JICLT
Journal of International Commercial Law and Technology
Vol.9, No.4 (2014)

# DATA MINING AND DATA MATCHING: REGULATORY AND ETHICAL CONSIDERATIONS RELATING TO PRIVACY AND CONFIDENTIALITY IN MEDICAL DATA

Thilla Rajaretnam*
Associate Lecturer, School of Law,
University of Western Sydney (UWS), NSW Australia,
E-mail: t.rajaretnam@uws.edu.au

**Abstract**. The application of data mining techniques to health-related data is beneficial to medical research. However, the use of data mining or knowledge discovery in databases, and data matching and profiling techniques, raises ethical concerns relating to consent and undermines the confidentiality of medical data. Data mining and data matching requires active collaboration between the medical practitioner and the data miner. This article examines the ethical management of medical data including personal information and sensitive information in the healthcare sector. It offers some ethical and legal perspectives on privacy and the confidentiality of medical data. It examines the international landscape of health information privacy protection, relevant Australian legislation and recommendations to improve the ethical handling of medical data proposed by the Australian Law Reform Commission.

**Key words:** Data mining, data matching, medical data, ethics, privacy, regulation

## 1 Introduction

Over recent decades concerns about health and the promotion of wellbeing has become of paramount importance to individuals and governments in all societies.[1] The World Health Organisation defines health as a 'state of complete physical, mental and social well-being and not merely the absence of disease or infirmity'.[2] Health has come to mean the attainment of a state of wellbeing and the attainment of physical fitness, and psychological stability. Protection of the body becomes synonymous with the protection of the self.[3] Individuals can experience feelings of deep violation of the self when the body is under threat, not only from disease but also when there is a profound sense of invasion of a sphere of their lives over which they have no control.[4] The principle of autonomy dictates that individuals deserve respect concerning the choices that they make, both about what happens to their bodies and, in the modern world, to their personal data.[5] The autonomy and dignity of individuals is recognised in the duty of confidentiality.[6] In the medical context, patient-related data has

---

* LLB (Hons) (Lond.), CLP (Malaysia), LLM (UWS), PhD (UWS).

[1] Laurie, Graeme (2002) *Genetic Privacy: A Challenge to Medical-legal Norms*, Cambridge University Press, p. 12.
[2] The World Health Organisation, *Constitution*, adopted by the International Health Conference held in New York from 19 June to 22 July 1946, signed on 22 July 1946 by the representatives of 61 States (*Off. Rec. Wld Hlth Org*., **2**, 100), and entered into force on 7 April 1948. Amendments adopted by the Twenty-sixth, Twenty-ninth, Thirty-ninth and Fifty-first World Health Assemblies (resolutions WHA26.37, WHA29.38, WHA39.6 and WHA51.23) came into force on 3 February 1977, 20 January 1984, 11 July 1994 and 15 September 2005 respectively and are incorporated in the present text.
[3] Laurie, Graeme (2002) *Genetic Privacy: A Challenge to Medical-legal Norms*, Cambridge University Press, p. 12.
[4] Danish Council of Ethics, (1993) *Ethics and Mapping the Human Genome* (Copenhagen, Notex) p. 52, as cited in Laurie, Graeme (2002) *Genetic Privacy: A Challenge to Medical-legal Norms*, Cambridge University Press, p.12.
[5] Laurie, Graeme (2002) *Genetic Privacy: A Challenge to Medical-legal Norms*, Cambridge University Press, p. 203.
[6] McMahon, Marilyn (2006) 'Re-thinking Confidentiality' in I Freckelton and K Petersen (eds), *Disputes and Dilemmas in Health Law*, Federation Press, p. 563, 579.

traditionally been recorded in doctors' surgeries and hospitals. This meant that patients knew exactly what information they had confided in their doctors, and doctors and hospitals, being bound by ethical and professional codes of conduct, maintained the confidentiality of patients' medical data.[7] Today, however, advances in information technology and particularly the use of innovative information-harvesting technologies mean that data collection generally has become almost indiscriminate. Some of these technologies are also being used in the medical sphere.

Two methods used by agencies and organisations to collect, process and analyse information are data matching and data mining.[8] Data matching is 'the large scale comparison of records or files …collected or held for different purposes, with a view to identifying matters of interest',[9] while data mining has been defined as 'a set of automated techniques used to extract buried or previously unknown pieces of information from large databases' about individuals from a number of unknown sources that may be unauthorised.[10] In the medical context, health service providers such as doctors and hospitals are using data matching and data mining technologies to monitor their patients' health. Medical researchers are also using such techniques. A growing e-health industry harvests medical data using sensing and monitoring technologies such as bio-sensing technology,[11] radio frequency identification ('RFID') technology[12] and smartphones.

Developments in information processing technologies, its use by healthcare providers and the handling of sensitive healthcare information by healthcare service providers have heightened patient concerns regarding privacy in the medical context.[13] For example the use of data mining and profiling techniques has raised concerns about the ethical collection, use and disclosure of data generally and the privacy and confidentiality of individuals' personal information, sensitive information and health information.[14] As government agencies and private sector organisations collect and store vast amounts of information generated by the everyday activities of individuals—for example, surfing the net or renting a car, using an ATM machine or a debit or credit card for purchases, using a Medicare card when visiting a doctor or hospital, having a prescription filled at the pharmacy or purchasing medication over the counter—these concerns arise in an ever wider context.

This article examines the ethical management of data including personal information, sensitive information and health information in the healthcare sector. It offers some ethical and legal perspectives on the privacy and confidentiality of medical data. The article then considers guidelines and conventions dealing with the privacy of medical information in the international sphere, the current situation under Australian law, and recommendations of the Australian Law Reform Commission for proposed law reform in relation to the ethical handling of medical data.

## 2 Data Matching and Data Mining in the Medical Context

[7] Laurie, Graeme (2002) *Genetic Privacy: A Challenge to Medical-legal Norms*, Cambridge University Press, p. 19.
[8] Australian Law Reform Commission, (2008) *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108), vol 1 p. 402.
[9] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108) (2008), vol 1 p. 402-4 [9.48]-[9.54]; Office of the Federal Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration: Guidelines* (1998), [14].
[10] Information and Privacy Commissioner Ontario, (1998) *Data Mining: Staking a Claim on Your Privacy*, p. 4.
[11] A biosensor is a detection device that combines a biological component with a physicochemical detector component. For example, the use by miners of a canary in a cage to warn of gas could be considered a biosensor. Many biosensor applications today similarly use organisms which respond to toxic substances at a much lower concentration than humans can detect to warn of the presence of the toxins. This technology has application in the healthcare, agri-food, environment and security sectors: <http://www.news-medical.net/health/Biosensors-What-are-Biosensors.aspx> (accessed 15 November 2013).
[12] Radio frequency identification is any method of identifying unique items using radio waves, most usually by means of a small electronic device consisting of a chip and an antenna.
[13] Laurie, Graeme (2002) *Genetic Privacy: A Challenge to Medical-legal Norms*, Cambridge University Press, p. 19.
[14] These terms are defined in s 6(1) of the *Privacy Act 1988* (Cth): for definitions see 5.2.1 of this article.

## 2.1 Technologies Used

Data matching and data mining technologies used to collect medical data include sensing and monitoring technologies such as RFID technology, bio-sensing technology and smartphone technology. The types of health information collected by health service providers using such technology include tracking pharmaceutical handling, assessing patients' medical condition—for example, blood pressure, heart rate and body temperature—and genetic information, and remote patient diagnostics.[15]

RFID tags use radio signals to wirelessly transfer information about the item to which the tag is attached, such as its movement and storage history. Pharmaceutical manufacturers, wholesalers, importers and distributors use RFID technology to trace and monitor the storage and transport of pharmaceutical products from the manufacturer to the distribution centre, retail point-of-supply and hospitals,[16] as required by the Australian Government's Therapeutic Goods Administration.[17]

Bio-sensing technology is used by medical centres to provide point-of-care health monitoring. Biosensors can be programmed to monitor a broad range of conditions, for example measuring specific components such as heart rate, body temperature and blood pressure, and to diagnose certain medical conditions. Through the use of bio-sensing technology, medical researchers are able to detect compounds or elements that may represent risks to human health.

In addition, developments in bio-sensing technology and the wide availability of smartphones have led to new smartphone-based medical tools.[18] Smartphones provide a convenient platform for mobile healthcare applications because of their sensing and diagnostic capabilities and ability to connect medical services to patients through mobile communications networks.[19] For example, an ultrasound probe with a USB interface can connect to a smartphone or laptop computer, improving access to medical technology through lower costs and portability.[20] Another advantage of using bio-sensing technology is that a patient's medical data can be collected from biosensors and forwarded to medical facilities and specialists for analysis in a click of the mouse.[21]

## 2.2 The Benefits

The benefit of using RFID tags over barcodes to monitor pharmaceutical handling is that while barcodes require line-of-sight scanning, RFID uses proximity sensing and may include smart tags to store extra data. With the use of RFID tags, large amounts of personal and sensitive data[22] can be organised, analysed and transmitted to health service providers quickly. RFID technology also assists pharmacists to monitor the pharmaceutical history of particular patients and to ensure that prescribed quantities and processes are met.[23]

Monitoring the health of patients locally and remotely has many benefits. The data collected from such monitoring assists in the early detection of adverse health conditions and helps health service providers to provide improved patient care and influence patients' behaviour to improve health.[24] Access to their own medical and DNA data assists individuals to make informed decisions about their health and lifestyle and can prevent future diseases. It is the nature of genetic disorders to reveal little about the future risk of the disorder, such as the likelihood of onset, date of onset or the severity of the affliction. DNA samples might reveal possible

---

[15] Australian Communications and Media Authority, (2011) *Sensing and Monitoring: Recent Developments*, p. 13.
[16] Australian Communications and Media Authority, (2011) *Sensing and Monitoring: Recent Developments*, p. 13.
[17] National Coordinating Committee on Therapeutic Goods, (2011) *Australian Code of Good Wholesaling Practice for Medicines in Schedules 2, 3, 4 and 8* <http://www.tga.gov.au/pdf/manuf-medicines-cgwp-schedule2-3-4-8.pdf> (accessed 12 September 2013).
[18] Australian Communications and Media Authority, (2011) *Sensing and Monitoring: Recent Developments*, pp. 15-16.
[19] Australian Communications and Media Authority, (2011) Sensing *and Monitoring: Recent Developments*, pp. 15-16.
[20] Australian Communications and Media Authority, (2011) *Sensing and Monitoring: Recent Developments*, pp. 15-16.
[21] Australian Communications and Media Authority, (2011) *Sensing and Monitoring: Recent Developments*, p. 13-14.
[22] Australian Communications and Media Authority, (2011) *Sensing and Monitoring: Recent Developments*, pp. 12-13.
[23] Australian Communications and Media Authority, (2011) *Sensing and Monitoring: Recent Developments*, p.13.
[24] Virone, G et al., (2006) *An Advanced Wireless Sensor Network for Health Monitoring*, Department of Computer Science, University of Virginia <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.64.7346> (accessed 12 September 2013).

future health benefits not only to the individual from whom the information was initially derived but also to related individuals. A person's knowledge of their genetic status allows them to make informed decisions, for example about future reproductive choices.[25]

As social regulator, employer, facilitator of choice and protector of its citizens from harm, the state has an interest in medical and genetic information. One of the primary ways the state protects individuals is by ensuring individuals are able to access basic public healthcare. Over recent years there have been a number of major initiatives by doctors, hospitals, the pharmaceutical industry and the Australian Government to create and develop electronic record systems. The creation of a national shared electronic health information system to store personal information on a central database has been initiated by the Government.[26]

While the application of data mining techniques to medical data can be beneficial to individuals, health service providers, the pharmaceutical industry, medical researchers and the state, the information collected is inherently connected to and part of, the private sphere of an individual's life. Use and disclosure of such information must ensure the privacy of individual data subjects is respected.

## 3 Considerations Relating to Ethical Principles, Privacy and Confidentiality in the Medical Context

### 3.1 Ethical Principles

Ethics serve to identify good, desirable or acceptable conduct and to provide reasons for those conclusions.[27] Ethical principles extend to all spheres of human activity. The application of ethical principles governs not just the interaction between doctor and patient and interactions in commerce, employment and politics, but all our interactions with each other and also our dealings with animals and the environment.

The purpose of medical ethical principles is to protect the welfare and rights of participants in the healthcare sector.[28] Ethical as well as legal duties are owed by health service providers such as doctors, hospitals, the pharmaceutical industry and the state, and medical researchers, to prevent the use of medical data for a purpose inconsistent with the purpose for which the data was provided.[29]

Data mining and data matching requires active collaboration between the medical practitioner and the data miner, and raises ethical concerns because often the personal and sensitive information about an individual being collected using data mining and data matching technologies may be used by health service providers and shared with unknown persons without the individual's knowledge or consent.[30] This in turn is a threat to the privacy and confidentiality of an individual's sensitive medical data.

### 3.2 Privacy

Gavison defines privacy as the right to limit 'the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention'; this requires 'secrecy, anonymity and solitude'.[31] A threat to a person's privacy is a threat to the integrity of the person,[32] and

---

[25] Evans, James P, Skrzynia, Cecile and Burke, Wylie (2001) The Complexities of Predictive Genetic Testing, vol. 322 *British Medical Journal* 1052.
[26] Australian Law Reform Commission, (2008) *For your Information: Australian Privacy Law and Practice* (ALRC Report 108) (2008) vol. 2, pp. 2045-52 [61.3]-[61.35].
[27] Commonwealth of Australia, (1999) National Health and Medical Research Council, *National Statement of Ethical Conduct in Research Involving Humans*, Preamble, p 1.
[28] *Guidelines for the Implementation of the Universal Declaration on the Human Genome and Human Rights* <http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/SHS/pdf/Guidelines-Genome_EN.pdf> (accessed 17 November 2013).
[29] Refer to [5.1] below.
[30] Australian Law Reform Commission, (2008) *For your Information: Australian Privacy Law and Practice* (ALRC Report 108) vol. 3, pp. 2013-37.
[31] Gavison, Ruth (1980) *Privacy and the Limits of Law*, vol. 89 (Issue 3) Yale Law Journal, pp. 421, 423.
[32] Fried, Charles (1968) *Privacy*, vol. 77 Yale Law Journal p. 475.

it is the right of each individual to protect his or her integrity and reputation by exercising control over information about them which reflects and affects their personality.[33] Those personality interests can be seriously compromised if individuals cannot control the disclosure or use of their personal information in cyberspace.[34]

Recognising the right of an individual to control such information enables that individual to selectively restrict others from his or her physical and mental state, communication and information,[35] and to control how he or she wishes to be presented, to whom and in what context.[36] This control enables an autonomous individual to make choices, and to select those persons to whom he or she will allow access to his or her body, home, decisions, communication, and information, and those to whom he or she will not allow access. In the context of medical data, this approach would give individuals the right to determine who obtains their medical data and for what purposes.[37] Clearly not all information of any kind would be subject to individual control. Much information in the public domain would not be considered private and subject to individual control, for example a person's status or profession.

But what are the boundaries and what purposes would be served by those limits? If control were limited to personal information of an intimate nature,[38] this would not extend to the vast array of information collected about individuals. Nor is the problem resolved by a broader and unbounded formulation of a right to control any information relating to the individual. An individual's ability to control disclosure of information about themselves is valued as a means of protecting personality rather than property interests. The capacity to control disclosure is seen an element of personal integrity, reputation, human dignity, expectations, autonomy and self-determination,[39] happiness and freedom. Control includes the ability to consent, to make decisions and choices whether to allow or disallow others into the individual's private space and to access information about them. Control over information is connected to how individuals want to be seen, to whom they want to be seen, and in what context.[40] The disclosure of those facts that are considered personal and intimate exposes and reveals an individual's vulnerability and psychological processes that are necessarily part of what it is to be human.

Consent is the expression of autonomy, the right of individuals to make decisions about how they will live their lives. When a person exercises their autonomy to make decisions concerning themselves, what is required?[41] The key elements to consent are: the individual must have the capacity to understand, provide and communicate their consent; the individual must be adequately informed; and the consent must be provided voluntarily.[42] Free and informed choice is an essential element of giving consent. Consent of the patient is required before the patient is subjected to any form of medical or surgical treatment. The rule is that a patient has an absolute right to decide what shall be done to his or her own body; to submit a person to any form of

---

[33] The duality of the concept of the right to privacy as both a part of and a protection for individual personality is more fully discussed by Warren, Samuel and Brandeis, Louis (1980) *The Right to Privacy*, 4 Harv L Rev 193, 194.
[34] Cohen, Julie (1991) *A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace* vol. 28 University of Connecticut Law Review p. 981.
[35] Westin, Alan (1967) *Privacy and Freedom,* Athenaeum Press, pp. 31-32; Moore, Adam D (2003) *Privacy: Its Meaning and Value,* vol. 40, (Issue 3) American Philosophical Quarterly p. 215; Moore, Adam D (2001) *Intellectual Property and Information Control: Philosophic Foundations and Contemporary Issues,* Transaction Publishing.
[36] Rossler, Beate (2005) *The Value of Privacy*, Polity Press, p. 116. Rossler writes that 'the reason why the protection of privacy matters so much is that it is an intrinsic part of self-understanding as autonomous individuals within familiar limits to have control over their self-presentation, that is control of how they want to be presented or stage themselves to whom they want to do so and in which context control over how they want to see themselves and how they want to be seen.'###NEED PAGE REF FOR QUOTE###
[37] Rossler, Beate (2005) *The Value of Privacy*, Polity Press.
[38] Fried, Charles (1968) *Privacy*, vol. 77 Yale Law Journal, pp. 475-77.
[39] Rossler, Beate (2005) *The Value of Privacy*, Polity Press, p. 129; Schoeman, Ferdinand D (ed), (1984) *Philosophical Dimensions of Privacy: An Anthology,* Cambridge University Press; Penny, Jonathan W, (2008) *Privacy and the New Virtualism*, vol. 10, (Issue 194) Yale Journal of Law & Technology, p. 56, 216.
[40] Greenawalt, Kent (1974) *Privacy and Its Legal Protections*, vol. 2 (Issue 3) Hastings Centre Studies p. 45; Rossler, Beate (2005) *The Value of Privacy,* Polity Press, p. 116.
[41] The principles set out are taken from Mappes, Thomas A and DeGazia, David, *Biomedical Ethics* (Mcgraw-Hill College, 4th ed, 1995) 25-29.
[42] National Health and Medical Research Council, (2004) *The Regulation of Health Information Privacy in Australia: A description and comment*, p 15 <http://www.nhmrc.gov.au/_files_nhmrc/publications/attachments/nh53.pdf>.

treatment without his or her consent is a trespass to the person for which damages may be recovered in a civil action.[43] This means that the patient has the right to give and withhold consent to medical treatment; the right to choose his or her own doctor; and the right to professional secrecy. Special care must also be taken when obtaining consent from those with special needs, those from non-English speaking backgrounds and young people.[44] The consent must be valid at law and the patient must be legally capable of giving consent.

In the context of medical data, a medical practitioner is obliged to obtain his or her patient's consent to be released from the obligation not to disclose to any third party information which was acquired because of the medical practitioner's professional relationship with the patient. The patient's consent is important to the medical practitioner and other health service providers because the consent process enables an individual considering whether or how to use medical data to make decisions with the best possible outcome for the patient.

### 3.3 Confidentiality

Confidentiality is concerned with the protection of a relationship, and with personal information. It extends to the security of personal information.[45] The ethical justification for the duty of confidentiality is found in the fundamental principles of our social values.[46] The moral and legal principles of individual autonomy require that personal and sensitive information such as medical data is confidential and to be respected.[47] Considerable utility may flow from respecting the confidentiality of medical data, as this can protect individuals from harm such as discrimination and stigmatisation resulting from the disclosure of personal information, whether sensitive information or otherwise. Keeping such information confidential fosters trust in relationships. Adhering to an autonomy model requires respect for the patients themselves and their interests, including their interests in personal information.[48] Protecting the confidentiality of an individual's personal information is to respect the individual.

In addition to moral principles and social values, a legal duty of confidentiality may arise in equity, at common law and under contract.[49] Health service providers may also be subject to confidentiality provisions in professional codes of conduct.

## 4 Threats to Privacy and Confidentiality of Medical Data

There are many ways in which the providers of modern healthcare and machines of modern medicine can invade privacy in the collection of medical data. First, states have created an array of government patient-tracking systems and are building health profiles of individuals from birth to death.[50] A national shared electronic health information system in Australia will facilitate access by a range of health service providers to electronic health information. With many modern medical instruments, despite the efforts of health service providers it is unlikely that the data subject knows at the outset exactly what type of personal and sensitive information is being collected about them, nor how the information is intended to be used. The data collected may be personal and highly sensitive information such as genetic information. Secondly, when bio-sensing, RFID and smartphone technologies are used to collect information, the patient is probably not aware of the vast

[43] Burton, Arthur W (1997) *Medical Ethics and the Law*, Australasian Medical Publishing Company Ltd. Glebe, p 35.
[44] National Health and Medical Research Council, (2000) *Ethical Aspects of Human Genetic Testing: an Information Paper,* p 39 [3.4].
[45] Laurie, Graeme (2002) *Genetic Privacy: A Challenge to Medical-legal Norms*, Cambridge University Press, p. 212.
[46] Laurie, Graeme (2002) *Genetic Privacy: A Challenge to Medical-legal Norms*, Cambridge University Press, p. 213.
[47] See Ngwena, C and Chadwick, R , 'Genetic Diagnostic Information and the Duty of Confidentiality' Med law Int. (1993) 1 (1A) pp. 73-95, 74 as cited in Laurie, Graeme (2002) *Genetic Privacy: A Challenge to Medical-legal Norms*, Cambridge University Press, p. 213.
[48] Laurie, Graeme (2002) *Genetic Privacy: A Challenge to Medical-legal Norms*, Cambridge University Press, p. 214.
[49] Laurie, Graeme (2002) *Genetic Privacy: A Challenge to Medical-legal Norms*, Cambridge University Press, p. 214.
[50] Citizens' Council for Health Freedom, '50-State Report Unveiled: States Track Medical Data from Birth to Death Without Consent', <http://www.cchfreedom.org/cchf.php/802> (accessed on 23 August 2013); Martin Evans, 'DNA databases created from babies' blood samples' The Telegraph, 23 May 2010 (online) <http://www.telegraph.co.uk/health/7756320/DNA-database-created-from-babies-blood-samples.html> (accessed 21 September 2013).

array of patient-tracking and state surveillance systems this information could be entered into to track them and potentially also their children. The data subject is not able to consent at the time the information is being collected to data matching and data mining that may subsequently occur, particularly if bio-sensing, RFID and/or smartphone technologies are used in the collection of the information. Patient consent to collection and use of their data is typically not required, although dissent is sometimes permitted. If there is not enough information given to the patient prior to collection of the data, the patient is not able to make meaningful choices about the collection, use and sharing of their personal information with others. Once medical data is collected the data subject loses control over their personal information. The public enterprise of the healthcare activity takes away from the patient control of his or her environment and personal and genetic data. Individuals may have difficulties accessing their own health information, especially those who wish to transfer their medical records to another medical practitioner.[51]

Secondly, computerised databanks facilitate not only the rapid processing of digital medical data, but also data matching and the manipulation of medical data.[52] In most cases the medical data collected and stored in databases is meaningless in the absence of context, as in the case of conventional data derived from bio-sensing technology or DNA samples. The establishment of genetic databanks in particular represents significant harm to personal and sensitive information about individuals. Raw data is intelligible only to highly trained individuals,[53] but unlike conventional health data, DNA is a unique marker pointing the way to a single individual. DNA-based genetic information cannot be completely anonymised.[54] There are also concerns that biometric technologies such as facial recognition technologies may be used to identify individuals without their consent.[55] The information collected can be used to discover profoundly personal attributes of an individual's life, invading the person's private sphere and family identity and adversely affecting their opportunities for education, employment and insurance.

Thirdly, the information collected into central databases is sourced from a number of agencies and organisations and may be inaccurate or incomplete,[56] and if individuals are not able to correct inaccurate and incomplete medical data about themselves there is the risk that an individual may be evaluated based on inaccurate and incomplete data. Such information may also be misused. For example, the state or other employers may be making use of genetic testing to create profiles of individuals so as to ensure that at-risk individuals are not placed in dangerous situations.[57] The profiling of individuals based on their medical or DNA data can affect families and ethnic groups that share genetic similarities. Access to such profiles may lead to discrimination or the restriction of employment opportunities. Insurance companies have a financial interest in personal data and some forms of genetic information as this helps them to better assess risks and premiums.[58]

In sum, privacy is a fundamental principle of healthcare and underpins quality healthcare. Ethical and legal duties of confidentiality are owed by all health service providers such as doctors, nurses and pharmacists, and by medical researchers. While privacy and the duty of confidentiality are not absolute, it is in the public interest to foster a relationship of trust and confidence between health service providers and those seeking health services. If there is no assurance to individuals that their medical data will remain private and confidential, it is likely that

[51] Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice (ALRC Report 108) (2008), p. 2015.
[52] Laurie, Graeme (2002) *Genetic Privacy: A Challenge to Medical-legal Norms*, Cambridge University Press, p. 108-9.
[53] Laurie, Graeme (2002) *Genetic Privacy: A Challenge to Medical-legal Norms*, Cambridge University Press, p. 108.
[54] Gostin, Lawrence O, (1995) *Genetic Privacy* (1995) vol. 3 (Issue 4), The Journal of Law, Medicine & Ethics p. 320-30, 322.
[55] Australian Law Reform Commission, (2008) *For Your Information: Australian Privacy Law and Practice, Biometric Information* [6.109-6.113], [9].
[56] Australian Law Reform Commission, (2008) For your Information: Australian Privacy Law and Practice (ALRC Report 108) (2008) vol 1, p. 402.
[57] Laurie, Graeme (2002) *Genetic Privacy: A Challenge to Medical-legal Norms*, Cambridge University Press, p. 127-29.
[58] Laurie, Graeme (2002) *Genetic Privacy: A Challenge to Medical-legal Norms*, Cambridge University Press, p. 129.

individuals may not seek healthcare,[59] being reluctant to disclose their medical condition for fear of being stigmatised when their medical data is revealed to others.[60]

## 5 Ethical and Legal Obligations Governing the Collection, Use and Disclosure of Medical Data

### 5.1 Codes of Ethics and Guidelines

The Hippocratic Oath which was formulated in the 5th century BC forms the basis of what is considered to be proper professional behaviour of physicians. Since the time of its formulation, physicians have been guided by its principles in imposing upon themselves codes of medical ethics. The principle of confidentiality between practitioner and patient in the Hippocratic Oath is in one translation expressed as follows: 'I will keep silent on that which I hear or see in the course of treatment or in everyday life which should not be repeated, holding such to be a secret'.[61] The modern equivalent of the Hippocratic Oath is contained in the Declaration of Geneva adopted by the World Medical Association in 1948.[62] In the Declaration of Geneva the principle relating to confidentiality between practitioner and patient is stated in terms that 'I will respect the secrets that are confided in me, even after the patient has died'. The World Medical Association subsequently adopted the International Code of Medical Ethics in 1949, and this restates the principle of confidentiality between practitioner and patient in the following terms:

> A physician shall respect a patient's right to confidentiality. It is ethical to disclose confidential information when the patient consents to it or when there is a real and imminent threat of harm to the patient or to others and this threat can be only removed by a breach of confidentiality.[63]

This formulation clearly acknowledges that the principle of confidentiality between practitioner and patient is not absolute. The Australian Medical Association's Code of Ethics expresses the principle of confidentiality between practitioner and patient as follows:

> Maintain your patient's confidentiality. Exceptions to this must be taken very seriously. They may include where there is a serious risk to the patient or another person, where required by law, where part of approved research, or where there are overwhelming societal interests.[64]

This formulation further specifies that not only real risks to the health of the patient or others may override the principle of confidentiality, but also the law and the public interest, for example in approved research.

International awareness of respect for ethical codes in research involving human participation is a recent phenomenon, accelerated in response to revelations of unethical practices during the Second World War. The judgment of the Nuremberg military tribunal on war crimes contained a set of principles and standards relating to permissible medical experiments. Since referred to as the Nuremberg Code, these have significantly influenced the subsequent development of codes of ethics. Some of these include the Declaration of Helsinki: Ethical Principles for Medical Research Involving Human Subjects adopted by the World Medical Association

---

[59] Commonwealth of Australia, (1999) National Health and Medical Research Council, *National Statement of Ethical Conduct in Research Involving Humans*, p 52-53.
[60] Laurie, Graeme (2002) *Genetic Privacy: A Challenge to Medical-legal Norms*, Cambridge University Press, p. 145.
[61] Burton, Arthur W, (1979) *Medical Ethics and the Law*, (1979, 3rd ed.) Australian Medical Publishing Company Ltd, Glebe, NSW p 28.
[62] World Medical Association, *Declaration of Geneva* <http://www.wma.net/en/30publications/10policies/g1/> (accessed 17 November 2013).
[63] World Medical Association ('WMA'), *International Code of Medical Ethics* adopted by the 3rd General Assembly of the WMA, London, England, October 1949 and amended by the 22nd World Medical Assembly, Sydney, Australia, August 1968; the 35th World Medical Assembly Venice, Italy, October 1983; and the 57th WMA General Assembly, Pilanesberg, South Africa, October 2006 <http://www.wma.net/en/30publications/10policies/c8/index.html> (accessed 17 November 2013).
[64] Australian Medical Association, *AMA Code of Ethics* 2004 editorially revised 2006 <https://ama.com.au/codeofethics> (accessed 17 November 2013).

in 1964,[65] the World Health Organisation's Proposed International Guidelines on Ethical Issues in Medical Genetic Services,[66] and UNESCO's Guidelines for the Implementation of the *Universal Declaration on the Human Genome and Human Rights*.[67] In Australia, the National Statement on Ethical Conduct in Human Research 2007 (updated May 2013) provides for codes of ethical principles relating to research involving humans.[68] Such documents demonstrate a trend towards making more explicit the ethical standards which must be met if research on humans is to be ethically acceptable.

Despite the development and emergence of ethical codes of practice, there are incidents of unethical medical data collection and the treatment of people in health research continues to occur.[69] The modern use of data matching and data mining technologies raises ethical concerns at the undermining of the privacy and confidentiality of patients' medical data. This means that continuing revision of ethical standards is necessary.

### 5.2 International Covenants and Conventions

Privacy is today recognised as a fundamental human right protected by international conventions and covenants such as the *Universal Declaration of Human Rights* ('*UDHR*')[70] and the *International Covenant on Civil and Political Rights* ('*ICCPR*').[71] Such covenants impose an obligation to ensure adequate and effective protection against the violation of privacy interests. In recent years access to medical information has also become a subject for international conventions. For example, the Council of Europe's *Convention for the Protection of Human Rights and Dignity of Human Being with Regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine*, Chapter III, Article 10 states that:

1. Everyone has the right to respect for private life in relation to information about his or her health.
2. Everyone is entitled to know any information collected about his or her health. However, the wishes of individuals not to be so informed shall be observed.
3. In exceptional cases, restrictions may be placed by law on the exercise of the rights contained in paragraph 2 in the interest of the patient.[72]

### 5.3 Australian Law

In Australia, there is no common law right to privacy. The Australian Federal Parliament has the power to make laws with respect to matters relating to Australia's obligations under bona fide international treaties and

---

[65] World Medical Association, *Declaration of Helsinki: Ethical Principles for Medical Research Involving Human Subjects* <http://www.wma.net/en/30publications/10policies/b3/> (accessed 17 November 2013).
[66] World Health Organisation, *Proposed International Guidelines on Ethical Issues in Medical Genetic Services* (1997), WHO/HGN/GL/ETH/98.1.
[67] *Guidelines for the Implementation of the Universal Declaration on the Human Genome and Human Rights* <http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/SHS/pdf/Guidelines-Genome_EN.pdf> (accessed 17 November 2013).
[68] National Health and Medical Research Council, Australian Research Council and Australian Vice-Chancellors' Committee, *National Statement on Ethical Conduct in Human Research 2007 (updated May 2013)* <http://www.nhmrc.gov.au/_files_nhmrc/publications/attachments/e72_national_statement_130813.pdf> (accessed 17 November 2013).
[69] Commonwealth of Australia, (1999) National Health and Medical Research Council, *National Statement on Ethical Conduct in Research Involving Humans*, p. 2.
[70] *Universal Declaration of Human Rights* adopted by General Assembly resolution 217A (III) of 10 December 1948. Article 12 of the *UDHR* provides that: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'
[71] *International Covenant on Civil and Political Rights* adopted and open for signature, ratification and accession by United Nations General Assembly resolution 2200A [XX1] of 16 December 1966 (entry into force 23 March 1976). Article 17 of the *ICCPR* provides that: '1. No one shall be subject to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.'
[72] The Convention was adopted by the Committee of Ministers on 19 November 1996 (reference DIR/JUR (96) 14), and opened for signature in Oviedo, April 1997.

agreements, or customary international laws. The primary federal privacy protection law is the *Privacy Act 1988* (Cth) ('*Privacy Act*'). This provides for the lawful collection, use and disclosure of personal, sensitive and health information in the Commonwealth public sector and in private sector organisations that fall within the scope of the Act.

All States and Territories have legislation regulating information privacy protection in their public sectors.[73] As noted above, information privacy in the Australian private sector generally is regulated by the *Privacy Act*, however three jurisdictions—the Australian Capital Territory, New South Wales and Victoria—have enacted legislation that additionally protects the privacy of health information in their private sectors, respectively the *Health Records (Privacy and Access) Act 1997* (ACT), the *Health Records and Information Privacy Act 2002* (NSW), and the *Health Records Act 2001* (Vic). In these jurisdictions, the difficulty facing handlers of health information is that both the *Privacy Act* and the local legislation apply. If they are not identical, the task of ensuring compliance with both statutes may be complex or onerous. In fact, there are limitations and inconsistencies in these statutes that do make the task of health service providers in these jurisdictions more difficult to comply with the *Privacy Act* and state legislation. The following section examines some of these inconsistencies and limitations.

### 5.3.1 *Privacy Act 1988* (Cth)

The *Privacy Act* sets out minimum standards or obligations in relation to the collection and handling of personal information in the Commonwealth public sector[74] and in the private sector.[75] The obligations on the public sector are set out in 11 Information Privacy Principles ('IPPs'),[76] while the minimum standards for the private sector are contained in ten National Privacy Principles ('NPPs')[77] which are broadly based on the eight principles in the Organisation for Economic Cooperation and Development's *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*.[78] The NPPs set minimum standards for the collection and handling, use and disclosure of personal information about individuals by organisations (including individual health service providers and medical researchers), and the sharing of such information with third parties, data security, transfer of personal information, and transborder flows of personal information. An organisation must comply with an approved privacy code or with the NPPs.[79] An act or practice of an organisation that breaches an approved privacy code that binds the organisation or, if the organisation is not bound by an approved privacy code, breaches a NPP, in relation to 'personal information' relating to an individual is an interference with the privacy of that individual.[80]

'Personal information' is defined as:

---

[73] This article does not consider other state legislation. For a summary of applicable legislation see National Health and Medical Research Council, (2004) *The Regulation of Health Information Privacy in Australia: A description and comment*, pt 5<http://www.nhmrc.gov.au/_files_nhmrc/publications/attachments/nh53.pdf>.
[74] The definition of 'agency' in s 6(1) of the *Privacy Act 1988* (Cth) largely corresponds to the Commonwealth public sector.
[75] The scope of the application of the *Privacy Act* to the private sector is determined by its definitions of 'organisation', 'sensitive information' and 'health information'. The definition of 'organisation' in *Privacy Act 1988* (Cth) s 6C corresponds, with some exceptions, to the private sector.
[76] Agencies are to comply with the IPPs set out in *Privacy Act 1988* (Cth) s 14, and an act or practice engaged in by an agency that breaches an IPP in relation to personal information relating to an individual is an interference with the privacy of that individual: *Privacy Act 1988* (Cth) ss 16, 13(a).
[77] See *Privacy Act 1988* (Cth) sch 3.
[78] Organisation for Economic Cooperation and Development, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 23 September 1980 <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>. The NPPs are similar but not identical to the fair information principles in the OECD Guidelines.
[79] *Privacy Act 1988* (Cth) s 16A(1)-(2), pt IIIA (Approved Privacy Codes).
[80] *Privacy Act 1988* (Cth) s 13A(1)(a)-(b).

> information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.[81]

Information about a person does not qualify as personal information under the *Privacy Act* unless the identity of the individual is apparent or can be reasonably ascertained. Further, the *Privacy Act* applies only to the collection of personal information for inclusion in a record or generally available publication, and only to collected personal information if it is held by an organisation in a record.[82] In general terms a 'record' means a document or database, but does not include a generally available publication; anything kept in a library, art gallery or museum for the purposes of reference; or Commonwealth records such as those in the National Archives of Australia or Australian War Memorial.[83] A distinction is thus made between personal information in records and in the public record.

The *Privacy Act* excludes from its protection certain categories of personal data that can identify or be linked to an individual. Where an individual's identity is apparent or can reasonably be ascertained from biometric information such as genetic information then such biometric information can be 'personal information for the purposed of the *Privacy Act*.[84] The definition of a record excludes personal information in the public record. Yet public documents and records can include personal information and sensitive information such as, for example, a list of names and addresses that may identify an individual.[85]

Some personal information is additionally considered to be 'sensitive information', defined as follows:

> (a) information or an opinion about an individual's:
> (i) racial or ethnic origin; or
> (ii) political opinions; or
> (iii) membership of a political association; or
> (iv) religious beliefs or affiliations; or
> (v) philosophical beliefs; or
> (vi) membership of a professional or trade association; or
> (vii) membership of a trade union; or
> (viii) sexual preferences or practices; or
> (ix) criminal record;
> that is also personal information; or
> (b) health information about an individual; or
> (c) genetic information about an individual that is not otherwise health information.[86]

---

[81] *Privacy Act 1988* (Cth) s 6(1) (definition of 'personal information').
[82] *Privacy Act 1988* (Cth) s 16B.
[83] *Privacy Act 1988* (Cth) s 6(1) ('record means (a) a document; or (b) a database (however kept); or (c) a photograph or other pictorial representation of a person; but does not include: (d) a generally available publication; or (e) anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition; or (f) Commonwealth records as defined by subs 3(1) of the *Archives Act 1983* (Cth) that are in the open access period for the purposes of that Act; or (fa) records (as defined in the *Archives Act 1983*) in the care (as defined in that Act) of the National Archives of Australia in relation to which the Archives has entered into arrangements with a person other than a Commonwealth institution (as defined in that Act) providing for the extent to which the Archives or other persons are to have access to the records; or (g) documents placed by or on behalf of a person (other than an agency) in the memorial collection within the meaning of the *Australian War Memorial Act 1980*; or (h) letters or other articles in the course of transmission by post').
[84] Australian Law Reform Commission, (2008) *For Your Information: Australian Privacy Law and Practice, Biometric Information* [6.109-6.113], [9].
[85] *Archives Act 1983* (Cth) s 3 defines 'record' to mean a document, or an object, in any form (including any electronic form) that is, or has been, kept by reason of: (a) any information or matter that it contains or that can be obtained from it; or (b) its connection with any event, person, circumstance or thing. *Acts Interpretation Act 1901* (Cth) s 25 defines 'document' to include: (a) any paper or other material on which there is writing; (b) any paper or other material on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; and (c) any article or material from which sounds, images or writings are capable of being reproduced with or without the aid of any other article or device; and 'record' includes 'information stored or recorded by means of a computer'.
[86] *Privacy Act 1988* (Cth) s 6(1) (definition of 'sensitive information').

Additional requirements must be met in relation to the collection by organisations of sensitive information and of health information.[87] The *Privacy Act* defines 'health information' as:

> (a) information or an opinion about:
> (i) the health or a disability (at any time) of an individual; or
> (ii) an individual's expressed wishes about the future provision of health services to him or her; or
> (iii) a health service provided, or to be provided, to an individual;
> that is also personal information; or
> (b) other personal information collected to provide, or in providing, a health service; or
> (c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or
> (d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.[88]

It is suggested that the definitions of personal information and sensitive information in the *Privacy Act* are too narrow. As noted above, the *Privacy Act* only protects personal information about an individual if the identity of the individual is apparent or can be reasonably ascertained. It is suggested that the definition of personal information be extended to cover identifiers, irrespective of whether it is obvious to the collector or discloser of the information that an individual's identity can reasonably be ascertained from that identifier and/or whether or not an individual can be contacted by use of the identifier.[89] This would cover DNA identifiers. It is difficult to establish categories of information which are universally considered to be 'sensitive' because of the nature of the information, the context in which it is handled, and how it is viewed by persons to whom the information relates.[90] It is also suggested that personal health information requires a high level of protection. The ALRC has proposed that the definition of health information in the *Privacy Act* be amended to make express reference to information or opinion about the physical, mental or psychological health or disability of individuals and include genetic information.[91]

The NPPs provide that the data subject's consent is required to the collection, use or disclosure of personal information for a purpose other than the primary purpose of collection,[92] the data subject's consent is required. Such consent may be express or implied.[93] The data subject's consent is required prior to the collection of sensitive information[94] unless the exceptions under NPP10 apply.[95] It is important to note that the consent of the healthcare recipient is not required for a unique healthcare identifier to be assigned.[96] Researchers are permitted to obtain and use personal information for health and medical research without the consent of the individuals concerned where this is approved by a Human Research Ethics Committee ('HREC').[97] To give its approval, a HREC must have concluded that the public interest in the use and disclosure of health information for the purposes of research or the compilation or analysis of statistics relevant to public health or public safety

---

[87] *Privacy Act 1988* (Cth) sch 3 NPP 10.
[88] *Privacy Act 1988* (Cth) s 6(1) (definition of 'health information'). See also *Privacy Act 1988* (Cth) s 6(1) (definition of 'health service').
[89] For identifiers see *Privacy Act 1988* (Cth) sch 3 NPP 7.
[90] Australian Law Reform Commission, (2008) For Your Information: Australian Privacy Law and Practice (2008): *The Privacy Act- Some Important Definitions – Sensitive information,* p. 316 [6.88].
[91] Australian Law Reform Commission, (2008) For Your Information: Australian Privacy Law and Practice (2008): Key Recommendations for Health Information Privacy Reform, Recommendation 62-1, [62.01]- [62.20], p.
[92] *Privacy Act 1988* (Cth) sch 3 NPP 2.1(b).
[93] *Privacy Act 1988* (Cth) s 6(1) (definition of 'consent').
[94] *Privacy Act 1988* (Cth) sch 3 NPP 10.1(a).
[95] *Privacy Act 1988* (Cth) sch 3 NPP 10.1(a)-(e), 10.3
[96] *Healthcare Identifiers Act 2010* (Cth) s 9(4); See also National Statement on Ethical Conduct in Human Research 2007 (updated May 2013).
[97] *Privacy Act 1988* (Cth) s 95A(2), sch 3 NPP 2.1(d)(ii); National Health and Medical Research Council, *Guidelines approved under Section 95A of the Privacy Act 1988* (2001), A.1.4 <http://www.comlaw.gov.au/Details/F2008B00222> (accessed 17 November 2013).

substantially outweighs the public interest in maintaining the level of privacy protection afforded by the NPPs, but even where the HREC has concluded that the balance of the public interests is in favour of use or disclosure, the organisation that collected the information may decline to use or disclose the information.[98] It is suggested that the *Privacy Act* require that consent to the use of sensitive and health information, and the collection of personal information, be express rather than implied.

The *Privacy Act* applies to non-exempt data collectors.[99] These include all private sector organisations with an annual turnover of more than $3m,[100] health service providers,[101] and contractors to the Australian Government so far as their activities are for the purposes of the contract.[102] It is suggested all data collectors should be required to comply with the *Privacy Act*, as exemptions for particular groups of data collectors limit its scope. For example, where small businesses with an annual turnover of less than $3m are involved in the collection and use of personal, sensitive and medical data, this data is not currently protected under the *Privacy Act* since small businesses are exempt under the *Privacy Act.*

### 5.3.2 State Legislation

As noted above, the current regulation involve a patchwork of federal and state and territory laws, official guidelines and personal and professional ethics, institutional restraints etc. [103] The Australian Capital Territory, New South Wales and Victoria have enacted specific legislation to protect the privacy of health information: the *Health Records (Privacy and Access) Act 1997* (ACT), the *Health Records and Information Privacy Act 2002* (NSW) and the *Health Records Act 2001* (Vic) respectively. Under this legislation, health information[104] is treated as a subset of 'sensitive information' under the *Privacy Act*.[105] Each statute contains a different set of Health Privacy Principles ('HPPs')—for example, the *Health Records (Privacy and Access) Act 1997* (ACT) provides for 14 privacy principles modified to suit the requirements of heath records; the *Health Records and*

---

[98] Office of the Privacy Commissioner (2009) *Synopsis of Australian Government response to ALRC Report 108 – Health Services & Research (Part H)* at <www.pmc.gov.au/privacy/alrc.cfm> (accessed 20 September 2013); Australian Law Reform Commission, (2008) *For Your Information: Australian Privacy Law and Practice*; Australian Law Reform Commission, (2011) *Key Recommendations for Health Information Privacy Reform* <http://www.alrc.gov.au/news-media/2011/australian-privacy-law-practice-key-recommendations-health-information-privacy-refor> (accessed 20 September 2013).

[99] *Privacy Act 1988* (Cth) ss 13A–13D provide for those organisations that are exempt.

[100] *Privacy Act 1988* (Cth) ss 6C, 6D. Businesses with an annual turnover of $3 million or less are bound by the NPPs in certain circumstances, such as when a business discloses personal information about an individual for a benefit, service or advantage: *Privacy Act 1988* (Cth) s 6D(4).

[101] *Privacy Act 1988* (Cth) s 6D(4)(b) provides that the NPPs apply to private sector organisations holding health information and providing a health service that might otherwise be exempt from the provisions of the *Privacy Act 1988* (Cth) under the small business exemption.

[102] *Privacy Act 1988* (Cth) s 7B(2) (Commonwealth contract), 7B(5) (State contract).

[103] See *Health Records and Information Privacy Act 2002* (NSW) s 17 sch1, HPP 10(1)(c); *Health Records Act 2001* (Vic) pt 2 div 3; *Health Records (Privacy and Access) Act 1997* (ACT) s 14 and sch 1.

[104] The *Privacy Act* defines 'health information' as information or an opinion about the health or a disability (at any time) of an individual; or an individual's expressed wishes about the future provision of health services to him or her; or a health service provided, or to be provided, to an individual; that is also personal information; or other personal information collected to provide, or in providing, a health service; or other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual. *Privacy Act 1988* (Cth) s 6(1).

[105] Australian Law Reform Commission, (2008) For Your Information: Australian Privacy Law and Practice (Report 108), [6.88] < http://www.alrc.gov.au/publications/6.%20The%20Privacy%20Act%3A%20Some%20Important%20Definitions/sensitive-information>.

*Information Privacy Act 2002* (NSW) contains 15 HPPs outlining how health information must be collected, stored, used and disclosed; and the *Health Records Act 2001* (Vic) contains 11 HPPs—and private sector health service providers in these jurisdictions are required to comply with the HPPs or with an approved health privacy code of practice.[106] Each statute contains mandatory requirements, exemptions similar to the *Privacy Act*, and provides for the development of approved health privacy codes of practice.[107] The co-existence of provisions under the *Privacy Act* and State and Territory legislation has caused confusion and uncertainty about the federal and state regulatory regimes for private sector health service providers and researchers, and increased compliance costs. Further, the differences between the federal and state statutes make it difficult for private sector health service providers operating across jurisdictional borders or nationally to comply.[108] Such difficulties led the Australian Health Ministers Advisory Council in 2003 to propose and draft a National Health Privacy Code, designed to apply to all health service providers in their handling of health information.[109] In 2008 the Australian Law Reform Commission ('ALRC') recommended that there should be national consistency and harmonization of laws in the regulation of privacy and confidentiality of personal, sensitive and health information.[110] The following section examines law reform initiatives as a result of the ALRC's review of the *Privacy Act* and the handling of health information in Australia.

### 5.4 Law Reform in Australia

The ALRC reviewed the *Privacy Act* in 2006 and its final recommendations were submitted to the Australian Parliament in 2008.[111] As noted above, having multiple laws regulating privacy and personal health information in some jurisdictions gives rise to complexities and inconsistencies. As one of its key recommendations the ALRC recommended the achievement of national consistency, suggesting as a first step that the *Privacy Act* apply to the exclusion of State and Territory laws dealing specifically with the handling of personal information by private sector organisations.[112] The ALRC recommended the simplification and streamlining of the *Privacy Act* and related laws and regulations that are currently detailed and complex, suggesting a basic restructuring of the *Privacy Act*[113] supplemented by regulations covering specific fields such as health information privacy;[114] that the current IPPs and NPPs be consolidated into a single set of privacy principles referred to in the ALRC report as Unified Privacy Principles ('UPPs'), which would apply to both Commonwealth public sector agencies and to private sector organisations;[115] that the States and Territories agree to enact legislation regulating the handling of personal information in the State and Territory public sectors that would apply the UPPs and contain certain other minimum provisions consistent with the *Privacy Act*, thus ensuring that information privacy protection would be consistent across the public and private sectors in all jurisdictions;[116] amendments to some

---

[106] *Health Records (Privacy and Access) Act 1997* (ACT) s 6, sch 1; See *Health Records and Information Privacy Act 2002* (NSW) s 17, sch 1; *Health Records Act 2001* (Vic) ss 11, 21, sch 1.
[107] Australian Law Reform Commission, (2008) For Your Information: Australian Privacy Law and Practice (Report 108), Recommendation 3-1 p. 25, 188-193.
[108] Commonwealth of Australia, (2003) The Protection of Human Genetic Information in Australia (ALRC Report 96), Executive Summary p.1
[109] National Health and Medical Research Council, (2004) *The Regulation of Health Information Privacy in Australia: A description and comment*, pt 6: National Health Privacy Code <http://www.nhmrc.gov.au/_files_nhmrc/publications/attachments/nh53.pdf> (accessed 20 September 2013). Four alternative implementation strategies for the Code were contemplated (p 66), but the Code has not been implemented.
[110] Australian Law Reform Commission, (2008) *For Your Information: Australian Privacy Law and Practice*, pp. 70-78 [60]-[63]. See also Australian Law Reform Commission, (2011) *Key Recommendations for Health Information Privacy Reform*. <http://www.alrc.gov.au/news-media/2011/australian-privacy-law-practice-key-recommendations-health-information-privacy-refor> (accessed 20 September 2013).
[111] Australian Law Reform Commission, (2008) *For Your Information: Australian Privacy Law and Practice*, p. 122.
[112] Australian Law Reform Commission, (2008) *For Your Information: Australian Privacy Law and Practice*, Recommendation 3-1.
[113] Australian Law Reform Commission, (2008) *For Your Information: Australian Privacy Law and Practice*, Recommendation 5-2.
[114] Australian Law Reform Commission, (2008) *For Your Information: Australian Privacy Law and Practice*, Recommendations 5-1, 60-1.
[115] Australian Law Reform Commission, (2008) *For Your Information: Australian Privacy Law and Practice*, Recommendation 18-2.
[116] Australian Law Reform Commission, (2008) *For Your Information: Australian Privacy Law and Practice*, Recommendation 3-4.

important definitions including 'personal information', 'sensitive information', 'record',[117] 'health information' and 'health service';[118] that many exemptions, including the small business exemption, under the *Privacy Act* be removed;[119] improved complaints handling mechanisms for the Office of the Australian Information Commissioner;[120] and stronger penalties for conduct constituting interference with the privacy of an individual.[121]

Specifically in relation to health information, as well as suggesting new *Privacy (Health Information) Regulations* drafted to contain only those requirements that are different to or more specific than provided for in the UPPs[122] and amendments to the definition of 'health information' and 'health service', with respect to electronic health information systems the ALRC recommended that if a national unique healthcare identifiers ('UHIs') or a national shared electronic health records ('SEHR') scheme were to go ahead, it should be established under specific enabling legislation. The ALRC recommended that this legislation should address information privacy issues, such as:

- the nomination of an agency or organisation with clear responsibility for managing the respective systems, including the personal information contained in the systems;
- the eligibility criteria, rights and requirements for participation in the UHI and SEHR schemes by health consumers and health service providers, including consent requirements;
- permitted and prohibited uses and linkages of the personal information held in the systems;
- permitted and prohibited uses of UHIs and sanctions in relation to misuse; and
- safeguards in relation to the use of UHIs, including providing that it is not necessary to use a UHI in order to access health services.[123]

The Australian Government supported in principle the ALRC's recommendation for greater clarity and consistency in information privacy protection and it has adopted some of the recommendations mentioned above. The *Privacy Amendment (Enhancing Privacy Protection) Act 2013* (Cth) comes into effect from 12 March 2014. This Act repeals the IPPs and the NPPs under the *Privacy Act* and replaces them with a set of 14 unified privacy principles called the Australian Privacy Principles ('APPs'). The APPs apply to both Commonwealth public sector agencies and private sector organisations.

Amendments to the definitions of personal information and sensitive information have been adopted as recommended. 'Personal information' is now defined as:

> information or an opinion about an identified individual, or an individual who is reasonably identifiable:
> (a) whether the information or opinion is true or not; and
> (b) whether the information or opinion is recorded in a material form or not.

'Sensitive information' is now defined as:

> (a) information or an opinion about an individual's:

[117] Australian Law Reform Commission, (2008) *For Your Information: Australian Privacy Law and Practice*, Recommendations 6-1 - 6-7.
[118] Australian Law Reform Commission, (2008) *For Your Information: Australian Privacy Law and Practice*, Recommendations 62-1, 62-2.
[119] Australian Law Reform Commission, (2008) *For Your Information: Australian Privacy Law and Practice*, Recommendation 39-1, and see generally pt E—Exemptions.
[120] Australian Law Reform Commission, (2008) *For Your Information: Australian Privacy Law and Practice*, Recommendations 49-1 - 49-13.
[121] Australian Law Reform Commission, (2008) *For Your Information: Australian Privacy Law and Practice*, Recommendations 50-1 - 50-4.
[122] Australian Law Reform Commission, (2008) *For Your Information: Australian Privacy Law and Practice*, Recommendation 60-1.
[123] Australian Law Reform Commission, (2008) *For Your Information: Australian Privacy Law and Practice*, Recommendation 61-1, p. 2040.

(i) racial or ethnic origin; or
(ii) political opinions; or
(iii) membership of a political association; or
(iv) religious beliefs or affiliations; or
(v) philosophical beliefs; or
(vi) membership of a professional or trade association; or
(vii) membership of a trade union; or
(viii) sexual *orientation* or practices; or
(ix) criminal record;
that is also personal information; or

(b) health information about an individual; or
(c) genetic information about an individual that is not otherwise health information*; or*
*(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or*
*(e) biometric templates* (emphasis added).

The ALRC recommended that those elements of the privacy principles that dealt specifically with the handling of health information should be set out in a new health-specific privacy regulation was rejected by the Government, as were its suggested amendments to the definitions of 'health information' and 'health service' in the *Privacy Act*. The Australian Government's response to the ALRC Report 108[124] is that health service providers may collect health data from an individual such as a doctor about patients to provide health services and disclose such data where the patient's medical data is relevant and necessary to provide health service; and if it would be reasonably expected that such information is to be collected.[125]

'Health information' is now defined as:

(a) information or an opinion about:
(i) the health or a disability (at any time) of an individual; or
(ii) an individual's expressed wishes about the future provision of health services to him or her; or
(iii) a health service provided, or to be provided, to an individual;
that is also personal information; or
(b) other personal information collected to provide, or in providing, a health service; or
(c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or
(d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

In 2006, the Council of Australian Governments agreed to a national approach to developing, implementing and operating systems for healthcare identifiers for individuals and health service providers as part of work on a national electronic health records system to improve safety for patients and increase efficiency for health service providers. The National Partnership Agreement for E-Health signed in 2009 set out the objectives and scope of the Healthcare Identifiers Service, and relevant governance, legislative, administrative and financial arrangements.[126] The *Healthcare Identifiers Act 2010* (Cth) was subsequently enacted in 2010. This Act implements a national system for consistently identifying individuals and health service providers and sets out

[124] Australian Law Reform Commission, (2008) *For Your Information: Australian Privacy Law and Practice*, Recommendations 63-1, 63-2, 63-3 pp. 2088, 2097 & 2106.
[125] Office of the Privacy Commissioner, (2009) *Synopsis of Australian Government response to ALRC Report 108—Health Services & Research (Part H)* October 2009 <http://www.oaic.gov.au/images/documents/migrated/2009-11-19010103/2009-10%20Synopsis%20on%20Government%20response%20-%20Health%20and%20Research%20-%20Part%20H%20with%20header-web.pdf> (accessed 20 September 2013).
[126] See Healthcare Identifiers Bill 2010 (Cth), Replacement Explanatory Memorandum <http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r4299_ems_3e46e39a-571e-446f-9a13-46a30db9477a/upload_pdf/343938repem.pdf;fileType=application%2Fpdf#search=%22legislation/ems/r4299_ems_3e46e39a-571e-446f-9a13-46a30db9477a%22>.

clear purposes for which healthcare identifiers can be used. Section 3 of the *Healthcare Identifiers Act 2010* (Cth) states that the healthcare identifier is 'to provide a way of ensuring that an entity that provides, or an individual who receives, healthcare is correctly matched to health information that is created when healthcare is provided'; this is to be achieved 'by assigning a unique identifying number to each healthcare provider and healthcare recipient'.

## 6 Conclusion

This article has examined the application of data mining and data matching techniques by health service providers and medical researchers and has provided some ethical and legal perspectives on the collection, use and disclosure of medical data obtained through data mining and data matching. The collection of medical data through data mining and the process of data matching do raise ethical and privacy concerns. In seeking to justify sensing and monitoring of the sensitive medical data of individuals, there are competing tensions between public and private interests and a balance needs to be struck. While 'medical ethics' can be difficult to define, fundamentally it means that there must be mutual respect and confidence between the doctor and his or her patient, between the health service provider and the individual. Each of us deserves respect as humans beings possessed of human dignity, and this respect must also extend to intimate adjuncts of our personalities, and that includes personal information whether sensitive information or not. As long as information remains personal in any sense, it preserves a moral resonance that requires that it be treated with adequate respect.

This article has examined the international landscape of information privacy protection and the statutory protection under Australian law. The protection under international conventions, guidelines and declarations demonstrates a trend towards making more explicit the ethical standards which must be met if research on human beings is to be ethically acceptable. Complexities within the *Privacy Act* and inconsistencies with State and Territory legislation limit the protection available for health information. The article also examined some Australian law reform initiatives relating to the handling of personal information, sensitive information and health information. Although the *Privacy Amendment (Enhancing Privacy Protection) Act 2013* (Cth) amends the definitions of 'personal information' 'sensitive information' and 'health information' in the *Privacy Act* to give greater scope for the protection of such information, the Act still allow indiscriminate collection in the current information technology era as the *Privacy Act* is technology neutral[127] and exempts small businesses from compliance with the Privacy Act. This greatly limits the protection for personal information, sensitive information and health information as for those exempt from the federal and state legislation are still able to collect, use and disclose such information without consent of the data subject.

* * * *


Cite as: Rajaretnam,T. "Data Mining and Data Matching" *Journal of International Commercial Law and Technology,* Vol.9 Issue 4 (Nov, 2014)

[127] Commonwealth of Australia, (2009) Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission (Report 108) *For your Information: Australian Privacy Law and Practice*, p. 37.