(2016) 24 Journal of Law and Medicine

"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 informa-tion"; 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 consid-ering 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].