30 August 2017

Senate Finance and Public Administration Committees
PO Box 6100
Parliament House
Canberra ACT 2600

By email: fpa.sen@aph.gov.au

Dear Committee Secretary

Submission to the Senate Finance and Public Administration References Committee's inquiry into the circumstances in which Australians' personal Medicare information has been compromised and made available for sale illegally on the 'dark web'

We thank the Senate Finance and Public Administration References Committee for the opportunity to make a submission to its inquiry into the circumstances in which Australians' personal Medicare information has been compromised and made available for sale illegally on the 'dark web'.

Our submission concerns legal aspects of data security issues associated with the My Health Record system and related matters.

Please find attached two of our publications, both of which were peer-reviewed: 'My Electronic Health Record: For Whose Benefit (Cui Bono)?' (2016) 24 *Journal of Law and Medicine* 283; and 'Health Privacy and Confidentiality' in Ian Freckelton and Kerry Peterson (eds), *Tensions and Traumas in Health Law* (Federation Press, 2017) (forthcoming).

In these publications, we have discussed key concerns that we have with the My Health Record system, which we believe are relevant to the Committee's current inquiry. Specifically:

- The My Health Record system permits innumerable individuals and entities to access information that has historically been confined to the therapeutic relationship between health practitioner and patient;
- There are no meaningful mechanisms for overseeing and monitoring who accesses the My Health Record system, and the use and dissemination of information stored in it;
- Patients may not have any knowledge of or control over, or have consented to, third parties' extensive capacity to collect, use and disclose their confidential information for the purposes of the My Health Record system; and
- Given the structure of the My Health Record system, there is a high risk of intentional and inadvertent breaches of the system's security, enabling third parties' unauthorised access to and disclosure of patients' confidential information.

We are happy to provide any further information that might be useful to the Committee's inquiry.

Please be advised that we are both employed in the Law School at Deakin University, but the views expressed in this letter and in our publications represent our own views and not those of Deakin University.

Yours sincerely,

Professor Danuta Mendelson and Dr Gabrielle Wolf

Professor Danuta Mendelson
MA, LLM, PhD
Chair in Law (Research)
Deakin School of Law
Faculty of Business & Law
Deakin University

Dr Gabrielle Wolf
Senior Lecturer
School of Law
Faculty of Business & Law
Deakin University

Legal Issues

Editor: Danuta Mendelson

"MY [ELECTRONIC] HEALTH RECORD" – CUI BONO (FOR WHOSE BENEFIT)?

By Danuta Mendelson and Gabrielle Wolf[*]

We examine the operation of Australia's national electronic health records system, known as the "My Health Record system". Pursuant to the My Health Records Act 2012 (Cth), every 38 seconds new information about Australians is uploaded onto the My Health Record system servers. This information includes diagnostic tests, general practitioners' clinical notes, referrals to specialists and letters from specialists. Our examination demonstrates that the intentions of successive Australian Governments in enabling the collection of clinical data through the national electronic health records system, go well beyond statutorily articulated reasons (overcoming "the fragmentation of health information"; improving "the availability and quality of health information"; reducing "the occurrence of adverse medical events and the duplication of treatment"; and improving "the coordination and quality of healthcare provided to healthcare recipients by different healthcare providers"). Not only has the system failed to fulfil its statutory objectives, but it permits the wide dissemination of information that historically has been confined to the therapeutic relationship between patient and health practitioner. After considering several other purposes for which the system is apparently designed, and who stands to benefit from it, we conclude that the government risks losing the trust of Australians in its electronic health care policies unless it reveals all of its objectives and obtains patients' consent to the use and disclosure of their information.

INTRODUCTION

On 27 November 2015, the substantially amended *Personally Controlled Electronic Health Records Act 2012* (Cth) was enacted as the renamed *My Health Records Act 2012* (Cth).[1] The major amendment – Schedule 1 to the *My Health Records Act 2012* (Cth) – enables a non-consensual "opt-out" automated system of registering patients, labelled "healthcare recipients", in the My Health Record system. Pursuant to the *My Health Records (Opt-out Trials) Rule 2016* (Cth), Sussan Ley, the Minister for Health, initiated "in mid-June 2016" two opt-out model trials, one in Northern Queensland and another in the Nepean Blue Mountains.[2] The *My Health Records Act 2012* (Cth) provides that, should the Minister decide:

[*] Danuta Mendelson, Chair in Law (Research), Deakin Law School, Faculty of Business and Law, Deakin University; Gabrielle Wolf, Lecturer, Deakin Law School, Faculty of Business and Law, Deakin University.

Correspondence to: 221 Burwood Highway, Burwood, Victoria, 3125, Australia.

[1] The *Health Legislation Amendment (eHealth) Act 2015* (Cth) also amended the *Healthcare Identifiers Act 2010* (Cth), the *Privacy Act 1988* (Cth), the *Copyright Act 1968* (Cth), the *Health Insurance Act 1973* (Cth) and the *National Health Act 1953* (Cth).

[2] Australian Digital Health Agency, *My Health Record for Northern Queensland and Nepean Blue Mountains Areas* (last updated 27 May 2016) <https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/trials>.

> that the opt-out model results in participation in the My Health Record system at a level that provides value for those using the My Health Record system, the Minister may make My Health Records Rules applying the opt-out model to all healthcare recipients in Australia.[3]

These developments illustrate a profound conceptual shift in the Australian Government's approach to clinical data since the proposal in 2000 by the National Electronic Health Records Taskforce (Australia) (Taskforce) for a nationally co-ordinated and distributed system of electronic health records,[4] and the subsequent implementation of this scheme. Historically, at least from the time of Hippocratic writing,[5] health practitioners' clinical records have contained only information imparted by parties to a therapeutic relationship and were used solely for patients' benefit.[6] This is not the case under the national electronic health records scheme, in which patients are labelled "consumers" or "healthcare recipients"[7] and their clinical records, together with documents uploaded from other agencies, are outsourced to data management services. As of 2016, this information is being uploaded onto the system in sufficient volume, velocity and variety (text, diagnostic images and sounds) to warrant it being described as "Big Data". The ever-increasing collection of datasets can be subjected to Big Data analytics (predictive analytics, user behaviour analytics, business analytics), and medical, sociological, economic and other research. They can also be commodified and exploited for other purposes that are similarly removed from the longstanding therapeutic objectives of creating clinical records.

Electronic health (eHealth) initiatives, in private medical and other healthcare practices and facilities, as well as in some public hospitals, were introduced in the 1990s. They tended to be self-contained and independent of the Australian Government. In 1999, however, the government established the Taskforce, which in 2000 delivered its report entitled, *A Health Information Network for Australia*.[8] The Taskforce envisaged that a system, to be called Health*Connect*, would comprise "a secure network as a basis for exchanging health information (including personal and other health information)". Its principal aim was:

> to assist consumers [to] establish a record of their healthcare interactions, and for providers of healthcare (in partnerships with consumers) to make better-informed decisions at the point of care. Participation both on the part of consumers and providers is voluntary – with consumers agreeing to make their personal health information (in whole or in part) available to nominated providers for specified purposes.[9]

From the outset, the proposal prompted concern that the system was not grounded in medical ethics and approached health records as a mere commodity. Medical record-keeping specialists were apprehensive about the system being "hijacked by individuals who have technical skills but no real understanding of the [health] data they seek to manage".[10] While the Taskforce emphasised the need for explicit consent by "consumers" to make their information available, the "specified purposes" were not formulated, providing a leeway for the electronic records to be used not only to assist in patients' clinical care, but also for other unstipulated, non-therapeutic objectives.

---

[3] *My Health Records Act 2012* (Cth) Sch 1 cl 2(1).

[4] National Electronic Health Records Taskforce (Australia), *A Health Information Network for Australia: Report to Health Ministers* (Department of Health and Aged Care, 2000).

[5] D Mendelson, "Medical Duty of Confidentiality in the Hippocratic Tradition and Jewish Medical Ethics" (1998) 5 JLM 227; D Mendelson, "Aspects of Causation in Hippocratic Medicine and Roman Law of Delict" in I Freckelton and D Mendelson (eds), *Causation in Law and Medicine* (Ashgate, 2002) 58-83.

[6] D Mendelson, "Travels of a Medical Record and the Myth of Privacy" (2003) 11 JLM 136; D Mendelson, "Electronic Medical Records: Perils of Outsourcing and the Privacy Act 1988 (Cth)" (2004) 12 JLM 8; L Iacovino, D Mendelson and M Paterson, "Privacy Issues, Health*Connect* and Beyond" in I Freckelton and K Peterson (eds), *Disputes and Dilemmas in Health Law* (Federation Press, 2006) 604-622.

[7] See *Health Legislation Amendment (eHealth) Bill 2015* (Cth) Sch 3 "Renaming consumers as healthcare recipients".

[8] National Electronic Health Records Taskforce (Australia), n 4.

[9] National Electronic Health Records Taskforce (Australia), n 4, 122.

[10] S Walker and J Craig, "e-Health – A New World Order for Health Information Managers" (2002) 30(1) *Health Information Management Journal* <http://www.himaa.org.au/memberarea/journal/30_1_2001/walker/walker.html>.

The Health*Connect* scheme, scheduled to commence in 2004,[11] did not materialise;[12] however, the Taskforce report's language was adopted by Deloitte Touche Tohmatsu, a multinational professional services company,[13] which in 2008 was commissioned "to develop a strategic framework and plan to guide national coordination and collaboration in E-Health".[14] This framework was further developed by the National Health and Hospitals Reform Commission in its 2009 report entitled, *A Healthier Future for All Australians*. That report recommended the "introduction of a person-controlled electronic health record for each Australian", which it promised would provide "one of the most important systemic opportunities to improve the quality and safety of health care, reduce waste and inefficiency, and improve continuity and health outcomes for patients".[15] The Australian Government accepted these recommendations, and two intertwined statutes were enacted: the *Healthcare Identifiers Act 2010* (Cth);[16] and the *Personally Controlled Electronic Health Records Act 2012* (Cth), now reincarnated as the *My Health Records Act 2012* (Cth).

The Commonwealth Parliament's alteration of the name "Personally Controlled Electronic Health Record" to "My Health Record"[17] is deeply symbolic. The government explained that the new title "is intended to better reflect the partnership between individuals and healthcare providers in healthcare".[18] Arguably, however, its actual objective is to impart to Australians a sense of ownership of their electronic health records, and thus foster their trust in the system. Studies have demonstrated "that simply by providing users [with] a feeling of control, businesses can encourage the sharing of data regardless of whether or not users actually gained control".[19] The implications of the new name – that the networked electronic health records are controlled by patients exclusively for their benefit and use, and thus enabling a "partnership between individuals and healthcare providers" – are inaccurate.

Moreover, the fact that, "smartphone penetration [in Australia] approached 89% by early 2016",[20] renders anachronistic the notion that the government, through its My Health Record system, is in the best position to enable patients' "control" over their health records, and to improve "the coordination

[11] On 10 March 2004, the Australian Government's Department for Health and Ageing announced that the whole-of-state implementations in Tasmania and South Australia would commence in July 2004, then moving to implementation in larger States, with Queensland as a priority. The announcement was available at the time on <http://www.health.gov.au/medicareplus>; however, like the National Electronic Health Records Taskforce (Australia) report (see n 4), it is no longer available even on the National Library's Australian Government Web Archive portal (which only goes back to January 2008).

[12] D Mendelson, "Health*Connect* and the Duty of Care: A Dilemma for Medical Practitioners" (2004) 12 JLM 69; Mendelson (2004), n 6; Iacovino, Mendelson and Paterson, n 6.

[13] Deloitte Touche Tohmatsu, *About Deloitte* <http://www2.deloitte.com/au/en/pages/about-deloitte/articles/about-deloitte.html>.

[14] See the "Foreword" in Australian Health Ministers' Conference, *National E-Health Strategy Summary* (Victorian Department of Human Services, 2008) <http://www.health.gov.au/internet/main/publishing.nsf/content/69B9E01747B836DCCA257BF0001DC5CC/$File/Summary%20National%20E-Health%20Strategy%20final.pdf>.

[15] National Health and Hospitals Reform Commission, *A Healthier Future For All Australians: Final Report* (Commonwealth of Australia, 2009) 8. The Commission noted that, "giving people better access to their own health information through a person-controlled electronic health record is also essential to promoting consumer participation, and supporting self-management and informed decision-making" <http://www.health.gov.au/internet/nhhrc/publishing.nsf/Content/1AFDEAF1FB76A1D8CA257600000B5BE2/$File/EXEC_SUMMARY.pdf>.

[16] For a discussion of this legislation, see D Mendelson, "Healthcare Identifiers Legislation: A Whiff of Fourberie" (2010) 17 JLM 660; D Mendelson and A Rees, "Medical Confidentiality and Patient Privacy" in B White, F McDonald and L Willmott (eds), *Health Law in Australia* (Thomson Reuters, 2nd ed, 2014) 371.

[17] Explanatory Memorandum, *Health Legislation Amendment (eHealth) Bill 2015* (Cth) 2.

[18] Explanatory Memorandum, *Health Legislation Amendment (eHealth) Bill 2015* (Cth) 2.

[19] Cited in O Tene and J Polonetsky, "Big Data for All: Privacy and User Control in the Age of Analytics" (2013) *Northwestern Journal of Technology and Intellectual Property* 239, 261, with reference to Alessandro Acquisti's work reported in L Brandimarte et al, "Misplaced Confidences: Privacy and the Control Paradox" (Paper presented at the Ninth Annual Workshop On The Economics Of Information Security, Harvard University, Massachusetts, 7-8 June 2010).

[20] Smartphones, and to a lesser extent tablets, are being used to access the internet. H Lancaster, *Australia – Mobile Communications – Smartphones, Tablets and Handset Market* (2016) <https://www.budde.com.au/Research/Australia-Mobile-Communications-Smartphones-Tablets-and-Handset-Market>.

and quality of healthcare provided to healthcare recipients by different healthcare providers".[21] EHealth apps for smartphones allow individuals total control over collecting and storing medical information (for instance, about their allergies, illnesses and medical conditions), diagnostic imaging, pathology, pharmacy, immunisation, and other records independently of the My Health Record system. In general, these smartphone apps have mechanisms for both, the protection of health data through encryption and passwords, and for enabling access to critical medical information in emergencies.[22] Accessible online and offline, records on smartphone apps can be forwarded (encrypted) to and by healthcare providers.

The potential non-therapeutic uses of electronic health records have not been entirely hidden from the public. For example, in 2015, Mr Martin Bowles, Secretary of the Federal Department of Health, requested Deloitte Touche Tohmatsu to provide a "perspective on the proposed legislative changes to *Electronic Health Records [Act 2012* (Cth)] and *Healthcare Identifiers [Act 2010* (Cth)]".[23] Deloitte Touche Tohmatsu responded with a "vision and roadmap for eHealth in Australia", noting that:

> Over time, as the breadth and depth of data that is held in the shared repositories [of the My Health Record system] grows there is also the opportunity to use this data set as a means through which to support translational research[24] and population health surveillance.[25]

In addition, the *My Health Records Act 2012* (Cth) defines the My Health Record system as a means of assembling information from many sources:

> so that it can be made available, in accordance with the healthcare recipient's wishes *or in circumstances specified in this Act*, to facilitate the provision of healthcare to the healthcare recipient *or for purposes specified in this Act*.[26]

Circumstances and purposes articulated in the statute include provision of information captured by the My Health Record system to courts and tribunals,[27] as well as use of this information for law enforcement purposes.[28] Although other uses of this information and their scope are yet to be explicitly revealed,[29] it is clear that information previously considered to be within the private domain *of individuals* and under the control of their chosen health providers is being reconceptualised as shared data *about individuals*, to be collected, distributed and managed by government and private entities.

We first explain the operation of the very complex My Health Record system, and then examine the purposes of the accumulation of eHealth data in the system and whom the My Health Record system may be intended to benefit.

---

[21] *My Health Records Act 2012* (Cth) s 3.

[22] See, eg <http://www.mymedicalapp.com/>; <http://www.freehealthtrack.com/>; <http://www.myhealthdataapp.com/>; <http://www. apple.com/au/ios/health/>.

[23] Deloitte Touche Tohmatsu, *Accelerating Delivery of Benefits from Australia's Investment in National eHealth System* (2015) 1 <https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/consultation-submissions/$FILE/069%20-%20Deloitte%20Touche%20Tohmatsu.PDF>.

[24] "Translational research" is defined by the European Society for Translational Medicine as "an interdisciplinary branch of the biomedical field supported by three main pillars: benchside [basic science], bedside and community": RJ Cohrs et al, "Translational Medicine Definition by the European Society for Translational Medicine" (2015) 2(3) *New Horizons in Translational Medicine* 86 <http://www.newhorizonsintranslationalmedicine.com/article/S2307-5023(14)00078-2/abstract>.

[25] Deloitte Touche Tohmatsu, n 23, 4.

[26] *My Health Records Act 2012* (Cth) s 5 (definition of "My Health Record system") (emphasis added).

[27] *My Health Records Act 2012* (Cth) s 69.

[28] *My Health Records Act 2012* (Cth) s 70.

[29] As of 13 October 2016, consultation on "Secondary Use of My Health Record Data" was postponed by the Australian Digital Health Agency: <https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/home>.

BACKGROUND

The *Healthcare Identifiers Act 2010* (Cth) provides the technological infrastructure for the electronic health records system through the creation of electronic personal identifiers. Under this statute, the Service Operator – which can be the Chief Executive Medicare or a body established by a Commonwealth law and prescribed to be such by the regulations[30] – assigns three kinds of unique, non-transferable numbers to different individuals and entities:

- Individual Healthcare Identifiers to every person enrolled under the Medicare scheme or registered with the Department of Veterans' Affairs;
- Individual Healthcare Provider Identifiers to each clinical healthcare provider registered with the Healthcare Identifiers service;[31] and
- Healthcare Provider Identifiers–Organisation to organisations that deliver health care.

These unique numbers enable "sharing", that is, matching, cross-matching, and transfer of information contained in the electronic health records across healthcare provider organisations, healthcare providers and agencies. Individual Healthcare Identifiers provide "building blocks"[32] for the national Personally Controlled Electronic Health Records system, which came into operation in July 2012. Its aim is to provide a "secure, national infrastructure to support a shared electronic health record" that can be accessed by patients and their authorised healthcare providers and healthcare organisations.[33]

The term "record" was defined in the *Personally Controlled Electronic Health Records Act 2012* (Cth) as including "a database, register, file or document that contains information in any form (including in electronic form)".[34] The intention is that each record will contain constantly updated information on patients' medication,[35] allergies, diagnoses and treatment, Medicare Benefit and Pharmaceutical Benefit claims data, records of visits to healthcare providers, discharge summaries from hospitals, referrals to specialists, letters from specialists, organ donation statuses, locations of advance care directives, emergency contacts, immunisations and early developmental history of children (including voluntary contributions by their parents).[36]

Despite the government's claim that there was "overwhelming support for continuing implementation of a consistent electronic health record system for all Australians",[37] by 2015, very few patients had voluntarily opted into it, and only a tiny proportion of general practitioners had uploaded medical information onto the system. According to the *Sixth Clinical Safety Review of the My Health Record System*,[38] between 2013 and 2015:

---

[30] *Healthcare Identifiers Act 2010* (Cth) s 6.

[31] J Kelly, *Healthcare Identifiers Act and Service Review – Final Report* (Department of Health, 2013) [1.3]: "The Australian Health Practitioner Regulation Agency (AHPRA) is a Trusted Data Source responsible for assigning identifiers for registered Healthcare Providers that fall within AHPRA's area of responsibility. Identifiers for other providers not registered by AHPRA are assigned by DHS. The Department of Veterans' Affairs is also a Trusted Data Source for the HI Service": <http://www.health.gov.au/internet/publications/publishing.nsf/Content/hlth-id-act-srvc-review~1.~1.3>.

[32] Australian Health Ministers' Conference, n 14.

[33] J Halton, "Executive Summary" in Personally Controlled Health Record Operator, *Annual Report 2012-2013* (2013) <http://www.health.gov.au/internet/publications/publishing.nsf/Content/pcehr-system-operator-annual-report-2012-2013-toc~1-exec-summary>.

[34] *Personally Controlled Electronic Health Records Act 2012* (Cth) s 5 (definition of "record"). This definition has been retained in the *My Health Records Act 2012* (Cth) s 5.

[35] Through the eTP Electronic Transfer of Prescriptions system, "secure exchange of prescription information between prescribers and dispensers is … [supposed] to use the HI Service to identify the parties involved". See Kelly, n 31, [1.3].

[36] Australian Digital Health Agency, *Managing Your Child's My Health Record* (last updated 29 March 2016) <https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/find-out-more?OpenDocument&cat=Managing%20your%20child%27s%20My%20Health%20Record>.

[37] Explanatory Memorandum, *Health Legislation Amendment (eHealth) Bill 2015* (Cth) 1 (referring to Kelly, n 31).

[38] PwC, *Sixth Clinical Safety Review of the My Health Record System* (Australian Commission on Safety and Quality in

> approximately 8,000 ES [electronic summaries][39] documents [were] uploaded to the [now called] My Health Record system. Almost 90% of these summaries were created by just 20 healthcare organisations, and these organisations appear to mostly utilise two desktop GP clinical software products available on the market.[40]

In response, as noted above, a new section 4A, together with Schedule 1 in the *My Health Records Act 2012* (Cth) changed the consent-based system ("opt-in") that previously underpinned the Personally Controlled Electronic Health Record scheme to a non-consensual "opt-out model for the participation of healthcare recipients in the My Health Record system".[41] Under the "opt-out" model, patients are automatically registered and the onus is on each individual to initiate and complete the opting out process. The legislation does not provide procedures for this process, but the My Health Record website indicates that it is possible to opt-out online, by calling a help line or visiting a Medicare Service Centre.[42]

The Parliamentary Joint Committee on Human Rights scrutinised the *Health Legislation Amendment (eHealth) Bill 2015* (Cth) pursuant to the *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth).[43] The Committee found that the "opt-out" scheme limited human rights, and queried:

> whether the objective of the bill, in automatically uploading personal sensitive health information onto the database in an attempt to drive increased use of the database by healthcare professionals, is a legitimate objective for the purposes of international human rights law.[44]

Nevertheless, legislation for the "opt-out" model was enacted, though it is not yet operative.[45]

How Does the My Health Record System Operate?

Tellingly, healthcare recipients are omitted from the definition in the *My Health Records Act 2012* (Cth) of a "participant in the My Health Record system".[46] The "participants" in the My Health Record system who help facilitate its operation that the Act identifies include: "registered healthcare provider organisations";[47] the operator of the National Repositories Service (discussed below);[48] "registered repository operators" (including the Chief Executive Medicare), who hold records of information included in My Health Records for the purposes of the My Health Record system;[49] "registered portal operators", who operate "an electronic interface that facilitates access to the My

Healthcare, 2015) <http://www.safetyandquality.gov.au/wp-content/uploads/2016/05/Sixth-Clinical-Safety-Review-of-the-My-Health-Record-System.pdf>.

[39] *My Health Records Act 2012* (Cth) defines "shared health summary of a registered healthcare recipient, at a particular time" as the most recent such record "prepared by the healthcare recipient's nominated healthcare provider" and "uploaded to the National Repositories Service": *My Health Records Act 2012* (Cth) s 10.

[40] PwC, n 38.

[41] *My Health Records Act 2012* (Cth) Sch 1 Pt 1 title.

[42] The myhealthrecord.gov.au site does not refer to an "opt-out" option, though it does enable accessing someone else's record using a Personal Access Code (PAC): <https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/before_you_register_anotherperson>.

[43] *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth) s 8.

[44] Parliamentary Joint Committee on Human Rights, *Chair's Tabling Statement to the Twenty-ninth Report of the 44th Parliament* (13 October 2015) 2. The Committee further observed (at 2) that "to be capable of justifying a proposed limitation of human rights, a legitimate objective must address a pressing or substantial concern and not simply seek an outcome regarded as desirable or convenient": <http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports/2015>.

[45] Following "trial" of the "opt-out model", the Minister may apply the model to all healthcare recipients: *My Health Records Act 2012* (Cth) Sch 1 cll 1-2. See also Explanatory Memorandum, *Health Legislation Amendment (eHealth) Bill 2015* (Cth) 2.

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

[47] *My Health Records Act 2012* (Cth) ss 5, 44.

[48] *My Health Records Act 2012* (Cth) s 5.

[49] *My Health Records Act 2012* (Cth) ss 4-5, 38, 48-49.

Health Record system";[50] and "registered contracted service providers", who provide information technology or health information management services relating to the My Health Record system to registered healthcare providers.[51]

The key "participant", however, is the System Operator. The *My Health Records Act 2012* (Cth) provides that the System Operator 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.[52] The current System Operator is the Australian Digital Health Agency,[53] which has outsourced several of its major functions, including maintenance of the system and its security controls, to a private company, Accenture Australia Holdings Pty Ltd. That company has been "contracted by the System Operator [to act] as the eHealth record system's National Infrastructure Operator".[54] In turn, Accenture in its role as the National Infrastructure Operator relies on a subcontractor (DCS) to provide data centre services for the system.[55] Presumably, DCS is also a private entity.[56]

Section 13(A)(1) of the *My Health Records Act 2012* (Cth) empowers the System Operator 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 under this Act".[57] These purposes include the operation of a National Repositories Service for storing up to 22 million key eHealth records[58] that form part of a "registered healthcare recipient's My Health Record (including the healthcare recipient's shared health summary)",[59] and establishing and maintaining:

- an index mechanism that "allows information in different repositories to be connected to registered healthcare recipients; and … facilitates the retrieval of such information when required, and ensures that registered healthcare recipients, and participants in the My Health Record system who are authorised to collect, use and disclose information, are able to do so readily";[60]
- the system of registration and the Register of healthcare recipients and participants in the My Health Record system,[61] as well as "an audit service that records activity in respect of information in relation to the My Health Record system";[62]

[50] *My Health Records Act 2012* (Cth) ss 5, 48-49.

[51] *My Health Records Act 2012* (Cth) ss 5, 48-49; *My Health Records Rule 2016* (Cth) rr 34(1)-(2).

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

[53] *My Health Records Regulation 2012* (Cth) reg 2.1.1.

[54] Personally Controlled Health Record Operator, *Annual Report 2012-2013* (2013) [2.1]. See also Australian Government Aus Tender, *Contract Notice View – CN3370507* <https://www.tenders.gov.au/?event=public.CN.view&CNUUID=E47BDD27-0AE6-0069-4131AFAF9D8C438E>.

[55] Office of Australian Privacy Commissioner, *National Repositories Service: Implementation of Recommendations – My Health Record System Operator* (September 2016) [2.3] <https://www.oaic.gov.au/resources/privacy-law/assessments/national-repositories-service-implementation-of-recommendations-my-health-record-system-operator.pdf>.

[56] At the time of writing, the authors were unable to identify the subcontractor.

[57] *My Health Records Act 2012* (Cth) s 13(A)(1).

[58] *My Health Records Act 2012* (Cth) s 15(i); Office of Australian Information Commissioner, *National Repositories Service eHealth Record System Operator – Audit Report* (November 2014) Appendix B, [b1.3] <https://www.oaic.gov.au/resources/privacy-law/assessments/nrs-ehealth-audit-report.pdf>.

[59] The *My Health Records Act 2012* (Cth) mandates that the System Operator ensure that My Health Records of healthcare recipients containing health information that have been uploaded to the National Repositories Service are retained for "30 years after the death of the healthcare recipient; or … if the System Operator does not know the date of death of the healthcare recipient – 130 years after the date of birth of the healthcare recipient": *My Health Records Act 2012* (Cth) s 17.

[60] *My Health Records Act 2012* (Cth) s 15(a).

[61] See also *My Health Records Act 2012* (Cth) s 56.

[62] *My Health Records Act 2012* (Cth) s 15(g).

- access control mechanisms enabling registered healthcare recipients to set and specify controls on the healthcare provider organisations and nominated representatives who may obtain access to their My Health Record documents and data (the System Operator is also vested with power to "specify default access controls that apply if a registered healthcare recipient has not set such controls");[63]
- mechanisms that enable registered healthcare recipients, on application to the System Operator, to obtain electronic access to a summary and complete record of the flows of information in relation to their My Health Record.[64]

How Comprehensive is Patients' Control over Their Electronic Health Records?

On the My Health Record website, subjects of the Queensland and Nepean Blue Mountains trials were informed that from 15 July 2016 "your authorised doctor and other healthcare providers connected to the system will be able to see your My Health Record, unless you have set access controls".[65] Omitted from this advice is any reference to the access available to healthcare recipients' My Health Records by participants.

If the electronic health records system was genuinely devised primarily for patients' benefit, we might reasonably expect that healthcare recipients would have principal control over their My Health Records – as the name of the My Health Record system implies – in the sense that they were able to determine which information was contained in those records and who could access and use them. In fact, however, healthcare recipients' control over these matters is potentially quite limited.

Consistent with the government's rhetoric about the nature and purpose of the My Health Record system, registered healthcare recipients – individuals who have received, receive or may receive healthcare and whose records are contained in the system – have authority to collect, use and disclose, for any purpose, health information in their My Health Record.[66] Healthcare recipients can remove records from their My Health Records (by rendering them inaccessible to healthcare recipients, their nominated representatives and any registered healthcare provider organisations involved in their care).[67] Conversely, healthcare recipients can authorise the System Operator to restore records that have previously been removed.[68] Healthcare recipients are also able to advise healthcare providers not to upload health information about them to the My Health Record system, and healthcare providers must comply with those instructions.[69] In addition, healthcare recipients can elect not to make available to the System Operator health information about them that is held by the Chief Executive Medicare.[70]

Outside and irrespective of these personal controls, collection, use and disclosure of information in healthcare recipients' My Health Records can occur without their knowledge or consent. As noted above, healthcare recipients are permitted to set "advanced access controls" that restrict the registered

[63] *My Health Records Act 2012* (Cth) s 15(b)-(c); *My Health Records Rule 2016* (Cth) rr 4, 5. Other functions of the System Operator include: establishing and maintaining "a reporting service that allows assessment of the performance of the system against performance indicators", and "a mechanism for handling complaints about the operation of the My Health Record system": *My Health Records Act 2012* (Cth) s 15(d), (j). The System Operator also must "ensure that the My Health Record system is administered so that problems relating to the administration of the system can be resolved", "advise the Minister on matters relating to the My Health Record system", "educate healthcare recipients, participants in the My Health Record system and members of the public about the My Health Record system", and perform "such other functions as are conferred on the System Operator by this Act or any other Act": *My Health Records Act 2012* (Cth) s 15(k)-(m), (n).

[64] *My Health Records Act 2012* (Cth) s 15(h).

[65] Australian Digital Health Agency, n 2.

[66] *My Health Records Act 2012* (Cth) ss 5, 67.

[67] *My Health Records Rule 2016* (Cth) rr 4 (definition of "effectively remove"), 5(e)(i), 6(1).

[68] *My Health Records Rule 2016* (Cth) rr 5(e)(ii), 6(1).

[69] *My Health Records Act 2012* (Cth) ss 4, 45(d), Sch 1 cl 9(1).

[70] *My Health Records Act 2012* (Cth) Sch 1 cl 13.

healthcare provider organisations and healthcare recipients' nominated representatives who can access their My Health Records.[71] Yet, while the Act specifies that collection, use and disclosure of health information in the My Health Record system should be in accordance with access controls that healthcare recipients have set,[72] it also provides exceptions, where healthcare recipients' access controls can be ignored. A subdivision of this statute is headed, "collection, use and disclosure other than in accordance with access controls", and lists situations in which access controls may be disregarded, such as where "the collection, use or disclosure is undertaken in response to a request by the System Operator for the purpose of performing a function or exercising a power of the System Operator".[73] And although healthcare recipients can set an "advanced access control" in order to be "alerted by means of an electronic communication when their My Health Record is accessed by a third party",[74] they may be unaware of their ability to establish this control.

Moreover, healthcare recipients are unlikely to know that many individuals and entities are permitted under the *My Health Records Act 2012* (Cth) to have access to information in their My Health Records. Schedule 1 to this Act details information about healthcare recipients, their authorised and nominated representatives and healthcare providers, which the participants, the service operator, Chief Executive Medicare, Veterans' Affairs Department, Defence Department, and any prescribed entity (the Attorney-General's Department has already been prescribed as such an entity) can collect, use and disclose under the opt-out model, regardless of whether the individuals or entities know about or consent to them doing so.[75]

Healthcare recipients and their authorised and nominated representatives will probably not know about the sharing of their "identifying information" that the legislation permits to be undertaken between: the service operator and the System Operator; the Chief Executive Medicare and the System Operator; the Chief Executive Medicare and any participant in the system; the Veterans' Affairs Department and Defence Department and the System Operator; the Veterans' Affairs Department and Defence Department and the service operator; and between the Attorney-General's Department and the System Operator.[76] "Identifying information" is defined very broadly in the *My Health Records Act 2012* (Cth) to encompass data that many individuals would wish to protect, and could include healthcare recipients' Medicare and Veterans' Affairs Department file numbers, addresses,[77] telephone numbers and details of their driver's licences if they have been used to verify information about their identities.[78]

The *My Health Records Act 2012* (Cth) authorises further sharing of information about individuals in the My Health Record system without those individuals' knowledge or consent by enabling the participants to access and store it in the way the participants choose to do so and give third parties access to it. If a participant originally obtained a healthcare recipient's personal health information by means of the My Health Record system, but then "stored it in such a way that it could be obtained other than by means of the My Health Record system", and another "person subsequently obtained the health information by those other means",[79] ensuing distribution of that data is not subject to restrictions on use or disclosure of the information that the Act otherwise imposes. In short, once under the management of the participants, the original information in a healthcare recipient's My

[71] *My Health Records Rule 2016* (Cth) r 4 (definition of "advanced access controls").

[72] *My Health Records Act 2012* (Cth) s 61(1)(b)(i).

[73] *My Health Records Act 2012* (Cth) s 63(b). See also *My Health Records Act 2012* (Cth) ss 63-65, 68.

[74] *My Health Records Rule 2012* (Cth) r 6(1)(d).

[75] *My Health Records Act 2012* (Cth) Sch 1 cl 8(1); *My Health Records Regulation 2012* (Cth) reg 4.1.2. See also Explanatory Memorandum, *Health Legislation Amendment (eHealth) Bill 2015* (Cth) 92: the Explanatory Memorandum notes that, under Sch 1, the System Operator can obtain healthcare recipients' "identifying information without application or consent".

[76] *My Health Records Act 2012* (Cth) Sch 1 cl 8(1); *My Health Records Regulation 2012* (Cth) reg 4.1.2.

[77] *My Health Records Act 2012* (Cth) s 9(3)(a)-(b), (d).

[78] *My Health Records Regulation 2012* (Cth) reg 1.1.7(a), (e).

[79] *My Health Records Act 2012* (Cth) s 71(4).

Health Record is considered not to be obtained by accessing or using the My Health Record system. The legislation provides an example to illustrate how such material could fall into the hands of third parties: a healthcare provider downloads information in a healthcare recipient's My Health Record into its clinical health records and the information is "later obtained from those records".[80]

Cui Bono (For Whose Benefit)?

The stated objects of the *My Health Records Act 2012* (Cth) (as in force on 5 March 2016) include enabling:

> the establishment and operation of a voluntary national system for the provision of access to health information relating to recipients of healthcare, to:
>
> (a) help overcome the fragmentation of health information; and
>
> (b) improve the availability and quality of health information; and
>
> (c) reduce the occurrence of adverse medical events and the duplication of treatment; and
>
> (d) improve the coordination and quality of healthcare provided to healthcare recipients by different healthcare providers.[81]

However, as noted above, at some time in 2017, the system, which already for the majority of registered individuals does not adhere to the original goal of "consumers agreeing to make their personal health information … available to nominated providers for specified purposes", is statutorily enabled to cease being voluntary. Moreover, none of the therapeutically-oriented statutory objects are likely to be met by the My Health Record system.[82]

Likewise, the purpose of creating records documenting patients' healthcare interactions that the Taskforce articulated, namely to enable healthcare providers to make better-informed decisions at the point of care, has not been fulfilled. For, even when healthcare recipients are made aware of access to, use or disclosure of their My Health Records, the information contained in them is not necessarily able to be used for their therapeutic benefit. The System Operator is required to establish and maintain "access history", which is a record of all activity related to an individual's My Health Record; there is an automatic viewable audit trail "every time a My Health Record is accessed, changed or removed from the record".[83] However, the audit record is only visible to the healthcare recipient whose My Health Record has been accessed or modified. Significantly, healthcare recipients can remove a clinical document from their records,[84] and once the document is removed:

> If they did not author the document … [healthcare provider organisations] will be *unable to see that the document has been removed or view the clinical document, even in the case of a medical emergency*.[85]

Consequently, the Australian Digital Health Agency, which has "responsibility for clinical safety, clinical functional assurance and clinical usability for all Agency products, services and solutions, including the My Health Record system for release to the Australian community",[86] advises healthcare providers that in relation to clinical information contained in a patient's My Health Record:

---

[80] *My Health Records Act 2012* (Cth) s 71(4) "note".

[81] *My Health Records Act 2012* (Cth) s 3.

[82] $485.1 million over four years has been allocated for the My Health Record system: Explanatory Memorandum, *Health Legislation Amendment (eHealth) Bill 2015* (Cth) 3.

[83] See definition of "access history" in Australian Digital Health Agency, *Glossary* (last updated 3 April 2016) <https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/glossary>.

[84] *My Health Records Rule 2016* (Cth) rr 5(e), 6(1). See also definition of "remove a document from view" in Australian Digital Health Agency, n 83.

[85] See definition of "remove a document from view" (emphasis added) in Australian Digital Health Agency, n 83.

[86] See "Who oversees the clinical safety assurance of the My Health Record system?" in Australian Digital Health Agency, *Frequently Asked Questions for Healthcare Providers* (last updated 29 March 2016) <https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/healthcare-providers-faqs>.

> It is safest to assume the information … is not a complete record of a patient's clinical history, so information should be verified from other sources and ideally, with the patient.[87]

In other words, the information stored on the My Health Record system should not be used in an emergency or any other circumstances where patients are incapable of providing their clinical history. The very agency responsible for the clinical usability of the system – the Australian Digital Health Agency – is advising signed up or linked treating clinicians and healthcare providers not to rely on it. In addition, the "fragmentation of health information" has not been "overcome": the My Health Record system does not encompass most private hospitals and specialists in private practice.[88]

If this electronic health records legislation is not intended principally to benefit patients, what then are its purposes?

One of the answers seems to lie in a provision of the *My Health Records Act 2012* (Cth) that requires the System Operator to "prepare and provide de-identified data for research or public health purposes".[89] Despite its name, the My Health Record system is designed not entirely for delivery of care to individual patients. Its other major purpose is to fulfil the vision articulated by Deloitte Touche Tohmatsu, whereby clinical records are used by the government and third parties "to support translational research and population health surveillance".

By employing algorithms, the System Operator is required to manage and de-identify datasets comprising millions of My Health Records with information about millions of named healthcare recipients, and with new data being uploaded every 38 seconds.[90] Electronic health information about each and every healthcare recipient is currently being gathered at an enormous speed. According to the Australian Digital Health Agency, as at 20 November 2016, there were 4,367,628 individual registrations (approximately 18% of Australia's total population).[91] Additionally, "a further 1 million people have had a My Health Record automatically created for them during the participation trials".[92] Among the 18% of Australia's population[93] who are registered as "consumers … for a My Health Record", 35% of them were under the age of 20 (minors and possibly young adults under guardianship).[94] On 23 November 2016, the Australian Digital Health Agency published statistics that "over 6,238,079 prescription and dispense records have been uploaded",[95] and there were "over 1.1 million clinical upload documents", including 140,314 event summaries and 30,851 specialist letters in identifiable form.[96] All of these records were uploaded by "over 9,480 healthcare providers

[87] See "How can I be sure that the information in the My Health Record system is up to date?" in Australian Digital Health Agency, n 86.

[88] Mendelson and Rees, n 16.

[89] *My Health Records Act 2012* (Cth) s 15(ma). The phrase "public health purposes" is not defined in this statute.

[90] Australian Digital Health Agency, *My Health Record Statistics – at 20 November 2016* (last updated 23 November 2016) <https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/news-002>.

[91] Australian Digital Health Agency, n 90.

[92] Australian Digital Health Agency, n 90. The "participation trials" are authorised by the *My Health Records Act 2012* (Cth) Sch 1 cl 1.

[93] Australian Digital Health Agency, n 90.

[94] Australian Digital Health Agency, n 90.

[95] Australian Digital Health Agency, n 90. A "Dispense Document" contains "information about the medications a consumer has been dispensed by a pharmacist" and "medication specific information recorded in [it] may include: Medication brand name and strength dispensed; generic medication name; dosage instructions; the number of repeats already dispensed and the number of remaining repeats; the date the medication was last dispensed". See Australian Digital Health Agency, n 83.

[96] Other uploads of clinical documents in identifiable form as of 20 November 2016 included: 428,376 shared health summaries; 631,601 discharge summaries; 29 eReferral notes; 29,279 diagnostic imaging reports; Medicare Documents including 836,107 documents from the Australian Childhood Immunisation Register, 391,943 from the Australian Organ Donor Register, 233,308,335 Medicare/DVA Benefits Reports, and 158,493,259 Pharmaceutical Benefits Reports. There were 32,257 Consumer Entered Notes. See Australian Digital Health Agency, n 90.

… connected [to the system]".[97] Though outside the scope of this study, uploading of medical specialist letters by registered healthcare providers without the knowledge and consent of the former raises profound ethical questions surrounding the medical duty of confidentiality.[98]

The My Health Record dataset fits the widely-adopted definition of Big Data as characterised by four "V"s: "Volume (ie the size of the dataset); Variety (ie data from multiple repositories, domains, or types); Velocity (ie rate of flow); and Variability (ie the change in other characteristics)".[99] Further, as noted above, as long as they operate under the System Operator's control, computer programs can be used "for any purposes for which the System Operator may make decisions under this Act".[100] The term "computer programs" encompasses software programs for data-mining and business analytics. In this context, "data is characterized as recorded facts … [and] information is the set of patterns, or expectations, that underlie the data".[101]

The initial developments of "cybernation"[102] that led to the Big Data phenomenon and business analytics were, and to a high degree still are, directed towards commerce, markets and administration. Such artificial intelligence tools as machine learning algorithms[103] use computational power for detecting and matching otherwise unrecognisable patterns,[104] identifying correlations in observable phenomena to produce automated results in the form of interpretations and predictions relating to these phenomena.[105] The extension of these automatic or semi-automatic processes that use machine learning algorithms to analyse electronic health records has meant that we, as patients-cum-healthcare recipients, have become mere numbers attached to constantly expanding valuable data about us. This information about each of us is capable of being converted into patterns and predictions,[106] classified

[97] The numbers are somewhat fuzzy. However, the healthcare provider organisations that are reported as being registered include: 5,878 general practitioners; 715 public hospital organisations, with each of their "facilities" counted separately; 113 private hospital organisations with each of their "facilities" counted separately; 1,265 retail pharmacies; 165 aged care residential services; 1,157 "other categories of health care providers including allied health"; and 187 organisations with a cancelled registration. See Australian Digital Health Agency, n 90.

[98] The practice may infringe s 51(xxiiiA) of the Commonwealth Constitution, which prohibits authorisation of "any form of civil conscription" in respect of medical and dental services. See, eg *British Medical Association v Commonwealth* (1949) 79 CLR 201; *General Practitioners Society v Commonwealth* (1980) 145 CLR 532; *Health Insurance Commission v Peverill* (1994) 179 CLR 226; *Alexandra Private Geriatric Hospital Pty Ltd v Commonwealth* (1987) 162 CLR 271; *Oreb v Professional Services Review Committee No 298* [2004] FCA 1408; *Wong v Commonwealth* (2009) 236 CLR 573; [2009] HCA 3; *Williams v Commonwealth* (2012) 248 CLR 156; [2012] HCA 23.

[99] National Institute on Standards and Technology, *NIST Big Data Interoperability Framework: Volume 1, Definitions* (2015) 4 <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-1.pdf>.

[100] *My Health Records Act 2012* (Cth) s 13A(1).

[101] IH Witten, E Frank and MA Hall, *Data Mining: Practical Machine Learning Tools and Techniques* (Morgan Kaufmann, 3rd ed, 2011) [1.6].

[102] A Etzioni, "A Cyber Age Privacy Doctrine: A Liberal Communitarian Approach" (2014) 10 *Journal of Law and Policy for the Information Society* 641, 641: "cybernation refers to information that is digitized, stored, processed, and formatted for mass distribution. Cybernated data can be employed in two distinct ways, and both represent a serious and growing threat to privacy. A discrete piece of personal information, collected at one point in time ('spot' information) may be used for some purpose other than that for which it was originally deemed constitutional, or spot information may be pieced together with other data to generate new information about the person's most inner and intimate life."

[103] Machine learning algorithms tend to be statistical in nature. They merge "ideas from neuroscience and biology, statistics, mathematics, and physics, to make computers learn" about data classifications, patterns and predictions: S Marsland, *Machine Learning* (CRC Press, 2nd ed, 2015) 4.

[104] ML Rich, "Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment" (2016) 164 *Tulane Law Review* 871.

[105] H Surden, "Artificial Intelligence and the Law" (2014) 89 *Washington Law Review* 87, 90.

[106] For example, "Automated Suspicion Algorithms convert data about an individual and her behavior into predictions of the likelihood that she is engaged in criminal conduct": Rich, n 104, 876.

in a way that discriminates on the grounds of health, economic status, genetics, ethnicity or age, even if such information "has been explicitly excluded from the data".[107] The data-mining experts have warned that:

> The potential use of data mining techniques means that the ways in which a repository of data can be used may stretch far beyond what was conceived when the data was originally collected.[108]

Electronic health record-based data algorithmic analyses of vast cohorts may reveal statistical associations that enable identification of adverse drug interactions.[109] It has the potential to help doctors diagnose uncommon illnesses and provide prognoses and insights into health-affecting conduct in various segments of the population. However, the "mere knowledge that something is happening, rather than why it is happening"[110] derived from data analytics concerns correlations, not causation in the sense of etiology. Moreover, realisation of data-mining's diagnostic and predictive potential will depend on the accuracy of uncovered patterns and the capacity of the algorithms to nuance the correlations. These two capabilities of machine learning algorithms are still being developed; likewise, operational and semantic (uniformity of meanings of health-related terms and expressions) interoperability of electronic health records and preservation of the authenticity of electronic healthcare records[111] are yet to be achieved.[112] The lack of semantic interoperability means that it is impossible to determine whether the relevant health information is accurate or complete. In the meantime, both the "raw" data (information contained in My Health Records) as well as data manipulated by the algorithms[113] into models and predictions can be examined by researchers, and accessed and shared with government agencies for surveillance and policy purposes that may, or may not, be benign.

In its *Privacy Impact Assessment Report* on the My Health Record system, Minter Ellison noted that the volume and richness of the information contained in the system under the opt-out model will make it an extremely valuable dataset especially for researchers and employers, but also for insurers, courts, and law enforcement agencies.[114] Circumstances in which the *My Health Records Act 2012* (Cth) authorises participants to collect, use and disclose information in the My Health Record system, including where they can disregard access controls set by healthcare recipients, reveal some of these additional purposes for which the My Health Record system appears to have been established, and individuals and entities, other than healthcare recipients, who stand to benefit from it.

Those circumstances – which are unconnected with providing health care to healthcare recipients and/or are not for their benefit – include where: the collection, use or disclosure is "for purposes relating to the provision of indemnity cover for a healthcare provider"[115] (so a healthcare provider could access a healthcare recipient's My Health Record in circumstances where it needs to conduct a

[107] Witten, Frank and Hall, n 101, [1.6]. See also JS Hiller, "Healthy Predictions? Questions for Data Analytics in Health Care" (2016) 53 *American Business Law Journal* 251.

[108] Witten, Frank and Hall, n 101, [1.6].

[109] NP Tatonetti, G Haskin Fernald and RB Altman, "A Novel Signal Detection Algorithm for Identifying Hidden Drug-Drug Interactions in Adverse Event Reports" (2012) 19(1) *Journal of the American Medical Informatics Association* 79; S Hoffman and A Podgurski, "The Use and Misuse of Biomedical Data: Is Bigger Really Better?" (2013) 39 *American Journal of Law and Medicine* 497, 500.

[110] K Lim, "Big Data and Strategic Intelligence" (2016) 31 *Intelligence and National Security* 619, 633-634; JT Graves, A Acquisti and N Christin "Big Data and Bad Data: On the Sensitivity of Security Policy to Imperfect Information" (2016) 83 *University of Chicago Law Review* 117.

[111] D Lekkas and D Gritzalis "Long-term Verifiability of the Electronic Healthcare Records' Authenticity" (2007) 76 *International Journal of Medical Informatics* 442.

[112] Hoffman and Podgurski, n 109.

[113] M Leta Ambrose, "Lessons from the Avalanche of Numbers: Big Data in Historical Perspective" (2015) 11 *Journal of Law and Policy for the Information Society* 201, 211.

[114] Minter Ellison, *Privacy Impact Assessment Report: Personally Controlled Electronic Health Record (PCEHR) System Opt-Out Model* (Department of Health, 2015) 74, 77.

[115] *My Health Records Act 2012* (Cth) s 68(1).

medical assessment on behalf of an insurance company);[116] "a participant reasonably believes that the collection, use or disclosure … is necessary to lessen or prevent a serious threat to public health or safety";[117] "the collection, use or disclosure is required or authorised by Commonwealth, State or Territory law";[118] and/or "the participant reasonably believes that the collection, use or disclosure 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" (the legislation does not specify who determines whether obtaining a healthcare recipient's consent is unreasonable or impracticable, or how such a decision is made).[119]

In addition, the *My Health Records Act 2012* (Cth) permits the System Operator to disclose health information in a healthcare recipient's My Health Record to a court or tribunal where it orders or directs it to do so in proceedings relating to this Act, unauthorised access to information through the My Health Record system or "the provision of indemnity cover to a healthcare provider",[120] and to a coroner who orders or directs it to do so.[121] Further, the System Operator can use and disclose this information if: it "reasonably believes" that it is "reasonably necessary" for various "things done by, or on behalf of, an enforcement body", including "the prevention, detection, investigation, prosecution or punishment of criminal offences … or breaches of a prescribed law", "the enforcement of laws relating to the confiscation of the proceeds of crime", or "the protection of the public revenue";[122] or it "has reason to suspect that unlawful activity that relates to" its functions "has been, is being or may be engaged in", and it "reasonably believes that use or disclosure of the information is necessary" to investigate the matter or report concerns.[123]

CONCLUSION

The My Health Record system and the legislation that establishes and supports it have fundamentally changed understandings of the functions of clinical records. No longer created and used simply to provide health care to patients, health practitioners' records of their treatment of patients have become property for use by government and commercial entities for a variety of purposes well beyond serving patients' therapeutic needs. Patients' lack of control over their electronic records and derivation of minimal, if any, benefit from the My Health Record system will ultimately engender distrust in the system. To have any hope of restoring the community's faith in electronic health records, the Australian Government will need to ensure that the My Health Record system genuinely serves patients' interests, be completely transparent about all of the objectives of the system, and obtain patients' agreement to the collection, use and disclosure of their health information for purposes that may not benefit them personally. In other words, the government operating the My Health Record system needs to be mindful of Immanuel Kant's second categorical imperative to "act in such a way that you treat humanity, whether in your own person or in the person of any other, never merely as a means to an end, but always at the same time as an end".[124]

[116] Minter Ellison, n 114, 56.

[117] *My Health Records Act 2012* (Cth) s 64(2).

[118] *My Health Records Act 2012* (Cth) s 65(1).

[119] *My Health Records Act 2012* (Cth) s 64(1)(a).

[120] *My Health Records Act 2012* (Cth) s 69(1).

[121] *My Health Records Act 2012* (Cth) s 69(2).

[122] *My Health Records Act 2012* (Cth) s 70(1)(a)-(c).

[123] *My Health Records Act 2012* (Cth) s 70(3).

[124] I Kant, *Grounding for the Metaphysics of Morals* (1785) (JW Ellington trans, Hackett, 3rd ed, 1993) 36 [4:429].

"Health Privacy and Confidentiality"

Danuta Mendelson and Gabrielle Wolf

Chapter 23

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

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. However, we have begun to witness very serious 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

[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.

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, 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 is 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,

[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.

purported legal safeguards of the confidentiality of patients' health information appear to be illusory.

Medical records, which over the centuries had changed from papyrus to paper, have been now largely 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, aggregation, search and transfer of large volumes of data in real time, while advanced algorithms[18] facilitate the exploitation of large data sets by: automatically linking information in different formats from diverse sources; extracting data from various entities; indexing and data fusion; applying predictive and text analytics; unsupervised machine learning; and advanced visualization techniques.

---

[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/

Although this "unprecedented computational power and sophistication make possible unexpected discoveries, innovations, and advancements in our quality of life",[19] they can also create "an asymmetry of power between those who hold the data and those who intentionally or inadvertently supply it".[20] Complex techniques, statistics, and machine learning can process health data to create models[21] 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".[22] 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)",[23] 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".[24] 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".[25]

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-

---

[19] 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

[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] 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

[22] Scott R. Peppet, Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent, 93 *Texas Law Review* 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

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

[24] 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/

[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/

compliant[26] approach".[27] Crossix Solutions LLC currently has the patent on "A Privacy Preserving Data-Mining Protocol" in Australia.[28]

It is arguable that legislation passed by the Commonwealth Parliament to develop a national electronic health records system, and technology used to operate it, reinforces an "asymmetry of power" in Australia between "those who hold" health information and the patients and healthcare practitioners "who intentionally or inadvertently supply 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),[29] which we contend 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.[30] Under this scheme, all "healthcare recipients" – individuals who have received, receive or may receive health care[31] – will be automatically registered in the My Health Record system and issued electronic "My Health Records" to which health information about them is uploaded.[32] The My Health Record system enables the accumulation of a vast volume of such data, including: clinical notes of participating general practitioners and allied healthcare professionals (as of15 January 2017, over 1.4 million clinical documents were uploaded);[33] information from hospitals, pharmacies (as of 15 January 2017, over 7,266,077 prescriptions and dispense documents were uploaded onto the My Health Record),[34] and aged care residential services; Medicare documents (as of 15 January 2017, 420,449,558 Medicare documents were uploaded);[35] 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.[36]

---

[26] "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.
[27] http://crossix.com/platform.aspx
[28] 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.
[29] Explanatory Memorandum, Health Legislation Amendment (eHealth) Bill 2015 (Cth) 2.
[30] *My Health Records Act 2012* (Cth) s 4.
[31] *My Health Records Act 2012* (Cth) s 5 (definition of 'healthcare recipient'). According to the My Health Record website, "over 4.4 million people have a My Health Record, with an average of 1 new record being created every 38 seconds. A further 1 million people have had a My Health Record automatically created for them during the participation trial". By far the highest "percentage of consumers registered for a My Health Record", namely 37%, are "20 or less" (mainly babies born or children treated in public hospitals). https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/news-002
[32] *My Health Records Act 2012* (Cth) s 4.
[33] https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/news-002
[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] Dashboard display of My Health Record statistics https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/news-002

Significantly, Commonwealth legislation allows innumerable individuals and entities to access this extensive information in healthcare recipients' My Health Records without the data-subjects' knowledge and consent to do so. This access is provided for purposes beyond the provision of healthcare to patients,[37] 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.[38] 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".[39]

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.[40]

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:[41]

- 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

[37] 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.
[38] 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.
[39] 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.
[40] 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.
[41] *My Health Records Act 2012* (Cth) s 5 (definition of "participant in the My Health Record system").

regulations,[42] and operates the National Repositories Service in which "key records that form part" of My Health Records are stored;[43]

- "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,[44] 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;[45]
- "registered portal operators", whom the System Operator registers to operate "an electronic interface that facilitates access to the My Health Record system";[46] 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.[47]

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".[48]

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;[49]
- 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";[50] 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.[51]

Importantly, with the exception of a registered healthcare recipient's "nominated representative",[52] 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

[42] *My Health Records Act 2012* (Cth) s 14.
[43] *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.
[44] *My Health Records Act 2012* (Cth) ss 5, 44.
[45] *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.
[46] *My Health Records Act 2012* (Cth) ss 5, 48-9.
[47] *My Health Records Act 2012* (Cth) ss 5, 48-9; *My Health Records Rule 2012* (Cth) rr 34(1)-(2).
[48] *My Health Records Act 2012* (Cth) ss 98(1), (3); Explanatory Memorandum, Health Legislation Amendment (eHealth) Bill 2015 (Cth) 88.
[49] *My Health Records Act 2012* (Cth) s 99(a).
[50] *My Health Records Act 2012* (Cth) ss 99(b), (d).
[51] *My Health Records Act 2012* (Cth) s 99(c).
[52] *My Health Records Act 2012* (Cth) s 62.

recipient's My Health Record when the disclosure is for one of the purposes permitted by this Act.[53] Consequently, the information could potentially be disclosed to anyone.

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.[54] 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".[55] 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";[56] "if the collection, use or disclosure is required or authorised by Commonwealth, State or Territory law";[57] and "for purposes relating to the provision of indemnity cover for a healthcare provider".[58]

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;

[53] See *My Health Records Act 2012* (Cth) ss 61, 63-5, 68-70, sch 1, pt 2, div 2, cls 7-8.
[54] *My Health Records Act 2012* (Cth) s 63.
[55] *My Health Records Act 2012* (Cth) s 64(1).
[56] *My Health Records Act 2012* (Cth) s 64(2).
[57] *My Health Records Act 2012* (Cth) s 65.
[58] *My Health Records Act 2012* (Cth) s 68. See also: *My Health Records Act 2012* (Cth) ss 69(1), (2), 70(1), (3).

(e) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal".[59]

Although the System Operator "must make a written note of the use or disclosure",[60] 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",[61] 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.[62] If they do not do so, however, default access controls that are established and maintained by the System Operator apply.[63] 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".[64] 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".[65]

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;[66] the Defence Department;[67] any "prescribed entity" (the Attorney-General's Department is one such entity);[68] 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.[69]

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

[59] *My Health Records Act 2012* (Cth) s 70(1).
[60] *My Health Records Act 2012* (Cth) s 70(4).
[61] *My Health Records Act 2012* (Cth) s 70(5).
[62] *My Health Records Rule 2012* (Cth) rr 4 (definition of "advanced access controls"), 6; *My Health Records Act 2012* (Cth) s 15(b)(i).
[63] *My Health Records Act 2012* (Cth) ss 4, 15(b)(ii).
[64] 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.
[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, 55.
[66] *My Health Records Act 2012* (Cth) sch 1, pt 2, div 2, cl 8.
[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; *My Health Records Regulation 2012* (Cth) reg 4.1.2.
[69] *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".

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 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,[70] 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.[71] However, 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.[72]

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",[73] 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".[74]

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".[75] Yet, even if contracted service providers are vetted, they in turn could employ sophisticated information technology personnel to assist them in providing information

[70] *My Health Records Rule 2012* (Cth) rr 42(1), (4), 47(1), (4).
[71] *My Health Records Rule 2012* (Cth) r 27(1).
[72] Consumers eHealth Alliance, Submission No 12 to Department of Health Legislation Discussion Paper: "Electronic Health Records and Health Identifiers", 19 July 2015, 6.
[73] 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.
[74] 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.
[75] Commonwealth, *Parliamentary Debates*, House of Representatives, 17 September 2015, 10528-30 (Sussan Ley).

technology services to healthcare providers, who have the knowledge and capacity to distribute information from My Health Records surreptitiously and maliciously.

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;[76] yet 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".[77] If any one of those systems is degraded, it could affect the entire My Health Record system and lead to widespread misdistribution 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".[78] 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.[79] 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.[80]

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.[81] Although the statute stipulates that this information must not include personal information about a healthcare recipient, or identifying information about an individual or entity,[82] 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

[76] 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.
[77] Explanatory Memorandum, Health Legislation Amendment (eHealth) Bill 2015 (Cth) 70.
[78] *My Health Records Act 2012* (Cth) s 13A.
[79] *My Health Records Act 2012* (Cth) ss 15(n), (o).
[80] *My Health Records Act 2012* (Cth) ss 15 (h), (i), (ia).
[81] *My Health Records Act 2012* (Cth) s 77(2).
[82] *My Health Records Act 2012* (Cth) s 77(2).

information in a healthcare recipient's My Health Record or circumstances that may compromise the security or integrity of the system.[83] Nevertheless, by the time a report is made and the System Operator suspends the offending individual or entity's access to the system,[84] or cancels or suspends the offending participant's registration,[85] 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".[86] 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";[87] 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".[88]

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[89] as "an important protection for consumers who have their health information contained within their health records".[90] 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".[91] It is also foreseeable that in the global world of the internet, overseas organisations would hack the "honey pot" of medical personal information created by the My Health Record system for nefarious purposes. However the Act does not address this problem.

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[92] – applies to the My

[83] *My Health Records Act 2012* (Cth) s 75.
[84] *My Health Records Rule 2012* (Cth) rr 17(1)-(2).
[85] *My Health Records Act 2012* (Cth) s 51(3).
[86] Consumers eHealth Alliance, Submission No 12 to Department of Health Legislation Discussion Paper: Electronic Health Records and Health Identifiers, 19 July 2015, 5.
[87] Explanatory Memorandum, Health Legislation Amendment (eHealth) Bill 2015 (Cth) 85.
[88] Explanatory Memorandum, Health Legislation Amendment (eHealth) Bill 2015 (Cth) 86.
[89] *My Health Records Act 2012* (Cth) ss 59-60.
[90] Commonwealth, *Parliamentary Debates*, House of Representatives, 17 September 2015, 10529 (Hon Sussan Ley, Minister for Health and Minister for Sport).
[91] 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.
[92] *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*

Health Record system,[93] does not ensure the protection of patients' right to maintain the confidentiality of their health information. The My Health Record system, with its exceptions 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",[94] 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)]".[95] 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".[96] 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".[97] "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".[98]

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)]".[99] 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' medical 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

---

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.

[93] *My Health Records Act 2012* (Cth) ss 4, 72-3.

[94] *My Health Records Act 2012* (Cth) s 73.

[95] *My Health Records Act 2012* (Cth) s 72.

[96] *Privacy Act 1988* (Cth) ss 2A (a), (d).

[97] *Privacy Act 1988* (Cth) s 6.

[98] *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).

[99] Explanatory Memorandum, Health Legislation Amendment (eHealth) Bill 2015 (Cth) 83.

organisations, embracing new products and services which rely on personal information for delivery".[100]

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%).[101] 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 medical confidentiality of their information is that such a concept was not at the forefront of the right to privacy as it was originally conceived.[102] In their 1890 seminal article on "*The Right to Privacy"*,[103] Samuel Warren and Louis Brandeis defined privacy simply as a "right to be left alone".[104] 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[105] 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);[106]

(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);[107]

(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

[100] 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
[101] 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
[102] Friedman LM in *Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety, and Privacy*, (2007) Stanford University Press, argues that 'privacy law' was an aspect on a number of legal doctrines, such as defamation, slander and libel designed to protect reputation.
[103] Samuel D. Warren & Louis D. Brandeis, "The Right to Privacy" (1890) 4 *Harvard Law Review* 193.
[104] Samuel D. Warren & Louis D. Brandeis, "The Right to Privacy"' (1890) 4 *Harvard Law Review* 193 at 193, 95. According to Ken Gormley, "One Hundred Years of Privacy" (1992) *Wisconsin Law Review* 1335 at 1335, this phrase was used by Judge Thomas M. Cooley in *Cooley on Torts* 29 (2d ed. 1888).
[105] Ken Gormley, "One Hundred Years of Privacy" (1992) *Wisconsin Law Review* 1335 at 1337-1338.
[106] Roscoe Pound, *Interests in Personality*, 28 *Harvard Law Review* 343 (1915) and Paul A. Freund, Address to the American Law Institute (May 23, 1975), quoted in 52 *American Law Institute Proceedings*. 574-75 (1975).
[107] Louis Henkin, "*Privacy and Autonomy"*, 74 *Columbia Law Review* 1410, 1425 (1974);

> have the right to decide "when, how, and to what extent information about them is communicated to others" (Alan Westin; Charles Fried);[108]

(4) privacy as comprising two components: "secrecy, anonymity and solitude,"[109] and "repose, sanctuary and intimate decision".[110]

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".[111]

Mills considered that control "of personal information is the least developed sphere of privacy and the sphere with the least legal protection".[112]

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[113] and apply to several, but not all government agencies,[114] 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").[115] 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".[116] 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

---

[108] Alan F. Westin, *Privacy and Freedom* 7-13 (1967) Atheneum, at 7; Charles Fried, "Privacy", (1968) 77 *Yale Law Journal* 475, 477-78.
[109] Ruth Gavison, "Privacy", (1980) 89 *Yale Law Journal* 421, 433.
[110] Gary L. Bostwick, Comment, "A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision", 64 (1976) *Cal. L. Rev.* 1447.
[111] Jon L Mills, *Privacy: The Lost Right* (2008) Oxford University Press, 13-14.
[112] Jon L Mills, *Privacy: The Lost Right* (2008) Oxford University Press, 16.
[113] *Privacy Act 1988* (Cth) s 15.
[114] 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.
[115] *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
[116] 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".

> 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".[117]

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) 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".[118] 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.[119]

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[120] 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

---

[117] *Privacy Act 1988* (Cth) sch 1.4 http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/sch1.html

[118] *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.

[119] Danuta Mendelson and Gabrielle Wolf "My [Electronic] Health Record" – Cui Bono (for whose Benefit)?" (2016) 24 *Journal of Law and Medicine* 283, 293-6.

[120] 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

using a pseudonym, when dealing with an APP entity in relation to a particular matter".[121] 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".[122] In the wake of "big data" and advanced algorithms, it takes relatively little time and skill to identify correctly individuals[123] and health-related information from anonymized data sets.[124] 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[125] that the Department of Health uploaded onto its open data portal in August 2016.[126]

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",[127] 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.

[121] *Privacy Act 1988* (Cth) sch 1, Australian Privacy Principle 2.1.
[122] Ira S. Rubinstein and Woodrow Hartzog, "Anonymization and Risk" (2016) 91 *Washington Law Review* 703 at 704.
[123] 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
[124] 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/.
[125] 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
[126] 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
[127] 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.