"Health Privacy and Confidentiality"

Chapter 23

in *Tensions and Traumas in Health Law*, I Freckelton and & K Petersen (Eds) (2017) Sydney: Federation Press (in print)

Danuta Mendelson and Gabrielle Wolf

The notion that a patient has the right to maintain the confidentiality of information disclosed in the course of a therapeutic relationship with a health practitioner has been entrenched in Western civilisation for thousands of years. For the first time, however, we have begun to witness an erosion of this entitlement, especially in Australia in recent years. The Federal Parliament has created a system of co-linked national electronic health records that, by virtue of new technology, permits government bodies and myriad other third parties to access and disseminate individuals' health information both lawfully and without authority, almost invariably in the absence of patients' knowledge and consent. Commonwealth legislation has also facilitated the substitution of patients' traditional right to confidentiality of their health information with a much broader and less clearly defined right to "personal privacy". This chapter examines how these changes have led to a fundamental upheaval of longstanding understandings about the protection of information communicated and learned in the once secluded space of the consulting room.

Changes to patients' historical right to the confidentiality of their health information

The substance of conversations between patient and doctor in the context of the therapeutic relationship is inherently highly personal. Historically, such information about individuals' medical and psychiatric problems and conditions was locked inside the clinical notes of health providers and protected by the medical duty of confidentiality. For the past 2,500 years, physicians in the Western medical tradition[1] have been subject to the Hippocratic Oath,[2] the penultimate clause of which imposes on them a duty to keep to themselves all that they observe or become aware of in relation to their patients.[3]

In common law countries, the right of patients to have their medical information kept confidential (unless disclosure is compelled by the law)[4] has reflected respect for the patient and recognition that trust between the parties to a therapeutic relationship is vital for efficacious medical treatment. In such a relationship, the doctor trusts the patient to disclose candidly his/her personal, often embarrassing, stigmatising and/or intimate information that may be relevant to the diagnosis, prognosis and treatment of his/her complaint or condition. The patient, in turn, trusts the doctor to use that knowledge solely for therapeutic purposes,

[1] See Danuta Mendelson, 'Medical Duty of Confidentiality in the Hippocratic Tradition and Jewish Medical Ethics.' (1998) 5(3) *Journal of Law and Medicine* 227-238.
[2] 'What I see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself holding such things shameful to be spoken about.' *Hippocratic Writings* (Chadwick J and Mann WN (trans), Lloyd GER (ed)) (Penguin Books, Harmondsworth, 1983).
[3] Danuta Mendelson, 'Medical Duty of Confidentiality in the Hippocratic Tradition and Jewish Medical Ethics.' (1998) 5(3) *Journal of Law and Medicine* 227-238.
[4] Danuta Mendelson, 'The Duchess of Kingston's Case, the Ruling of Lord Mansfield and Duty of Medical Confidentiality in Court' (2012) 35 (5) *International Journal of Law and Psychiatry* 480-489 http://dx.doi.org/10.1016/j.ijlp.2012.09.005.

unless the patient provides voluntary and informed consent for other uses of it. Hippocratic physicians of Classical Athens and the Hellenistic era, just like medical practitioners of today, created clinical records documenting their professional encounters with patients as aide-mémoire,[5] and for the purposes of treating the patients and referring them to other healthcare specialists. Mutual trust between the parties was maintained because only the patient and the treating professionals were privy to the patient's health information.

Laws and codes developed over the centuries for the protection of personal, medical and other health-related information were designed for one-to-one relationships between the patient and his/her healthcare practitioner, or at least for relationships between the patient and a defined number of persons who needed his/her health information in order to act in the patient's best interests.[6] Patients, as transmitters or suppliers of personal information about themselves, were in control of that information insofar as the recipients of it – healthcare professionals – had ethical and legal obligations to keep it confidential. This is still the position in continental Europe and civil law countries generally, where the obligation of medical confidentiality tends to be legislatively entrenched,[7] and recognised by Article 8 of the European convention on human rights.[8] However, since the *Duchess of Kingston Case* (1776),[9] at common law, which Australia inherited from Britain, patients' right to the confidentiality of their health information was considered an ethical rather than a legal principle,[10] and it did not amount to an evidentiary privilege that would enable a medical practitioner to remain silent on the witness stand.[11] Some Australian jurisdictions did nonetheless seek to protect this right,[12] though, as this chapter will illustrate, current, purported legal safeguards of the confidentiality of patients' health information appear to be illusory.

---

[5] *Hippocratic Writings*, translated by J Chadwick and WN Mann, Ed. GER Lloyd, Harmondsworth: Penguin Book 1983. "The 42 physicians' case histories preserved in the *Hippocratic Corpus* (mainly in book I and II of *Epidemics*), contain patient's gender, sometimes name, age, or other characteristic ("bald man"), the season of the year, and the locale. Each clinical record also includes the initial signs and symptoms, and where known, the cause of the disease, followed by daily observations of the patient's condition, treatment, complications, if any, and the outcome. The case histories range from a record of single consultation to 120 days of observations": Danuta Mendelson, "Electronic Medical Records: Perils of Outsourcing and the Privacy Act 1988 (Cth)" (2004) 12 *Journal of Law and Medicine* 8-14.

[6] For example, where a patient was sent to a multi-disciplinary pain treatment centre for assessment and possible therapy.

[7] For example, in France, Art. L.1110-4(1) of the Code of Public Health provides that, except where continuity of care or better health care outcomes are involved, "every patient has the right to respect for his privacy and the right to keep secret the data concerning him." Under Art 226-13 of the Penal Code ("Code Pénal"), a violation of medical secrecy may attract a prison sentence of one year and a fine of 15.000€. See Patient Rights in the EU http://europatientrights.eu/countries/signed/france/france_right_to_privacy_medical_secrecy.html

[8] http://www.echr.coe.int/Documents/Convention_ENG.pdf

[9] *Duchess of Kingston Case* (1776) 20 Howell's State Trials 355; [1775-1802] All ER Rep 623; see Danuta Mendelson, 'The Duchess of Kingston's Case, the Ruling of Lord Mansfield and Duty of Medical Confidentiality in Court' (2012) 35 (5) *International Journal of Law and Psychiatry* 480.

[10] *Royal Women's Hospital v Medical Practitioners Board of Victoria* [2006] VSCA 85. For a discussion of this case, see: Danuta Mendelson & Anne Rees, 'Medical Confidentiality and Patient Privacy', in *Health Law in Australia* B White, F McDonald & L Willmott (Eds), 2nd Edition, Thomson Reuters, 2014 Chapter 9, pp 371-411.

[11] *R v. Young* [1999] 46 NSWLR 681 at 699 per Spigelman CJ.

[12] For example, *Evidence (Miscellaneous Provisions) Act 1958* (Vic) s 28(3)–(5) and s 32B; *Evidence Act 2001* (Tas) ss 127A, 126B-126D; *Evidence Act 1939* (NT) s 12(2); *Evidence Act* 2011 (ACT), Div 3.10.1A, ss 126A-F; *Evidence Act* 1995 (NSW), Pt 3.10, Div 1A.

Medical records, which over the centuries had changed from papyrus to paper, have now largely been replaced by electronic health records. Digitization of health records in and of itself should not have made any difference to their confidentiality and, initially, it did not.

Before the rise of electronic networks, the lack of interoperability limited the disclosure of information stored on computerised patient record systems used by hospitals and other healthcare entities.[13] As they were in the era of paper health records, patients would have been aware that their identifiable health data was being forwarded to the Health Insurance Commission (named Medicare Australia since 2005), private health insurance funds[14] and, where relevant, law-enforcement or governmental bodies according to statutorily-mandated reporting duties (with respect, for example, to notifiable diseases, child abuse and prescriptions for controlled substances).[15] Nevertheless, the records were stored in situ and, therefore, control over them remained with the hospital, facility or treating doctor. Third parties had no access to the records unless they were specifically authorised to view them, for instance, pursuant to a subpoena. The risks relating to unauthorised access to these health records through hacking and viral contamination were comparable to risks faced by those who retain paper documents, such as theft and forgery.[16]

In the 21st century, however, the multi-faceted revolution in computer technology and, particularly, an exponential expansion of digitization ("the conversion of analogue data, including text, images, and video into digital form"),[17] has led to the emergence of new means for third parties to accumulate, access, use, interpret and distribute patients' digitized health records without their knowledge or consent. Modern technologies have enabled capture, search, aggregation and transfer of large volumes of data in real time, while advanced algorithms[18] facilitate its integration by: linking information from diverse sources; extracting data from various entities; indexing and data fusion; conducting analyses using computational intelligence algorithms, statistics, predictive and text analytics; machine

[13] Livia Iacovino, Danuta Mendelson & Moira Paterson, "Privacy Issues, Health*Connect* and Beyond" in *Disputes and Dilemmas in Health Law*, I Freckelton and K Petersen (Eds), (2006) Sydney: Federation Press 604-622.

[14] Bernadette McSherry, "Third Party Access to Shared Electronic Mental Health Records: Ethical Issues", (2004) 11(1) *Psychiatry, Psychology and Law* 53-62, DOI: 10.1375/pplt.2004.11.1.53

[15] Danuta Mendelson, "Travels of a Medical Record and the Myth of Privacy" (2003) 11 (2) *Journal of Law and Medicine* 136.

[16] However, as health databases have expanded exponentially, so has hacking. For example, in January 2017, a ransomware attack on England's biggest hospital trust, Barts Health NHS Trust, infected thousands of files stored on Window XP computers; it necessitated shutting down parts of the network for days to allow investigation by engineers. In November 2016, a ransomware attack shut down the system of the Northern Lincolnshire and Goole NHS Foundation Trust for four days; as a result, 2800 hospital appointments were cancelled: Ben Heather, "Barts Health NHS Trust hit with "IT attack", *Digital Health*, 13 January 2017 17:03 http://www.digitalhealth.net/cybersecurity/48415/barts-health-nhs-trust-hit-with-

[17] "Digitization", OED Online. Oxford University Press, December 2016. Web. 27 December 2016.

[18] An "algorithm" has been described as a tool for solving a well-specified computational problem/task through "a sequence of computational steps or instructions that transform the input into the output. The statement of the problem/task specifies in general terms the desired input/output relationship". Thomas H Cormen, Charles E Leiserson, and Ronald L Rivest, *Introduction to Algorithms*, Cambridge, US: MIT Press, 2009 at 5. See also Gavin Clarke "2016: The Rise of the Intelligent (cloud) Machines; Only smart survives the cloud consolidation" *The Register*, 25 Dec 2016; http://www.theregister.co.uk/2016/12/25/2017_rise_of_the_intelligent_machines/

learning; storing data (virtual machine technologies can emulate real computers and computer networks);[19] and managing data.

Although this "unprecedented computational power and sophistication make possible unexpected discoveries, innovations, and advancements in our quality of life",[20] they can also create "an asymmetry of power between those who hold the data and those who intentionally or inadvertently supply it".[21] Complex techniques, statistics, and machine learning can process health data to create models[22] of our health and lifestyle profiles. Further, "existing smartphone sensors can be used to infer a user's mood; stress levels; personality type; bipolar disorder; demographics (e.g., gender, marital status, job status, age); smoking habits; overall well-being; progression of Parkinson's disease; sleep patterns; happiness; levels of exercise; and types of physical activity or movement".[23] In addition, data-matching of patients' digitized health information, in Australia and across the globe, has grown into an enormous business of "data assets" worth billions of dollars. In November 2016, Crossix Solutions, a United States healthcare analytics firm with "an unrivaled breadth of data assets", including a "proprietary network of health and non-health data covering over 250 million U.S. consumers (76% of the U.S. population)",[24] expanded its data assets to cover, in addition to prescription purchase records (Rx), "hospital records, electronic health records (EHR) and electronic medical records (EMR), doctors' notes, lab results, and other clinical data".[25] Jeremy Mittler, VP, Industry Solutions at Crossix Solutions, explained that the acquisition enables the company:

> "To link, for example, the information gleaned from doctor notes to bloodwork results to Rx usage data to individuals exposed to display or mobile ads [which] offers a veritable wealth of insight into what factors trigger certain actions for distinct patient segments at different phases of their disease progression".[26]

---

[19] James E Smith, Ravi Nair, The Morgan Kaufmann Series in Computer Architecture and Design (Amsterdam: Morgan Kaufmann. 2005).

[20] Executive Office of the President, The White House, Big Data Privacy Report, "Big Data: Seizing Opportunities, Preserving Values", (May 2014) at 2-3 https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

[21] Executive Office of the President, The White House, Big Data Privacy Report, "Big Data: Seizing Opportunities, Preserving Values", (May 2014) at 2-3 https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

[22] Scott Monteith, Tasha Glenn, "Automated Decision-Making and Big Data: Concerns for People With Mental Illness" (2016) 18 *Current Psychiatry Reports* 112, doi:10.1007/s11920-016-0746-6

[23] Scott R. Peppet, Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent, 93 *TEX. L. REV*. 85, 115-16 (2014) (citations omitted) ("Regulating the Internet of Things"), available at http://www.texaslrev.com/wp-content/uploads/Peppet-93-1.pdf. Cited in Federal Trade Commission (US), "The Internet of Things: Privacy and Security in a Connected World" (2015) at p 15. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[24] http://crossix.com/about-crossix.aspx

[25] Andrew Matthius, "What Does Crossix's Latest Expansion of Connected Health Data Actually Mean for Pharma Marketers?" PM360 (December 20th, 2016). Interview with Jeremy Mittler, VP, Industry Solutions at Crossix Solutions. https://www.pm360online.com/what-does-crossixs-latest-expansion-of-connected-health-data-actually-mean-for-pharma-marketers/

[26] Andrew Matthius, "What Does Crossix's Latest Expansion of Connected Health Data Actually Mean for Pharma Marketers?" PM360 (December 20th, 2016). Interview with Jeremy Mittler, VP, Industry Solutions at Crossix Solutions. https://www.pm360online.com/what-does-crossixs-latest-expansion-of-connected-health-data-actually-mean-for-pharma-marketers/

Apparently, Crossix Solutions can access all the above-listed clinical information about patients because it has patented a "double-blinded, privacy-safe, distributed data-mining protocol, ensuring that … [its] clients have confidence in … de-identified, HIPAA-compliant[27] approach".[28] Crossix Solutions LLC currently has the patent on "A Privacy Preserving Data-Mining Protocol" in Australia.[29]

Also reinforcing an "asymmetry of power" in Australia between "those who hold" health information and the patients and healthcare practitioners "who intentionally or inadvertently supply it", are legislation passed by the Commonwealth Parliament to develop a national electronic health records system and technology used to operate it. We now examine this system (its name was altered from the "Personally Controlled Electronic Health Record" system to the "My Health Record" system in 2015),[30] which we argue may so profoundly undermine Australian patients' right to maintain the confidentiality of their health information that it renders this right meaningless.

Erosion of patients' right to the confidentiality of their health information under the My Health Record system

The *My Health Records Act 2012* (Cth) permits the Federal Government to change the My Health Record system from an "opt-in" to an "opt-out" model.[31] Under this scheme, all "healthcare recipients" – individuals who have received, receive or may receive health care[32] – will automatically be registered in the My Health Record system and issued electronic "My Health Records" to which health information about them is uploaded.[33] The My Health Record system enables the accumulation of a vast volume of such data, which can include: clinical notes of participating general practitioners and allied healthcare professionals (as of 20 December 2016, 1,378,118 clinical documents were uploaded);[34] information from hospitals, pharmacies (as of 20 December 2016, 6,806,784 prescriptions and dispense documents were uploaded onto the My Health Record),[35] and aged care residential services; Medicare documents (as of 20 December 2016, 407,711,478 Medicare documents were uploaded);[36] hospital discharge information; diagnostic reports and images, such as ultrasounds, x-rays, CT scans, MRI, and mammograms; pathology reports on tissue, blood, urine, stools or other body fluids and secretions tests; specialist letters if forwarded in electronic form; eReferral notes; as well as advance directives.[37]

Significantly, Commonwealth legislation allows innumerable individuals and entities to access this extensive information in healthcare recipients' My Health Records without the

---

[27] "HIPAA" is an acronym for the *Health Insurance Portability and Accountability Act 1996* (US) – its data privacy and security provisions for safeguarding medical information need to be updated.
[28] http://crossix.com/platform.aspx
[29] Intellectual property in Australia http://www.ipaustralia.com.au/applicant/crossix-solutions-llc/patents/ For an excellent analysis of the medical records data-mining business see Adam Tanner, *Our Bodies, Our Data How Companies Make Billions Selling Our Medical Records*, (2017) Penguin Random House.
[30] Explanatory Memorandum, Health Legislation Amendment (eHealth) Bill 2015 (Cth) 2.
[31] *My Health Records Act 2012* (Cth) s 4.
[32] *My Health Records Act 2012* (Cth) s 5 (definition of 'healthcare recipient').
[33] *My Health Records Act 2012* (Cth) s 4.
[34] https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/news-002
[35] https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/news-002
[36] https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/news-002
[37] Dashboard display of My Health Record statistics
https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/news-002

data-subjects' knowledge and authority to do so. This access is provided for purposes beyond the provision of healthcare to patients,[38] and irrespective of any obligation imposed on their health practitioners to keep that information confidential. Technology that facilitates the creation and operation of the My Health Record system similarly enables use and dissemination of such patient information in ways that instigate a dramatic shift in the traditional paradigm of patients' right to medical confidentiality.[39] Already in 1999, the National Health Information Management Advisory Council had proposed:

> "a national strategic approach to using information in the health system [electronic health records] to promote new ways of delivering health services, by harnessing the enormous potential of new technologies".[40]

Moreover, although the legislation stipulates measures designed to protect the confidentiality of information stored in the My Health Record system to some extent, there is a high risk of intentional or inadvertent breaches of the system's security, enabling third parties' unauthorised access to and disclosure of patients' health information.[41]

Lawful incursions into patients' right to the confidentiality of their health information

Healthcare recipients are unlikely to be aware of the broad range of individuals and entities who can lawfully access their health information that is contained in the My Health Record system and then further disseminate it, including when the patients do not know about and have not consented to this occurring and where it is not intended to benefit them.

Various "participants" in the My Health Record system whom the legislation explicitly authorises to collect, use and disclose information in a My Health Record for several enumerated purposes include:[42]

- the "System Operator", which is either the Secretary of the Department of Health or a body established by a Commonwealth law and prescribed to be such by the regulations,[43] and operates the National Repositories Service in which "key records that form part" of My Health Records are stored;[44]

---

[38] See: Consultation on Secondary Use of My Health Record Data Postponed: "The department has decided to postpone the consultations until early next year. There are a number of other consultations occurring at this time, for example on the National Digital Health Strategy, that will compete for the attention of health care providers and the broader community. In addition it is possible that the outcome of these consultations could further inform a discussion paper on secondary use of My Health Record data." https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/content/home Accessed on 10 January 2017.

[39] Sue Walker and Janelle Craig, "e-Health — a new world order for health information managers" (2002) 30(1) *Health Information Management Journal* at http://www.himaa.org.au/memberarea/journal/30_1_2001/walker/walker.html accessed on 5 September 2016.

[40] National Health Information Management Advisory Council, *Health Online: A health information action plan for Australia* (November 1999) cited in Sue Walker and Janelle Craig, "e-Health — a new world order for health information managers" (2002) 30(1) *Health Information Management Journal* at http://www.himaa.org.au/memberarea/journal/30_1_2001/walker/walker.html accessed on 5 September 2016.

[41] See for example Ronald Bayer, John Santelli, Robert Klitzman, "New Challenges for Electronic Health Records Confidentiality and Access to Sensitive Health Information about Parents and Adolescents" (2015) 313(1) *Journal of American Medical Association* 29; though discussed in American context, this issue is equally pertinent to Australia.

[42] *My Health Records Act 2012* (Cth) s 5 (definition of "participant in the My Health Record system").

[43] *My Health Records Act 2012* (Cth) s 14.

[44] *My Health Records Act 2012* (Cth) ss 4-5, 15. Note that section 5 of this statute refers to the operator of the National Repositories Service as another distinct participant.

- "registered healthcare provider organisations", defined as any "entity that has conducted, conducts, or will conduct an enterprise that provides healthcare" and whom the System Operator has registered,[45] regardless of whether they provide healthcare to registered healthcare recipients;
- "registered repository operators", including the Chief Executive Medicare and other entities such as pathology laboratories, whom the System Operator registers to hold records of information that, together with the records in the National Repositories Service, constitute My Health Records;[46]
- "registered portal operators", whom the System Operator registers to operate "an electronic interface that facilitates access to the My Health Record system";[47] and
- "registered contracted service providers", who are parties to contracts with registered healthcare providers, which require them to provide information technology or health information management services relating to the My Health Record system.[48]

The System Operator may delegate any of his/her/its functions and powers to an Australian Public Service employee in the Department of Health, the Chief Executive Medicare and, if the System Operator is the Secretary of the Department, to "any other person with the consent of the Minister".[49]

The *My Health Records Act 2012* (Cth) also allows the participants to share their authority to collect, use and disclose healthcare recipients' information with:

- their employees whose duties require them to rely on this authority;[50]
- any service provider, and its employees, where it enters a contract with a healthcare provider that requires it to "[provide] information technology services relating to the communication of health information, or health information management services, to the healthcare provider";[51] and
- anyone who performs services under a contract relating to the My Health Record system with the System Operator, a registered repository operator or a registered portal operator.[52]

Importantly, with the exception of a registered healthcare recipient's "nominated representative",[53] the *My Health Records Act 2012* (Cth) does not specify the persons and entities to whom the participants are permitted to disclose information in a healthcare recipient's My Health Record when the disclosure is for one of the purposes permitted by this Act.[54] Consequently, the information could potentially be disclosed to anyone.

---

[45] *My Health Records Act 2012* (Cth) ss 5, 44.
[46] *My Health Records Act 2012* (Cth) ss 4-5, 38, 48-9; *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* (Cth) guideline 4.5.
[47] *My Health Records Act 2012* (Cth) ss 5, 48-9.
[48] *My Health Records Act 2012* (Cth) ss 5, 48-9; *My Health Records Rule 2012* (Cth) rr 34(1)-(2).
[49] *My Health Records Act 2012* (Cth) ss 98(1), (3); Explanatory Memorandum, Health Legislation Amendment (eHealth) Bill 2015 (Cth) 88.
[50] *My Health Records Act 2012* (Cth) s 99(a).
[51] *My Health Records Act 2012* (Cth) ss 99(b), (d).
[52] *My Health Records Act 2012* (Cth) s 99(c).
[53] *My Health Records Act 2012* (Cth) s 62.
[54] See *My Health Records Act 2012* (Cth) ss 61, 63-5, 68-70, sch 1, pt 2, div 2, cls 7-8.

Some provisions of the *My Health Records Act 2012* (Cth) refer to patients' actual or perceived wishes regarding such disclosure of their information, but also permit the participants to pay mere lip service to them. For instance, the participants are authorised to collect, use or disclose health information in a My Health Record if they do so "for the purpose of the management or operation of the My Health Record system" and "the healthcare recipient would reasonably expect the participant" to do so.[55] Yet the legislation provides no guidance on how to ascertain a healthcare recipient's expectations. Similarly, the participants can collect, use and disclose information in My Health Records if they reasonably believe that it is "necessary to lessen or prevent a serious threat to an individual's life, health or safety", and "it is unreasonable or impracticable to obtain the healthcare recipient's consent to the collection use or disclosure".[56] The *My Health Records Act 2012* (Cth) does not, however, indicate who determines that obtaining a healthcare recipient's consent is unreasonable or impracticable, or how such a decision is made.

A participant need not even consider whether a healthcare recipient has consented or would consent to collecting, using and disclosing his/her health information before doing so in certain circumstances. Those situations include: "if the participant reasonably believes that the collection, use or disclosure by the participant is necessary to lessen or prevent a serious threat to public health or public safety";[57] "if the collection, use or disclosure is required or authorised by Commonwealth, State or Territory law";[58] and "for purposes relating to the provision of indemnity cover for a healthcare provider".[59]

The System Operator has additional powers, beyond those available to the other participants, to:

> "Use or disclose health information included in a healthcare recipient's My Health Record if the System Operator reasonably believes that the use or disclosure is reasonably necessary for one or more of the following things done by, or on behalf of, an enforcement body:
>
> (a) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
>
> (b) the enforcement of laws relating to the confiscation of the proceeds of crime;
>
> (c) the protection of the public revenue;
>
> (d) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
>
> (e) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal".[60]

---

[55] *My Health Records Act 2012* (Cth) s 63.
[56] *My Health Records Act 2012* (Cth) s 64(1).
[57] *My Health Records Act 2012* (Cth) s 64(2).
[58] *My Health Records Act 2012* (Cth) s 65.
[59] *My Health Records Act 2012* (Cth) s 68. See also: *My Health Records Act 2012* (Cth) ss 69(1), (2), 70(1), (3).
[60] *My Health Records Act 2012* (Cth) s 70(1).

Although the System Operator "must make a written note of the use or disclosure",[61] the legislation does not oblige the System Operator to seek patients' consent to the use or disclosure of their health information under this provision or to notify them that it has taken place. The System Operator cannot "use or disclose healthcare recipient-only notes",[62] but no other controls or filters are imposed on the relevance and nature of patients' personal and clinical information that can be used or disclosed.

Healthcare recipients are permitted to set "access controls" that restrict the registered healthcare provider organisations and nominated representatives who can access their My Health Records.[63] If they do not do so, however, default access controls that are established and maintained by the System Operator apply.[64] In its Privacy Impact Assessment Report on the My Health Record system, Minter Ellison predicted that many individuals would not appreciate the ramifications of the application of default access controls, including that "all information" in their My Health Records "will become accessible by an authorised employee accessing the My Health Record on behalf of a registered healthcare provider organisation".[65] This could mean, for example, that a patient's "optometrist and dentist can see from their PBS records that they have been prescribed antidepressants", and "that their boyfriend who works in the hospital where they were once treated for a broken arm, can see that they have recently terminated a pregnancy in a different hospital".[66]

In addition to the participants, the *My Health Records Act 2012* (Cth) authorises other entities to "use" information contained in the My Health Record system for purposes it permits, including: the Veterans' Affairs Department;[67] the Defence Department;[68] any "prescribed entity" (the Attorney-General's Department is one such entity);[69] and a "service operator for the purposes of the *Healthcare Identifiers Act 2010* [(Cth)]", which is either the Chief Executive Medicare or a body established by a Commonwealth law that the regulations prescribe to be a service operator.[70]

Potential unauthorised contraventions of patients' right to the confidentiality of their health information

Relevant legislation stipulates various measures designed to maintain, to a certain degree, the confidentiality of information in My Health Records, principally by controlling who accesses it, requiring the participants to report breaches of the system's security, and prosecuting any

---

[61] *My Health Records Act 2012* (Cth) s 70(4).
[62] *My Health Records Act 2012* (Cth) s 70(5).
[63] *My Health Records Rule 2012* (Cth) rr 4 (definition of "advanced access controls"), 6; *My Health Records Act 2012* (Cth) s 15(b)(i).
[64] *My Health Records Act 2012* (Cth) ss 4, 15(b)(ii).
[65] Minter Ellison, "Privacy Impact Assessment Report: Personally Controlled Electronic Health Record (PCEHR) System Opt-Out Model" for the Department of Health, 20 May 2015, 23.
[66] Minter Ellison, "Privacy Impact Assessment Report: Personally Controlled Electronic Health Record (PCEHR) System Opt-Out Model' for the Department of Health, 20 May 2015, 55.
[67] *My Health Records Act 2012* (Cth) sch 1, pt 2, div 2, cl 8.
[68] *My Health Records Act 2012* (Cth) sch 1, pt 2, div 2, cl 8.
[69] *My Health Records Act 2012* (Cth) sch 1, pt 2, div 2, cl 8; *My Health Records Regulation 2012* (Cth) reg 4.1.2.
[70] *My Health Records Act 2012* (Cth) sch 1, pt 2, div 2, cl 8; *Healthcare Identifiers Act 2010* (Cth) ss 5-6. *Health Identifiers Act 2010* (Cth) s 15: the *Healthcare Identifiers Act 2010* (Cth) permits a service operator not only to use that information, but also to collect and disclose identifying information about healthcare recipients or their authorised or nominated representatives "for the purposes of the My Health Record system".

unauthorised use and dissemination of healthcare recipients' records. Nevertheless, not only are those measures unlikely to be effective in protecting patients' information, but processes have not been built into the My Health Record system for properly scrutinizing access to and use and disclosure of information in it, and several features of the system, including the technology used to operate it, heighten the risk that the confidentiality of its records will be unlawfully compromised, either deliberately or unintentionally.

While the legislation enables countless individuals and entities to access information held in My Health Records, it creates no meaningful mechanisms for overseeing and monitoring who accesses the system and their use and dissemination of information stored in it. For instance, although healthcare provider organisations and contracted service providers must have written policies addressing how they authorise people to access the system and their security measures,[71] there is no provision for enforcing those policies or checking whether they have been satisfactorily implemented. Likewise, the maintenance officers of healthcare provider organisations must give the System Operator lists of all healthcare providers who are authorised to access the system via or on its behalf,[72] but the use and disclosure of information by individuals within those organisations – as well as by the participants' employees with whom the participants are permitted by the *My Health Records Act 2012* (Cth) to share their authority – could in practice be largely unscrutinised, and individuals without authority to access the system may do so unobserved.[73]

In the absence of adequate oversight, it is easy to foresee mistakes being made that undermine the confidentiality of patients' health information. Minter Ellison predicted that "privacy breaches" may occur if "clinical information" is erroneously "attributed to the wrong person",[74] and, indeed, in 2016, the Department of Human Services advised the Office of the Australian Information Commissioner that, in the 12 months to 30 June 2016, it "uploaded sensitive Medicare claims records to the wrong recipient's electronic health records 86 times".[75]

Unfortunately, it may not be difficult for the My Health Record system to be intentionally hacked into and information in it illegally disseminated. In 2015, the then Minister for Health and Aged Care, the Honourable Sussan Ley, noted that it is "important that we continue to … exercise effective controls over who is able to become a service provider in the digital health system".[76] Yet, even if contracted service providers are vetted, they in turn could employ sophisticated information technology personnel to assist them in providing information technology services to healthcare providers, who have the knowledge and capacity to distribute information from My Health Records surreptitiously and maliciously.

---

[71] *My Health Records Rule 2012* (Cth) rr 42(1), (4), 47(1), (4).
[72] *My Health Records Rule 2012* (Cth) r 27(1).
[73] Consumers eHealth Alliance, Submission No 12 to Department of Health Legislation Discussion Paper: Electronic Health Records and Health Identifiers, 19 July 2015, 6.
[74] Minter Ellison, "Privacy Impact Assessment Report: Personally Controlled Electronic Health Record (PCEHR) System Opt-Out Model" for the Department of Health, 20 May 2015, 72.
[75] Paris Cowan, "Medicare claims data sent to the wrong health records: Human Services admits privacy breach" *iTnews*, 14 November 2016, http://www.itnews.com.au/news/medicare-claims-data-sent-to-the-wrong-health-records-441292.
[76] Commonwealth, *Parliamentary Debates*, House of Representatives, 17 September 2015, 10528-30 (Sussan Ley).

The capacity for substantial sharing of information in the My Health Record system between myriad individuals and entities increases opportunities for the information it contains to be used and disclosed in unauthorised ways. The *My Health Records Act 2012* (Cth) explicitly authorises sharing of healthcare recipients' information between participants, other entities whom it authorises to "use" information contained in the My Health Record system for purposes it permits, and additional third parties,[77] but it does not prescribe any requirements to secure the safe transfer of information between them. Further, the system depends on the interoperability of numerous information technology systems; the Explanatory Memorandum notes, "the My Health Record system is an electronic system that interacts with the software and IT systems of a wide range of entities".[78] If any one of those systems is degraded, it could affect the entire My Health Record system and lead to widespread distribution of patients' health information.

The My Health Record system can potentially be operated automatically, free from human involvement, which further increases the scope for breaches of the system's security. The System Operator is permitted to arrange for the "use, under the System Operator's control, of computer programs for any purposes for which the System Operator may make decisions".[79] Purposes for which the System Operator is authorised to make decisions are unlimited, for the *My Health Records Act 2012* (Cth) states that it can "do anything incidental to or conducive to the performance" of its listed functions or further functions that are conferred on it.[80] It would be of great concern if some of the enumerated functions of the System Operator in particular were performed remotely by a computer due to the risk of inadvertent disclosure of patients' information, such as: establishing and maintaining mechanisms that enable healthcare recipients to obtain electronic access to a summary of the flows of information in relation to their My Health Records; operating the National Repositories Service; and establishing and operating a test environment for the system.[81]

The risk of breaches to the system's security is magnified, too, by the authorisation of the System Operator under the *My Health Records Act 2012* (Cth) "for the purposes of the operation or administration of the My Health Record system" to "hold and take", "process and handle" outside Australia records that it holds for the purposes of the system or information relating to those records.[82] Although the statute stipulates that this information must not include personal information about a healthcare recipient, or identifying information about an individual or entity,[83] it is unclear how adherence to this requirement would be monitored.

The *My Health Records Act 2012* (Cth) obliges the participants and entities that have been participants to report any possible unauthorised collection, use or disclosure of health information in a healthcare recipient's My Health Record or circumstances that may compromise the security or integrity of the system.[84] Nevertheless, by the time a report is

---

[77] See Danuta Mendelson and Gabrielle Wolf, "My [Electronic] Health Record" – Cui Bono (For Whose Benefit)?" (2016) 24 *Journal of Law and Medicine* 283, 291-2.
[78] Explanatory Memorandum, Health Legislation Amendment (eHealth) Bill 2015 (Cth) 70.
[79] *My Health Records Act 2012* (Cth) s 13A.
[80] *My Health Records Act 2012* (Cth) ss 15(n), (o).
[81] *My Health Records Act 2012* (Cth) ss 15 (h), (i), (ia).
[82] *My Health Records Act 2012* (Cth) s 77(2).
[83] *My Health Records Act 2012* (Cth) s 77(2).
[84] *My Health Records Act 2012* (Cth) s 75.

made and the System Operator suspends the offending individual or entity's access to the system,[85] or cancels or suspends the offending participant's registration,[86] it will probably be too late to prevent a serious infringement of the confidentiality of patients' records. The Consumers e-Health Alliance observes that it "may take many years to emerge" that there have been "criminal attacks [on the My Health Record system] resulting in misuse of data and fraud".[87] Likewise, the Explanatory Memorandum to the *My Health Records Act 2012* (Cth) envisages situations where corruption in one part of the system would probably only be uncovered once it had caused a substantial breach to the system's security: "a healthcare provider's clinical information system [could be] infected with a virus that allows a hacker to access information in the My Health Record system using the healthcare provider's IT or verification credentials";[88] and participants could have "malicious software in their IT systems that [connect] to the My Health Record system, and that malicious software may provide a 'back door' into health records in the My Health Record system".[89]

The Honourable Sussan Ley described the civil and criminal sanctions prescribed by the *My Health Records Act 2012* (Cth) for unauthorised collection, use and disclosure of healthcare recipients' information that is stored in the system[90] as "an important protection for consumers who have their health information contained within their health records".[91] Yet the existence of those penalties would be unlikely to deter some mischievous, improper and malevolent uses and disclosure of such information. Numerous situations in which people may be tempted to access and disseminate the information inappropriately, and would believe they would not be caught, can be envisaged. For instance, Minter Ellison predicted that individuals with access to the system would look up "the records of people they know personally, or public figures" for various reasons, such as "curiosity", "to create a nuisance", "gain leverage in a dispute", or profit from "selling the information".[92]

Substitution of patients' right to the confidentiality of their health information with the right to personal privacy

The fact that the *My Health Records Act 2012* (Cth) indicates that the *Privacy Act 1988* (Cth) – one of several privacy laws that Australians have enjoyed since 1988[93] – applies to the My Health Record system,[94] does not ensure the protection of patients' right to maintain the confidentiality of their health information. The My Health Record system, with its exceptions

[85] *My Health Records Rule 2012* (Cth) rr 17(1)-(2).
[86] *My Health Records Act 2012* (Cth) s 51(3).
[87] Consumers eHealth Alliance, Submission No 12 to Department of Health Legislation Discussion Paper: Electronic Health Records and Health Identifiers, 19 July 2015, 5.
[88] Explanatory Memorandum, Health Legislation Amendment (eHealth) Bill 2015 (Cth) 85.
[89] Explanatory Memorandum, Health Legislation Amendment (eHealth) Bill 2015 (Cth) 86.
[90] *My Health Records Act 2012* (Cth) ss 59-60.
[91] Commonwealth, *Parliamentary Debates*, House of Representatives, 17 September 2015, 10529 (Sussan Ley, Minister for Health and Minister for Sport).
[92] Minter Ellison, "Privacy Impact Assessment Report: Personally Controlled Electronic Health Record (PCEHR) System Opt-Out Model" for the Department of Health, 20 May 2015, 74-5.
[93] *Privacy Act 1988* (Cth); *Privacy and Personal Information Protection Act 1998* (NSW); *Health Records and Information Privacy Act 2002* (NSW); *Charter of Human Rights and Responsibilities Act 2006* (Vic); *Privacy and Data Protection Act 2014* (Vic); *Health Records Act 2001* (Vic); *Information Privacy Act 2009* (Qld); *Personal Information Protection Act 2004* (Tas); *Information Privacy Act 2014* (ACT); *Health Records (Privacy and Access) Act 1997* (ACT); *Human Rights Act 2004* (ACT). Similar legislation has been enacted in other countries.
[94] *My Health Records Act 2012* (Cth) ss 4, 72-3.

and authorisations, and its technology fail to implement effectively provisions of the *Privacy Act 1988* (Cth). But then the *Privacy Act 1988* (Cth) itself represents a culmination of changes that, since the last quarter of the 20th century, have steadily subsumed patients' right to medical confidentiality under a wider, though less legally-coherent, concept of a right to personal privacy.

The *My Health Records Act 2012* (Cth) states, "an act or practice that contravenes this Act in connection with health information included in a healthcare recipient's My Health Record … is taken to be, for the purposes of the *Privacy Act 1988* [Cth], an interference with the privacy of a healthcare recipient",[95] and "an authorisation to collect, use or disclose health information under this Act is also an authorisation to collect, use or disclose health information for the purposes of the *Privacy Act 1988* [(Cth)]".[96] Those purposes of the *Privacy Act 1988* (Cth) include: "to promote the protection of the privacy of individuals"; and "to promote responsible and transparent handling of personal information by entities".[97] The *Privacy Act 1988* (Cth) defines "personal information" 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".[98] "Health information" is encompassed within this definition, for the *Privacy Act 1988* (Cth) defines it as "information or an opinion" about an individual's health, "expressed wishes about the future provision of health services to the individual", or a "health service provided, or to be provided, to an individual" that is also "personal information".[99]

According to the Explanatory Memorandum to the *My Health Records Act 2012* (Cth), this statute "ensures that any use or disclosure [of information] done in accordance with the My Health Records Act does not contravene the Privacy Act [*1988* (Cth)]".[100] Yet, by permitting third parties, lawfully and without authority, to collect, access, use and distribute healthcare recipients' health information, the My Health Record system and its technology are enabling an interference with patients' privacy and neglecting to promote their privacy or responsible and transparent handling of their data. Such disregard for provisions of the *Privacy Act 1988* (Cth) ignores Australians' wishes. Timothy Pilgrim PSM, the Australian Privacy Commissioner, noted in 2016 that:

> "Australians continue to experience an expansion of the scope and diversity of how their personal information is being captured and used by public and private organisations, embracing new products and services which rely on personal information for delivery".[101]

---

[95] *My Health Records Act 2012* (Cth) s 73.
[96] *My Health Records Act 2012* (Cth) s 72.
[97] *Privacy Act 1988* (Cth) ss 2A (a), (d).
[98] *Privacy Act 1988* (Cth) s 6.
[99] *Privacy Act 1988* (Cth) s 6FA. Section 5 of the *My Health Records Act 2012* (Cth) confirms that references to "health information" in this statute have the same meaning as the definition of this term in the *Privacy Act 1988* (Cth).
[100] Explanatory Memorandum, Health Legislation Amendment (eHealth) Bill 2015 (Cth) 83.
[101] Timothy Pilgrim PSM, "Annual Report 2015-2016" Australian Privacy Commissioner; Australian Information Commissioner 27 September 2016 https://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201516/part-1-overview

Yet, despite endorsing such innovations and being active and revealing personal information on social media sites (including Facebook, Twitter and Instagram), Australians have clear views about what government agencies should or should not do with their personal data. A 2013 report by the Office of the Australian Information Commissioner on "Community Attitudes to Privacy" found that Australians are in "almost universal agreement" that government agencies "misuse personal information" when: (1) they reveal it "to other customers"/third parties (97%); (2) they use it "for a purpose other than the one [for which] it was provided" (97%); and (3) "an organisation that a person has not dealt with before" collects his/her personal information (96%).[102] The My Health Record system enables these three practices to occur in relation to patients' most sensitive health information.

Relevantly, the reason why the *Privacy Act 1988* (Cth) does not adequately protect individuals' right to the confidentiality of their information is that such a concept was not at the forefront of the right to privacy as it was originally conceived.[103] In their 1890 seminal article on "*The Right to Privacy"*,[104] Samuel Warren and Louis Brandeis defined privacy simply as a "right to be left alone".[105] Ever since then, however, legal scholars have been trying to provide a more systematic definition of this notion. In his 1992 article, which traced the evolution of the concept of privacy, Ken Gormley[106] identified four major legal theories of privacy in American scholarship:

(1) privacy as "an expression of one's *personality* or *personhood,* focusing upon the right of the individual to define his or her essence as a human being" (Roscoe Pound, 1915; Paul Freund, 1975);[107]

(2) privacy as an aspect of "*autonomy* - the moral freedom of the individual to engage in his or her own thoughts, actions and decisions" (Louis Henkin);[108]

(3) privacy as a right that enables citizens "to *regulate information* about themselves", and thus control their relationships with other human beings, such that individuals have the right to decide "when, how, and to what extent information about them is communicated to others" (Alan Westin; Charles Fried);[109]

(4) privacy as comprising two components: "secrecy, anonymity and solitude,"[110] and "repose, sanctuary and intimate decision".[111]

---

[102] Office of the Australian Information Commissioner, Community Attitudes to Privacy Report (2013), at p 19 https://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-reports/2013-community-attitudes-to-privacy-survey-report.pdf

[103] Friedman LM in *Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety, and Privacy*, Palo Alto: Stanford University Press, 2007, argues that 'privacy law' was an aspect on a number of legal doctrines, such as defamation, slander and libel designed to protect reputation.

[104] Samuel D. Warren & Louis D. Brandeis, 'The Right to Privacy' (1890) 4 *Harv. L. Rev.* 193.

[105] Samuel D. Warren & Louis D. Brandeis, 'The Right to Privacy' (1890) 4 *Harv. L. Rev.* 193 at 193, 195. According to Ken Gormley, 'One Hundred Years of Privacy' (1992) *Wis. L. Rev*. 1335 at 1335, this phrase was used by Judge Thomas M. Cooley in *Cooley On Torts* 29 (2d ed. 1888).

[106] Ken Gormley, 'One Hundred Years of Privacy' (1992) *Wis. L. Rev*. 1335 at 1337-1338.

[107] Roscoe Pound, *Interests in Personality,* 28 *Harv. L. REV.* 343 (1915) and Paul A. Freund, Address to the American Law Institute (May 23, 1975), quoted in 52 *A.L.I. PROC.* 574-75 (1975).

[108] Louis Henkin, '*Privacy and Autonomy*', 74 *Colum. L. Rev.* 1410, 1425 (1974);

[109] Alan F. Westin, *Privacy and Freedom* 7-13 (1967) at 7; Charles Fried, 'Privacy', (1968) 77 *Yale L.J*. 475, 477-78.

[110] Ruth Gavison, 'Privacy', (1980) 89 *Yale L.J*. 421, 433.

Writing in 2008, Jon L Mills re-conceptualised these theories in terms of four rights associated with overlapping spheres of:

> "privacy protection from intrusions by the government, private entities, or individuals: freedom of personal autonomy; the right to control personal information; the right to control property; and the right to control and protect personal physical space".[112]

Mills considered that control "of personal information is the least developed sphere of privacy and the sphere with the least legal protection".[113]

In Australia, the *Privacy Act 1988* (Cth) was amended in 2014 to include 13 Australian Privacy Principles (APPs) in its Schedule 1 that are legally binding[114] and apply to several, but not all government agencies,[115] all private sector and not-for-profit organisations with an annual turnover of more than $3 million, and all private health service providers and some small businesses (collectively called "APP entities").[116] The first two APPs are most relevant to the notion of personal privacy, but neither of them offers adequate protection of the confidentiality of patients' health records.

APP 1 requires "open and transparent management of personal information".[117] In particular, entities that come within the purview of the *Privacy Act 1988* (Cth) must be "open" about:

> "(a) the kinds of personal information that the entity collects and holds; (b) how the entity collects and holds personal information; (c) the purposes for which the entity collects, holds, uses and discloses personal information; (d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information … (f) whether the entity is likely to disclose personal information to overseas recipients; (g) if the entity is likely to disclose personal information to overseas recipients--the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy".[118]

There are several problems with this principle. While the first two requirements are relatively clear, the phrasing of obligation (c) is somewhat opaque. Specifically, it does not explicitly state that entities must disclose *all* of the purposes for which they collect, hold, use and disclose personal information and, indeed, the list of the "objects" of the *My Health Record Act 2012* (Cth) in that statute is clearly not exhaustive. Those goals are stated to be: (a)

---

[111] Gary L. Bostwick, Comment, *A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision*, 64 (1976) CAL. L. REV. 1447.
[112] Jon L Mills, *Privacy: The Lost Right* (Oxford University Press, 2008) 13-14.
[113] Jon L Mills, *Privacy: The Lost Right* (Oxford University Press, 2008) 16.
[114] *Privacy Act 1988* (Cth) s 15.
[115] Section 7 of the *Privacy Act 1988* (Cth) exempts from its operation federal courts, Norfolk Island courts, Ministers, the Integrity Commissioner; the ACC; Royal Commissions; Commissions of inquiry; intelligence agencies; the Defence Intelligence Organisation, the Australian Geospatial-Intelligence Organisation or the Australian Signals Directorate of the Defence Department; the Australian Security Intelligence Organisation; the Australian Secret Intelligence Service.
[116] *Privacy Act 1988* (Cth) ss 6, 6C-6F, Office of the Australian Information Commissioner https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles
[117] Section 6 of the *Privacy Act 1988* (Cth) indicates that section 187LA of the *Telecommunications (Interception and Access) Act 1979* extends the meaning of "personal information" to cover information kept under Part 5-1A of that Act, which includes information relating to "(a) the individual; or (b) a communication to which the individual is a party".
[118] *Privacy Act 1988* (Cth) sch 1.4 http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/sch1.html

helping to "overcome the fragmentation of health information"; (b) improving "the availability and quality of health information"; (c) reducing "the occurrence of adverse medical events and the duplication of treatment"; and (d) improving "the coordination and quality of healthcare provided to healthcare recipients by different healthcare providers".[119] Unstated, but evident purposes of the collection, use and disclosure of patients' health information under the My Health Record system are also research and population health surveillance.[120]

In addition, while (f) and (g) require the entities to be open about their likelihood of disclosing personal information to overseas recipients, APP 1 imposes no obligations of openness and transparency on the entities regarding their disclosure of personal information to recipients within Australia. Recipients of information stored on the My Health Record system are, among others, Australian intelligence agencies (through the Defence Department). There are many cases in which personal, sensitive[121] health information would be vital data for intelligence agencies that are tasked with safeguarding national interests and the well-being of Australians. However, as noted above, the legislation fails to incorporate significant controls (such as provisions governing the attribution of personal responsibility for breaches of privacy) on third parties, including law enforcement and national security agencies, that access, use, collect, distribute and manage clinical information that we provide to our healthcare professionals.

A full, candid disclosure of all the purposes of the My Health Record system would enhance the community's trust of the government. The government's unwillingness to reveal many of the non-therapeutic, non-health-related purposes of collecting and managing data under the *My Health Records Act 2012* (Cth) could be explained by its reluctance to acknowledge that, once patients' health records are digitized, under the My Health Record system their right to maintain the confidentiality of their health information becomes illusory.

Can the second APP protect patients' right to the confidentiality of their health information? APP 2 provides that "individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter".[122] While this principle appears to enable protection of patients' right to confidentiality, technological developments have undermined the capacity for maintaining anonymity and pseudonymity. Indeed, "the notion of perfect anonymization has been exposed as a myth".[123] In the wake of "big data" and advanced algorithms, it takes relatively little time and skill to

[119] *My Health Records Act 2012* (Cth) s 3. For a discussion of whether these statutory goals have been achieved, see Danuta Mendelson and Gabrielle Wolf "My [Electronic] Health Record" – Cui Bono (for whose Benefit)?" (2016) 24 *Journal of Law and Medicine* 283-296.
[120] Danuta Mendelson and Gabrielle Wolf "My [Electronic] Health Record" – Cui Bono (for whose Benefit)?" (2016) 24 *Journal of Law and Medicine* 283, 293-6.
[121] The term "sensitive information" refers to "a type of personal information and includes information about an individual's: health (including predictive genetic information); racial or ethnic origin; political opinions; membership of a political association, professional or trade association or trade union; religious beliefs or affiliations; philosophical beliefs; sexual orientation or practices; criminal record; biometric information that is to be used for certain purposes; biometric templates." Office of the Privacy and Information Commissioner, "Australian Privacy Principles" https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles
[122] *Privacy Act 1988* (Cth) sch 1, Australian Privacy Principle 2.1.
[123] Ira S. Rubinstein and Woodrow Hartzog, "Anonymization and Risk" (2016) 91 *Wash. L. Rev.* 703 at 704.

identify correctly individuals[124] and health-related information from anonymized data sets.[125] For example, in September 2016, Melbourne University researchers decrypted doctors' ID numbers from the "de-identified" Medicare and Pharmaceutical Benefits Scheme claims data-set dating back to 1984[126] that the Department of Health uploaded onto its open data portal in August 2016.[127]

Conclusion

Technological advances have made possible the development of a system of national electronic health records. While the digitization of health information does not inherently undermine the confidentiality of patients' health information, the My Health Record system that the Commonwealth Parliament has legislated to create, and the technology used to operate it, has enormous potential to do so. The old adage, "knowledge is power",[128] can be interpreted in several ways, including as a shorthand for saying that, the more the State knows about its citizens, the greater the power that it can exert over them for good and for bad. The My Health Record system exponentially expands the knowledge that Australian governments, but also other third parties, can acquire about individuals' health information and, consequently, their authority over them. The creation of the My Health Record system has coincided with the substitution of the concept of patients' right to the confidentiality of their health information with a much broader and less defined right to personal privacy. Both developments have significantly eroded our former capacity to secure information disclosed in the course of therapeutic relationships with our health practitioners.

[124] In December 2016, using software to filter through a database of mobile, internet and location metadata of the kind "that has been retained and made available to Australian government agencies for the past year", teams of three primary school students tracked down "the mock corporate whistleblower" within two hours. James Purtill, "How pre-teens using metadata found a whistleblower in two hours" ABC, Mon 12 Dec 2016, 10:34pm http://www.abc.net.au/triplej/programs/hack/how-team-of-pre-teens-found-whisteblower-using-metadata/8113668

[125] A Narayanan, V Shmatikov, Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset). In: Proceedings of the (2008) IEEE Symposium on Security and Privacy SP'08, pp. 111–125; Adam Tanner "Strengthening Protection of Patient Medical Data" The Century Foundation, January 10, 2017 https://tcf.org/content/report/strengthening-protection-patient-medical-data/.

[126] Paris Cowan, "Govt releases billion-line 'de-identified' health dataset" *iTnews* 15 August 2016 http://www.itnews.com.au/news/govt-releases-billion-line-de-identified-health-dataset-433814

[127] Paris Cowan, "Health pulls Medicare dataset after breach of doctor details" *iTnews* 26 September 2019, http://www.itnews.com.au/news/health-pulls-medicare-dataset-after-breach-of-doctor-details-438463

[128] Latin: "scientia potentia est"; Sir Francis Bacon in *Meditationes Sacrae* (1597) referred to "ipsa scientia potestas est" (knowledge itself is power) as an aspect of God's power.