information and Quality Authority 2012):

- The individuals who generate and use the data;
- The companies that produce, aggregate, use and manage that data;
- The researchers who collect and use the data to produce research results, and
- The government and other agencies, such as hospitals, which will use this information for various policy, regulatory or health care improvements.

Disclosed personal health data can be used for a vast amount of purposes. A few examples of uses split between these four stakeholder-groups are listed in Table 1.

Table 1 Examples of uses across stakeholder groups

Stakeholder group	Examples of uses
Individuals	<ul style="list-style-type: none"> • Self-tracking devices, such as Zeo, monitor sleep habits, which enable users to figure out sleep patterns and improve their sleep (The Economist 2012). • Accessing health information enables individuals to monitor chronic conditions, follow treatment plans, find and fix errors in their health records, and track progress in wellness or disease management programs (Health Information Privacy n.d.).
Companies	<ul style="list-style-type: none"> • Insurance companies have been known to use information on driving habits in walkable neighbourhoods. Those individuals that were more likely to drive everywhere were targeted with messages about healthy behaviours on social media (Robbins 2015). • Castlight Healthcare, which serves companies such as Walmart, has a program that attempts to predict when employees are pregnant or trying to conceive by monitoring their search queries and scanning their insurance claims to find workers who have stopped filling their birth-control prescriptions. Castlight’s presents these results to employers, by giving the number of workers who are “normal-risk pregnancy”, “high-risk pregnancy”, and “considering pregnancy” (Edwards 2016). • Google has used search data to try to predict flu trends. The basic idea is that when people are sick with the flu, many people search for flu-related information on Google, providing almost instant signals of overall flu prevalence (Lazer and Kennedy 2015). • The Durkheim Project, a collaboration between the Veterans Health Administration and Facebook, is using real-time prediction software to analyse voluntary, opt-in data from veterans’ social media accounts and mobile phones for suicide risk prevention (Young 2014).
Researchers	<ul style="list-style-type: none"> • The European Prospective Investigation into Cancer and Nutrition (EPIC), the largest study of diet and health ever undertaken, is researching how diet, lifestyle, and environmental factors influence health and disease. EPIC has for instance found that a large consumption of processed meat is associated with increased risk of cancer (Riboli 2001).
Governments and institutes	<ul style="list-style-type: none"> • A retrospective analysis of the 2010 cholera outbreak in Haiti showed that mining data from Twitter and online news reports could have given the county’s health officials an accurate indication of the disease’s spread with a lead time of two weeks (Kshetri 2014). • Through measuring the way New Yorkers interact with their urban environment, New York University and Hudson Yards developers aim to make the city a better place to live. To do this, they will collect information on pedestrian traffic, air quality, consumption, and health and activity levels of workers and residents (Anuta 2014). • In Dubai, medical professionals will be given secure log-in credentials to access electronic health records in order to prevent abuse of medical insurance (Webster 2016).

Case Study 2. Indiana's infant mortality project

The U.S state of Indiana has long suffered from a relatively high rate of infant mortality. Suspecting that the solution to Indiana's infant mortality problem may lay hidden in the state's records, the state government initiated a pilot study – addressing the problem by linking and analysing big data (Ravindranath 2014, Indiana State Department of Health 2014).

By crunching data from five agencies and four public sources – covering everything from finances to criminal histories – Indiana discovered young mothers enrolled in Medicaid who rarely visit a doctor during their pregnancy account for almost half of infant deaths in the state. The government found that the largest factor that they can influence, as a government entity, is getting those mothers to attend prenatal visits. As a result of this, Indiana's 2016-17 budget includes more than \$13.5 million for improving prenatal care for the state's youngest and economically challenged mothers, including a new smartphone app that will help them find doctors, remind them of appointments, and link them to transportation services (The Center for Digital Government 2015).

In addition to reducing infant deaths, the state expects to save money because infants born to the highest-risk mothers also tend to face health challenges. By getting mothers to attend prenatal visits, and if this can increase the probability that the babies are born at a normal birth weight, the actual cost to Medicaid in their first three years of life can be reduced by hundreds of thousands of dollars (The Center for Digital Government 2015).

The Washington Post recognises that Indiana's pilot comes at a time when federal, state and local governments are gradually showing interest in big data. In May 2014, the Obama administration published a review of big data applications in the public and private sectors, and last year the president signed an executive order requiring the government to make its data available to the public (Ravindranath 2014).

4. Benefits and concerns

In order for individuals to be willing to give up some amount of privacy and control over their data, they ultimately need to decide if the benefits outweigh the costs. While section 4.1 outlines what these benefits might be, section 4.2 outlines individual concerns and the potential harm that may come from giving up privacy and control over individual health data.

4.1 Publicly available health data has significant individual and societal benefits

The vast amount of personal health data generated and stored around the world each day offers significant opportunities for advances such as new scientific discoveries, research cost savings, new tools to help patients navigate the healthcare system and improved healthcare quality (Kostkova, et al. 2016, Heitmueller, et al. 2014, Hoffman 2015). Larry Page, Google co-founder and CEO, urged people to think about “the tremendous good that could come from sharing the right information with the right people in the right ways” (Sarasohn-Kahn 2014, Roski, Bo-Linn and Andrews 2014).

On multiple occasions, health data has already demonstrated its actual and potential economic and clinical value. As research has shown that individuals’ willingness to share their data are influenced by the value it will bring to them directly or to society as a whole (see section 2.3), the examples given in Table 2 are split between examples that can be considered to *directly* benefit the individuals who share their data and examples that are first and foremost benefiting society. While individual benefits will lead to benefits for society⁷, societal benefits do not necessarily always benefit the individual. Inequalities and individual harm that may arise from data sharing are discussed in section 4.2 and chapter 5.

⁷ Within economics, the concept of social benefit is the sum of all private benefits plus any external benefits that may come from production/consumption (Rittenberg and Tregarthen 2011).

Table 2 Examples of benefits from sharing personal health data

Direct individual benefits	Wider societal benefits
<ul style="list-style-type: none"> • The delivery of personalised medicine (individualised diagnoses and treatments based on a patient’s detailed risk profile) has been demonstrated for care of patients with cancer or other conditions. • The reliance on patient-generated data has been demonstrated using mobile devices to tailor diagnostic and treatment decisions, as well as educational messages to support desired patient behaviours. • A few studies point out that the internet has raised the possibility of consumers directly benefiting from the disclosure of personal data, such as through the use of networks and social media. • Other immediate benefits to the individual include improvements in care for long-term conditions and opportunities for home care using remote and telehealth technologies, enabled by easier access to health data. 	<ul style="list-style-type: none"> • The use of mobile phones with geo-location features has – based on call-patterns and mobility patterns – been used to anticipate epidemics: cholera in Rwanda, malaria in Kenya, and malnutrition in Tanzania. • In Portugal and Spain, Twitter tweets have been analysed to understand depression, eating disorders, flu and pregnancy. • The sharing of large population level data helps researchers to accurately describe health inequities and highlight problematic areas and specifically target groups, geographical and regional challenges. • Hospitals can use health data to improve efficiency, quality of care and reduce readmissions. • Health information exchanges can contribute to effective drug regulation and reduce direct costs of medical expenditure and indirect costs associated with lower productivity. • Better implementation of disease and risk prevention programmes such as vaccine programs, institutionalizing sanitation infrastructure, occupational hazard laws, education, and behavioural incentive programs. • Better implementation of management and response programs such as disease detections.

Source: Sarasohn-Kahn, 2014; Roski, et al., 2014; Kroft, 2014; Kostkova, et al., 2016; Groves, et al., 2013; Kshetri, 2014; Acquisti, 2014; Sedenberg & Mulligan, 2015.

Case study 3: The Human Genome Project

The Human Genome Project was a 13-year-long, international, publicly-funded project initiated in 1990, whose goal was the complete mapping and understanding the entire human genome within 15 years (Chial 2008). The Project has been highlighted as “the first successful biomedical big data program” and the factors that are believed to have contributed to this success include (Bipartisan Policy Center 2013):

1. National objectives of participating countries were clearly articulated.
2. A new culture of sharing rather than guarding data was defined and promoted within the scientific community.
3. The program fostered the development of data standardisation, archiving and distribution process.
4. The program included incentives to make the data easily, widely and quickly available.
5. Project funders built many of these steps into their requirements.

As a result of this project, the number of human disorders for which the molecular basis is now known grew from about 60 to almost 5,000. This has directly influenced the development of more than 100 drugs. Furthermore, the research has resulted in the discovery of more than 1,800 disease genes and has reduced the time it takes to find a gene suspected of causing an inherited disease from years to days (Bipartisan Policy Center 2013).

In its early days, the Human Genome Project was met with scepticism by many people, including scientists and non-scientists alike. One prominent question was whether the huge cost of the project would outweigh the potential benefits (Chial 2008). As the project went on, new issues were raised about ethical, legal, and social issues, which are why parts of the project’s budget were allocated to researching non-clinical issues – including philosophical, theological, and ethical perspectives on new genetic knowledge (Collins 1999).

Worries included preserving the confidentiality of an individual's DNA information and avoiding the stigmatisation of individuals who carry certain genes. Some feared that insurers will deny coverage to people carrying a gene that predisposes them to particular diseases, or that employers might start demanding genetic testing of job applicants. Also the Clinton administration endorsed the need for congressional action to protect against genetic discrimination in health insurance and employment (Collins 1999).

4.2 Concerns about individual harm make people less willing to share their health data

While there are clear benefits of research using personal health data – capturing, analysing, and sharing health data does come with particular concerns at an individual level, as disclosure affects the balance of power between the data subject and the data holder. The intended or unintended release of a person’s health information into the public has great potential to undermine personal dignity, cause embarrassment and financial harm (Heitmueller, et al. 2014, Acquisti, 2014).

Consider for instance genetic data: genomic analyses may not only reveal information about an individual's current health, but also about future health risks. These analyses are useful for patients and healthcare providers because they can, for instance, help facilitate the delivery of personalised medicine. However, by disclosing genomic information, individuals face privacy risks. For instance, as noted above, if such information reaches advertising agencies, insurance companies or employers, then they may use it to construct risk profiles for individuals and their biological relatives and use this information to their advantage (Acquisti, Taylor and Wagman 2016). Many organisations believe that making data anonymous before sharing with third parties would make it impossible to identify. This is often a convenient, but possibly a false assumption. Researchers have presented a variety of methods and techniques that can be used to re-identify personal data and re-associate information with specific individuals (Kshetri 2014).

The U.S survey study of 128 participants (mentioned in section 2.3), found that the main barriers to sharing personal health data included privacy concerns, lack of awareness of value of contribution, and concern about data being used for profit. Furthermore, when asked about sharing genomic data, specific concerns included: insurance discrimination, personal or family privacy, employment discrimination and racial discrimination (Pickard and Swan 2014).

In another survey by IPSOS, carried out among over 2000 Britons, the main outcome showed that there exists a large “data-trust-deficit” for many institutions. The findings illustrate that concerns may be driven by the feeling that data-sharing is not benefitting the individuals themselves and it is a strong suspicion that companies use their personal information for their own benefit and not for the individual's (IPSOS MORI 2014).

Moreover, disclosure of personal health data has been considered more likely to negatively affect the welfare of more vulnerable and technologically un-savvy individuals. These individuals may lack awareness/information, and are less likely to receive up-to-date and accurate information. They are also not in a position to assess the degree of sensitiveness of their online actions and are more likely to be tricked by illicit actors (Kshetri 2014).

4.2.1 A distinction between subjective and objective harm

Within the field of economics of privacy, there has been a distinction between subjective and objective privacy harm – which may make people less willing to share their data.

- **Subjective harm** derives from unwanted perceptions of observation (e.g. issues related to anticipation). This may include anxiety, embarrassment or fear; the psychological discomfort associated with feeling surveilled; the embarrassment associated when sensitive information is exposed publicly or fearing one's personal life will be intruded upon (Acquisti, 2014).
- **Objective harm** consists of the unanticipated or forced use of information concerning an individual, to be used against this individual (e.g. issues related to consequences). Examples include higher prices one pays due to adverse price discrimination. For instance, some analysts suggest medical insurance companies can increase premiums for people with a higher probability of a certain disease. Similarly, some life insurers reportedly predict life expectancy based on individuals' consumption patterns and use that information to offer rates (Lupton 2014, Acquisti, 2014, Kshetri 2014).

Other issues relate to profiling, segmentation, and discrimination. For instance, profiling could be used to nudge consumers towards products that may not enhance their wellbeing, and information revealed on a social network may lead to job market discrimination (Acquisti, 2014).

5. Cross-cutting issues

A common issue raised within the literature is the individual and societal trade-off that arises with sharing and protecting personal health data. In order to reap the individual and societal benefits gained from personal health data, individuals are required to give up some level of privacy. Research has shown that in order for agencies (including governments, companies, institutes and researchers) to gain social licence, factors that need to be addressed include trust, control and ownership, and value and use. By adequately and transparently addressing these factors, the probability of gaining social licence will likely increase.

However, it is important to note that the value of keeping some personal information protected, and the value of it being known, is almost entirely context-dependent – which is why analysing specific factors that influence people’s willingness to share their personal health data, and their approval of specific services or activities, becomes complex. Additionally, apart from being context-dependent, what constitutes sensitive information differs across individuals. For instance, a healthy, unemployed individual may flaunt his or her active lifestyle on social media, but hide the unemployment status to avoid shame; while the reverse may be true for the affluent manager who was just diagnosed with a sexually transmitted disease (Acquisti, Taylor and Wagman 2016).

Thus, there exist many shades of grey between the polar extremes of absolute sharing and complete protection of personal data; rather, it is possible to selectively protect or disclose different types of personal information, in order to optimise privacy trade-offs for individuals and society as a whole (Acquisti, 2014). Moreover, as researchers have presented a variety of techniques that can be used to re-identify personal data – solving privacy concerns through anonymising or de-identifying personal data becomes problematic. Anonymised and de-identified data also come with other concerns, such as making it harder to replicate results and link datasets, which will also limit the potential benefits that can be drawn from the health data (Daries, et al. 2014).

Drawing on the current state of the literature, it becomes clear that personal information, when shared, can become a public good whose analysis can reduce inefficiencies, inequalities and increase economic welfare (Acquisti, 2014). However, when misused, it can lead to transfer of economic wealth from data subjects to data holders, which would challenge both the potential value, the individual’s trust in a certain organisation, and the principle of inclusion⁸ – in saying that, all parts of society should have the opportunity to benefit from data use.

As noted by the New Zealand Minister of Finance, Bill English; one way to support social licence and counteract the possibility of exploitation is to improve data access by establishing citizen level control of how data is used. Increased control can be given in the form of consent – giving the individuals the possibility to opt-in or opt-out of sharing all or some of

⁸ The benefits and concerns raised across the literature relate to the four principles of data sharing and use developed by Data Futures Forum: value, inclusion, trust and control. In the context of sharing individual health data, value refers to the individual and societal benefit that would be derived from disclosing individual health data. Inclusion refers to that all parts of society should have the opportunity to benefit from data use. Trust relates to an individual’s confidence in the entities that will use the data, whereas control denotes the importance of the individual’s ownership of the data (Data Futures Partnership 2016).

their personal health data. In effect, this will shift the decision making on the use of data from the agency to its owner (Ministry of Social Development 2016). However, the option of consent comes with other challenges, including the possibility of biased results—challenging research findings, and extrapolation to the wider population. Consequently, consent might lower the potential to maximise inclusion and the value of the data.

5.1 Areas for further research

As the concept of social licence is relatively new – in particular within the context of sharing personal health data – the current state of the literature covering this issue is somewhat sparse and incoherent. However, it is clear that the debate around the issues of social licence within a health context is emerging – both within New Zealand and internationally. Additionally, while not specifically mentioning the issue of social licence, the academic literature, media, and politicians have increasingly started to cover and discuss many areas related to social licence. Common topics include personal privacy and consent.

Within this report, the sources identified (both *directly* mentioning social licence issues and areas *related to* social licence) came largely from the academic literature. While the topics covered within the academic literature are often a reflection of what is debated in society, a more in-depth review of the political and media landscape is required.

Moreover, other areas where further research is needed include (Kshetri 2014, Kostkova, et al. 2016, Kennedy, Poell and Dijck 2015, Acquisti, 2010):

- Analysis of how privacy and social licence-related barriers have hindered organisations' big data initiatives, as well as how these issues could be addressed.
- How existing laws and regulations reflect the issues and concerns within the context of sharing personal health data.
- Explore which big data-related activities and processes (e.g. collection, storing, analysis, processing, reuse and sharing) are key concerns in a social licence context.
- Explore how conscious individuals are of the ways in which their data (generated through use of mobile phone applications, networks and social media) are technically steered, repurposed, and resold. The distinction between the 'technological unconscious' and the 'conscious user' becomes relevant here.
- Analysis of what motivates people to share their data, especially as many terms and conditions provide no opt-out options. This includes an analysis of underlying factors that make people join data sharing communities (e.g. the "quantified self" movement and datadonors.org).
- Better understanding of the type of externalities that are created by sharing personal health data. Examples of positive externalities may be that agencies can introduce niche health products that, without focused data about potentially interested consumers, might have been too risky to develop. Negative externalities may include spam and adverse price discrimination.

6. References

- Acquisti, Alessandro. "From the Economics of Privacy to the Economics of Big Data." 2014. <http://www.heinz.cmu.edu/~acquisti/papers/economics-big-data-acquisti-lane-book.pdf> (accessed 06 11, 2016).
- . "The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines." 2010. <http://www.oecd.org/sti/ieconomy/46968784.pdf> (accessed 06 29, 2016).
- Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. *The Economics of Privacy*. Durham, North Carolina: Sloan Foundation Economics Research Paper, 2016.
- Anuta, Joe. *Hudson Yards to be first 'quantified community'*. 2014. http://www.craigslist.com/article/20140414/REAL_ESTATE/140419932/hudson-yards-to-be-first-quantified-community (accessed 06 27, 2016).
- Bersin, Josh. *Quantified Self: Meet the Quantified Employee*. 2014. <http://www.forbes.com/sites/joshbersin/2014/06/25/quantified-self-meet-the-quantified-employee/#77453213216d> (accessed 06 27, 2016).
- Bipartisan Policy Center. "Meeting Proceedings: A Policy Forum on the Use of Big Data in Health Care." Washington, 2013.
- Blakesley, Ian R., and Anca C. Yallop. "Consumer Perceptions about Digital Privacy and Online Data Sharing in the UK Insurance Sector." International Conference "Marketing - from Information to Decision", 2015.
- Brack, Matthew, and Tito Castillo. *Data Sharing for Public Health: Key Lessons from Other Sectors*. Centre on Global Health Security, Chatham house, 2015.
- Bull, Susan, et al. "Best Practices for Ethical Sharing of Individual-Level Health Research Data From Low- and Middle-Income Settings." *Journal of Empirical Research on Human Research Ethics*, 2015: Vol. 10(3) 302–313.
- Calit2. *Personal Data for the Public Good*. Health Data Exploration project, California Institute for Telecommunications and Information Technology, 2014.
- Carter, Pam, Graeme T Laurie, and Mary Dixon-Woods. "The social licence for research: why care.data ran into trouble." *Journal of Medical Ethics*, 2015: 0:1–6.
- Chial, Heidi. *DNA Sequencing Technologies Key to the Human Genome Project*. 2008. <http://www.nature.com/scitable/topicpage/dna-sequencing-technologies-key-to-the-human-828> (accessed 06 16, 2016).
- Collins, Francis S. "Shattuck Lecture - Medical and Societal Consequences of the Human Genome Project." *The New England Journal of Medicine*, 1999.
- Conge, Sue, Joanne H. Pratt, and Karen D. Loch. "Personal information privacy and emerging technologies." *Info Systems Journal* 23 (2013): 401-417.

- Council of Canadian Academies. *Accessing Health and Health-Related Data in Canada*. Ottawa : The Expert Panel on Timely Access to Health and Social Data for Health Research and Health System Innovation, Council of Canadian Academies, 2015.
- Daries, Jon, et al. "Quality social science research and the privacy of human subjects requires trust." *acmqueue* 12, no. 7 (2014).
- Data Futures Partnership. "Framework & Topic Selection." 2016.
- Data Futures Partnership. *Social license literature review*. Wellington: DFP WG Social license workshop 28 Jan 2016, 2016.
- DataDonors. *What is datadonors?* n.d. <http://datadonors.org/> (accessed 06 27, 2016).
- Edwards, Annabel. *Companies are using big data to track employee health and pregnancies*. 2016. <http://www.popsci.com/companies-use-big-data-to-track-employee-health-and-pregnancies> (accessed 06 27, 2016).
- Gluckman, Sir Peter. "The intended and unintended consequences of e-research: why scientists must engage openly with the community." *E-Research 2020 Workshop, office of the prime minister's chief science advisor*. Wellington, 2015.
- Groves, Peter, Basel Kayyali, David Knott, and Steve Van Kuiken. *The 'big data' revolution in healthcare*. McKinsey&Company, 2013.
- Health Information Privacy. "Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524." *U.S. Department of Health & Human Services*. n.d. <http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/> (accessed 06 29, 2016).
- Heath Information and Quality Authority. *International Review of Secondary Use of Personal Health Information*. Dublin: Health Information and Quality Authority, 2012.
- Heitmueller, Axel, Sarah Henderson, Will Warburton, Ahmed Elmagarmid, Alex Pentland, and Ara Darzi. "Developing Public Policy To Advance The Use Of Big Data In Health Care." *Health Affairs* 33, no. 9 (2014): 1523-1530.
- Hoffman, Sharona. "Citizen Science: The Law and Ethics of Public Access to Medical Big Data." *Berkeley Technology Law Journal* 30, no. 3 (2015).
- Hunter, I.M., R.J. Whiddett, A.C. Norris, B.W. McDonald, and J.A. Waldon. "New Zealanders' attitudes towards access to their electronic health records: preliminary results from a national study using vignettes." *Health Informatics J* (Health Informatics J) 15, no. 3 (2009): 212-28.
- Indiana State Department of Health. *About*. 2014. <http://www.in.gov/laboroflove/666.htm> (accessed 06 16, 2016).
- IPSOS MORI. *New research finds data trust deficit with lessons for policymakers*. 2014. <https://www.ipsos-mori.com/researchpublications/researcharchive/3422/New-research-finds-data-trust-deficit-with-lessons-for-policymakers.aspx> (accessed 06 08, 2016).

- Kennedy, Helen, Thomas Poell, and Jose van Dijck. "Data and Agency." *Big Data & Society*, 2015: 1-7.
- Kitova, Margarita. *The Growing Trend Of Clinical Research Crowdsourcing*. 15 09 2015.
<http://www.openhealthnews.com/articles/2015/growing-trend-clinical-research-crowdsourcing> (accessed 06 10, 2016).
- Klonoff, David. "Personalized Medicine for Diabetes." *Journal of Diabetes Science and Technology* 2, no. 3 (2008): 335-341.
- Kostkova, Patty, et al. "Who Owns the Data? Open Data for Healthcare." *Frontiers in Public Health*, February 2016.
- Kroft, Steve. *The Data Brokers: Selling your personal information*. 2014.
<http://www.cbsnews.com/news/data-brokers-selling-personal-information-60-minutes/> (accessed 11 06, 2016).
- Kshetri, Nir. "Big data's impact on privacy, security and consumer welfare." *Telecommunications Policy* 38 (2014): 1134-1145.
- Lazer, David, and Ryan Kennedy. *What we can learn from the epic failure of google flu trends*. 2015.
<http://www.wired.com/2015/10/can-learn-epic-failure-google-flu-trends/> (accessed 06 28, 2016).
- Li, Han, Ashish Gupta, Jie Zhang, and Rathindra Sarathy. "Examining the decision to use standalone personal health record systems as a trust-enabled fair social contract." *Decision Support Systems* 57 (2014): 376–386.
- Lupton, Deborah. "Health promotion in the digital era: a critical commentary." *Health Promotion International* 30, no. 1 (2014).
- Macnaughtan, Lorena, Gerardo Patriotta, Lorraine Pinnington, and Sujatha Raman. "Plurality of institutional logics in digital healthcare: The rise of the hybrid patient." ReserachGate, 2015.
- Meyer, Ralph R. *Human Genome Project - Ethical Issues*. n.d.
<http://medicine.jrank.org/pages/2412/Human-Genome-Project-Genomics-Proteomics.html> (accessed 06 16, 2016).
- Ministry of Social Development. *Speech from Hon Bill English, Deputy Prime Minister and Minister of Finance*. 2016. <https://www.msd.govt.nz/about-msd-and-our-work/newsroom/events/data-hui-2016/2016/speech-from-hon-bill-english-deputy-prime-minister.html> (accessed 06 14, 2016).
- Nature Biotechnology. "Incentivizing Data Donation." *Nature Biotechnology* 33 (2015): 885.
- Nimita, L., and I.B. Carol. "The Modern Social Contract between the Patient, the Healthcare Provider, and Digital Medicine." *Socialomics* 3, no. 1 (2014).
- Oxford Dictionaries. *Crowdsourcing*. 2016.
<http://www.oxforddictionaries.com/definition/english/crowdsourcing> (accessed 06 10, 2016).

- Parker, Michael, and Susan Bull. "Sharing Public Health Research Data: Toward the Development of Ethical Data-Sharing Practice in Low- and Middle-Income Settings." *Journal of Empirical Research on Human Research Ethics* Vol. 10(3) (2015): 217–224.
- Pickard, K. Thomas, and Melanie Swan. *Big Desire to Share Big Health Data: A Shift in Consumer Attitudes toward Personal Health Information*. MS Futures Group and DIYgenomics, 2014.
- QuantifiedSelf. *About Quantified Self*. n.d. <http://quantifiedself.com/about/> (accessed 06 27, 2016).
- Rainie, Lee, and Maeve Duggan. *Privacy and Information Sharing*. Pew Research Center, 2015.
- Ravindranath, Mohana. *In Indiana, state government tries using big data project to reduce infant mortality*. 2014. https://www.washingtonpost.com/business/on-it/in-indiana-state-government-tries-using-big-data-project-to-reduce-infant-mortality/2014/08/23/66d57bc0-2973-11e4-8593-da634b334390_story.html (accessed 06 16, 2016).
- Riboli, Elio. "The European Prospective Investigation into Cancer and Nutrition (EPIC): Plans and Progress." *The Journal of Nutrition* 131, no. 1 (2001): 1705-1755.
- Rittenberg, Libby, and Tim Tregarthen. "14.01SC Principles of Microeconomics." 2011. http://ocw.mit.edu/ans7870/14/14.01SC/MIT14_01SCF11_rtttext.pdf (accessed 06 29, 2016).
- Robbins, Rebecca. *Insurers want to nudge you to better health. So they're data mining your shopping lists*. 2015. <https://www.statnews.com/2015/12/15/insurance-big-data/> (accessed 06 27, 2016).
- Roski, Joachim, George W. Bo-Linn, and Timothy A. Andrews. "Creating Value In Health Care Through Big Data: Opportunities And Policy Implications." *Health Affairs* (Health Affairs) 33, no. 7 (2014): 1115-1122.
- Roski, Joachim, George W. Bo-Linn, and Timothy A. Andrews. "Creating Value In Health Care Through Big Data: Opportunities And Policy Implications." *Health Affairs* 33, no. 7 (2014): 1115-1122.
- Salas-Vega, Sebastian, Adria Haimann, and Elias Mossialos. "Big Data and Health Care: Challenges and Opportunities for Coordinated Policy Development in the EU." *Health Systems & Reform* 1, no. 4 (2015): 285-300.
- Sarasohn-Kahn, Jane. *Here's Looking at You: How Personal Health Information Is Being Tracked and Used*. California Health Foundation, 2014.
- Schaik, Tempest A. van, Nadezda V. Kovalevskaia, Elena Protopapas, Hamza Wahid, and Fiona G.G. Nielsen. "The need to redefine genomic data sharing: A focus on data accessibility." *Applied & Translational Genomics*, no. 3 (2014): 100-104.
- Scoop Media. *What do New Zealanders think about sharing their personal health data?* 2015. <http://www.scoop.co.nz/stories/GE1509/S00061/what-do-nz-ers-think-about-sharing-personal-health-data.htm> (accessed 06 08, 2016).

- Sedenberg, Elaine M., and Deirdre K. Mulligan. "Public Health as a Model for Cybersecurity Information Sharing." *Berkeley Technology Law Journal* 30, no. 3 (2015).
- Sedenberg, Elaine M., and Deirdre K. Mulligan. "Public Health as a Model for Cybersecurity Information Sharing." (Berkeley Technology Law Journal) 30, no. 3 (2015).
- Swan, Melanie. "Health 2050: The Realization of Personalized Medicine through Crowdsourcing, the Quantified Self, and the Participatory Biocitizen." *Journal of Personalized Medicine* 2 (2012): 93-118.
- The Center for Digital Government. *Big Data and Analytics*. Public CIO Special Report , 2015.
- The Economist. *The quantified self - Counting every moment*. 2012.
<http://www.economist.com/node/21548493> (accessed 06 16, 2016).
- . "Things are looking app." 12 03 2016.
<http://www.economist.com/news/business/21694523-mobile-health-apps-are-becoming-more-capable-and-potentially-rather-useful-things-are-looking> (accessed 06 12, 2016).
- The Palliative Care Council of New Zealand. *Sharing Patient Health Information: A review of health information privacy and electronic health records in New Zealand*. Cancer Control New Zealand , 2010.
- Vayena, Effy, Anna Mastroianni, and Jeffrey Kahn. "Caught in the Web: Informed Consent for Online Health Research." *Sci. Transl. Med.* 5, no. 173fs6 (2013).
- Vithiatharan, Rena N. "The potentials and challenges of big data in public health." *3rd Australian eHealth Informatics and Security Conference*. Edith Cowan University, 2014.
- Watson, Sara M. *You Are Your Data - And you should demand the right to use it*. 2013.
http://www.slate.com/articles/technology/future_tense/2013/11/quantified_self_self_tracking_data_we_need_a_right_to_use_it.html (accessed 06 16, 2016).
- Webster, Nick. *Plan to cut health fraud in UAE*. 2016.
<http://www.thenational.ae/uae/health/plan-to-cut-health-fraud-in-uae> (accessed 06 27, 2016).
- Whiddett, Richard, Inga Hunter, Judith Engelbrecht, and Jocelyn Handy. "Patients' attitudes towards sharing their health information." *International Journal of Medical Informatics* 75 (2006): 530-41.
- Yates, Brian F., and Celesa L. Horvath. "Social License to Operate: How to Get It, and How to Keep It." Pacific Energy Summit 2013, 2013.
- Young, Kerry. *Washington Health Policy Week in Review*. 2014.
<http://www.commonwealthfund.org/publications/newsletters/washington-health-policy-in-review/2014/jul/jul-14-2014/health-data-may-create-300-billion-in-efficiencies> (accessed 06 28, 2016).