THE MY HEALTH RECORD SYSTEM: POTENTIAL TO UNDERMINE THE PARADIGM OF PATIENT CONFIDENTIALITY?

GABRIELLE WOLF* AND DANUTA MENDELSON**

Australia's national electronic health records system – known as the 'My Health Record ('MHR') system' – may threaten to undermine the traditional paradigm of patient confidentiality within the therapeutic relationship. Historically, patients have felt comfortable imparting sensitive information to their health practitioners on the understanding that such disclosures are necessary and will be relied on principally for the purpose of treating them. The MHR system potentially facilitates access to patients' health information by individuals and entities beyond the practitioners who are directly providing them with healthcare and, in some circumstances, without the patients' consent. It may also enable patients' health practitioners and their employees to read records that those practitioners did not create or receive in the course of treating the patients and that are irrelevant to their treatment of them. The MHR system could have harmful consequences for individual and public health if patients become unwilling to disclose information to their healthcare providers because they fear it will not remain confidential. In addition to examining the risks of breaches of patient confidentiality in the MHR system, this article considers how the potential benefits of an electronic health records system might be achieved while maintaining patient confidentiality to a significant extent.

I INTRODUCTION

At least since Classical Greece, doctors have had an ethical duty to keep health information about their patients confidential.[1] This obligation has ensured

* Associate Professor, Deakin Law School, Deakin University, Australia.
** Professor, Deakin Law School, Deakin University, Australia.
The authors wish to thank the three anonymous reviewers whose observations and recommendations greatly improved the content of the article.

1 *Kadian v Richards* [2004] NSWSC 382, [97]; Daniel Y Dodek and Arthur Dodek, 'From Hippocrates to Facsimile: Protecting Patient Confidentiality Is More Difficult and More Important than Ever Before' (1997) 156 *Canadian Medical Association Journal* 847, 847; J O'Brien and C Chantler, 'Confidentiality and the Duties of Care' (2003) 29 *Journal of Medical Ethics* 36, 36; Danuta Mendelson, 'The Medical

that patients feel comfortable about disclosing personal details to their healthcare providers, and that those practitioners can provide optimal healthcare to their patients based on full knowledge of their conditions.[2] Australia's national electronic health records system – known as the 'My Health Record ('MHR') system' – potentially facilitates access to patients' sensitive information by individuals and entities beyond the practitioners who are directly providing them with healthcare and, in some circumstances, without the patients' consent and/or knowledge. This scheme may also enable patients' health practitioners and their employees to read records that those practitioners did not create or receive in the course of treating the patients, and that are irrelevant to their treatment of them. While these risks exist outside the MHR system, they are exacerbated in the scheme. The MHR system facilitates the aggregation and connection of confidential patient information. There are many potential access points into the system and insufficient means of minimising the risk of breaches of patient confidentiality that the system poses. Further, disclosure of patients' health information in the MHR system is authorised in certain situations beyond those that patients authorise or may contemplate. The erosion of the traditional paradigm of patient confidentiality within the therapeutic relationship that this scheme may engender could have harmful consequences for individual and public health.

The MHR system commenced in 2012 as the 'Personally Controlled Electronic Health Records ('PCEHR') system', and was renamed in 2015.[3] It is a national electronic scheme for 'the collection, use and disclosure' and 'holding' of Australians' health information, which encompasses details that may not be found in a typical clinical record.[4] A MHR is created for each individual who 'has received, receives, or may receive, healthcare' – described in the *My Health Records Act 2012* (Cth) as a 'healthcare recipient' ('HR')[5] – and who is registered in the MHR system.[6] A patient's MHR comprises records uploaded to and stored in various electronic repositories.[7]

Initially, people had to apply to be registered in the PCEHR system,[8] but the *My Health Records Act 2012* (Cth) contains enabling provisions for the Minister for Health to 'provide that the opt-out model is to apply', so that 'a [HR] … will be registered in the [MHR] system, and have a [MHR], unless the [HR] elects to opt-out of the system'.[9] On 30 November 2017, the Minister made the *My Health*

Duty of Confidentiality in the Hippocratic Tradition and Jewish Medical Ethics' (1998) 5 *Journal of Law and Medicine* 227, 227–9.

2 Dodek and Dodek, above n 1, 848–9.

3 On 27 November 2015, the *Personally Controlled Electronic Health Records Act 2012* (Cth) was enacted as the renamed *My Health Records Act 2012* (Cth): see *Health Legislation Amendment (eHealth) Act 2015* (Cth) sch 2 cl 15. For a discussion of the significance of this name change, see Danuta Mendelson and Gabrielle Wolf, '"My [Electronic] Health Record" – Cui Bono (For Whose Benefit)?' (2016) 24 *Journal of Law and Medicine* 283, 285.

4 *My Health Records Act 2012* (Cth) s 5 (definition of 'My Health Record system').

5 *My Health Records Act 2012* (Cth) s 5 (definition of 'healthcare recipient').

6 *My Health Records Act 2012* (Cth) s 4.

7 *My Health Records Act 2012* (Cth) s 4.

8 *Personally Controlled Electronic Health Records Act 2012* (Cth) s 39.

9 *My Health Records Act 2012* (Cth) s 4.

Records (National Application) Rules 2017 (Cth), which apply the opt-out model to all HRs.[10] The decision to shift to an opt-out model was based on an 'evaluation' of 'trials' of this model conducted in 2016 that apparently 'showed a high level of support by healthcare providers and individuals for the automatic creation of [MHRs], and found that individuals felt the benefits far outweighed the risks to privacy, confidentiality and security'.[11] The 'period in which people [could] choose to opt-out' before a MHR would be created for them ran from 16 July 2018 until 31 January 2019 (the original end date for opting out was extended on two occasions), but collection of information about patients' identities, including their contact details, already began before this period commenced.[12]

For those who do not opt-out, their MHRs could comprise varied, comprehensive and, in some instances, extremely sensitive details about them, which are derived from many sources. Such information might range from a doctor's or nurse's summary of the patient's medical conditions,[13] to the patient's Medicare claims history, diagnostic imaging reports, and letters to and from medical specialists.[14] Yet the MHR system lacks sufficient measures for ensuring that only patients' health practitioners have access to such information, and solely to the specific details that are required to treat the patients, at the time that they are providing healthcare to them and with the patients' consent.

The second part of this article outlines ethical, professional and legal bases for patient confidentiality, which underscore why maintaining it is so important. Part III of the article explains how the architecture of the MHR system increases the risk of loss of patient confidentiality. Part IV of the article evaluates the current statutory and technical mechanisms for reducing the risk of eroding patient confidentiality in the MHR system. The legislation establishing the MHR system is extremely complex: it includes two statutes and multiple legislative rules and regulations.[15] It is therefore necessary in Parts III and IV of the article to provide a detailed exposition and close analysis of that legislation. Part V of

10 *My Health Records (National Application) Rules 2017* (Cth) r 5.

11 Explanatory Statement, My Health Records (National Application) Rules 2017 (Cth) 1. See also Mendelson and Wolf, 'My [Electronic] Health Record', above n 3, 283–4, 287–8: prior to these trials, very few patients had opted into the scheme.

12 *My Health Records (National Application) Rules 2017* (Cth) rr 2, 5, 6; Explanatory Statement, My Health Records (National Application) Rules 2017 (Cth) attachment cls 2, 5; *My Health Records Act 2012* (Cth) ss 5, 9(3) (definition of 'identifying information'), sch 1 cl 8(1) item 1; *My Health Records Regulation 2012* (Cth) reg 1.1.7; Department of Health, *My Health Record: National Opt-Out* (15 November 2018) <http://www.health.gov.au/internet/main/publishing.nsf/Content/my-health-record-national-opt-out>; *My Health Records (National Application) Rules 2017* (Cth) rr 2, 6(3)(b); *My Health Records (National Application) Amendment (Extension of Opt-Out Period No 2) Rules 2018* (Cth) sch 1 cl 1, substituting *My Health Records (National Application) Rules 2017* (Cth) r 6(3)(b).

13 *My Health Records Act 2012* (Cth) s 10; Australian Digital Health Agency, *Shared Health Summaries* <https://www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/shared-health-summaries>.

14 Australian Digital Health Agency, *What's in a My Health Record* <https://www.myhealthrecord.gov.au/for-you-your-family/whats-in-my-health-record>.

15 See, eg, *My Health Records Act 2012* (Cth); *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth); *My Health Records Rule 2016* (Cth); *My Health Records Regulation 2012* (Cth); *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* (Cth); *My Health Records (National Application) Rules 2017* (Cth).

the article contemplates how it might be possible to achieve the potential benefits of an electronic health records system while maintaining patient confidentiality to a significant extent.

II ETHICAL, PROFESSIONAL AND LEGAL BASES OF PATIENT CONFIDENTIALITY

For millennia, medical practitioners have adopted the ethical duty to keep health information about their patients confidential.[16] In Classical Greece, physicians who adhered to Hippocratic ethics took the *Hippocratic Oath*, which enjoined: 'What I may 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.'[17]

The modern rendition of this injunction by the World Medical Association in its *Declaration of Geneva* (amended in 2017) states, 'I will respect the secrets that are confided in me, even after the patient has died'.[18] Graduating medical students in Australian universities make declarations based on these statements.[19]

Australian doctors have professional codes of practice that urge or require them to comply with this ethical duty of confidentiality. For instance, the Australian Medical Association's ('AMA') *Code of Ethics* instructs doctors to 'maintain the confidentiality of the patient's personal information including their medical records, disclosing their information to others only with the patient's express up-to-date consent or as required or authorised by law'.[20] Similarly, in *Good Medical Practice: A Code of Conduct for Doctors in Australia*, the Medical Board of Australia, which regulates the Australian medical profession, explains that 'good medical practice involves: treating information about patients as confidential' and 'using consent processes … for the release and exchange of health information'.[21] A doctor's 'serious or repeated failure to meet these standards' may be a ground for disciplinary action against him/her.[22]

Privacy legislation also upholds patient confidentiality. For instance, health service providers who work in the private sector are bound by the 'Australian

16 Dodek and Dodek, above n 1, 848.

17 Ludwig Edelstein, *Ancient Medicine* (Johns Hopkins Press, 1987) 6.

18 World Medical Association, *Declaration of Geneva* (1948, amended 2017) <https://www.wma.net/policies-post/wma-declaration-of-geneva/>.

19 Paul M McNeill and S Bruce Dowton, 'Declarations Made by Graduating Medical Students in Australia and New Zealand' (2002) 176 *Medical Journal of Australia* 123; Edmund D Pellegrino, 'Medical Commencement Oaths: Shards of a Fractured Myth, or Seeds of Hope against a Dispiriting Future?' (2002) 176 *Medical Journal of Australia* 99.

20 See, eg, Australian Medical Association, *AMA Code of Ethics* (at 2004, revised 2016) art 2.2.2 <https://ama.com.au/system/tdf/documents/AMA%20Code%20of%20Ethics%202004.%20Editorially%20Revised%202006.%20Revised%202016.pdf?file=1&type=node&id=46014>.

21 Medical Board of Australia, *Good Medical Practice: A Code of Conduct for Doctors in Australia* (at March 2014) arts 3.4.1, 3.4.3 <http://www.medicalboard.gov.au/Codes-Guidelines-Policies/Code-of-conduct.aspx>; see also arts 3.2.3, 3.4.

22 Ibid art 1.2; *Health Practitioner Regulation National Law Act 2009*, as enacted in each State and Territory, ss 5 (definitions of 'unprofessional conduct' and 'professional misconduct'), 178, 193.

Privacy Principles' ('APPs'), which are set out in the *Privacy Act 1988* (Cth) and regulate their use and disclosure of 'personal information', which includes health information.[23] APP6 prohibits health service providers from disclosing information that they have collected for the primary purpose of treating their patients for some secondary purpose unless certain circumstances exist (such as that the patients expressly or implicitly consent to the disclosure, or the patients would 'reasonably expect' this disclosure, and the primary and secondary purposes are 'directly related' to one another).[24] Depending on the Australian jurisdiction in which health service providers practise, they may also need to comply with state and territory privacy legislation, including statutes that govern health records, which applies to public and/or private sector health services.[25] In addition, article 17 of the *International Covenant on Civil and Political Rights*, which Australia has ratified (though not formally incorporated into its domestic law), provides that 'no one shall be subjected to arbitrary or unlawful interference with his privacy'.[26]

Finally, at common law, doctors have an 'obligation of confidence' that arises from their relationships with their patients.[27] A patient whose doctor breaches that duty may have an action in tort, contract or equity.[28]

The rationale behind all these bases of patient confidentiality is that it upholds mutual trust between doctors and patients, and such trust is essential for meaningful communication between them and medical treatment.[29] Patients are prepared to divulge intimate, embarrassing and distressing problems to their doctors only on the understanding that such disclosures are necessary and will be relied on for the purposes of diagnosis, treatment and, if applicable, billing and insurance claims, and that their information will usually not be revealed to third parties without their consent.[30] Doctors, in turn, are aware that without patients' candour regarding their symptoms, making diagnoses and providing treatment may be difficult, inappropriate and costly. There is also an awareness that

23 *Privacy Act 1988* (Cth) sch 1, ss 6 (definitions of 'personal information', 'sensitive information', 'APP entity' and 'organisation'), 6C(1)(a), 6FA, 15; Office of the Australian Information Commissioner, *Fact Sheet: Privacy and Your Health Information* (2014) <https://www.oaic.gov.au/engage-with-us/consultations/health-privacy-guidance/fact-sheet-privacy-and-your-health-information>.

24 *Privacy Act 1988* (Cth) sch 1 cls 6.1, 6.2, s 16B. A person who believes that a doctor has breached this APP could make a complaint to the Information Commissioner, who can make a determination if he/she finds the complaint substantiated, including 'a declaration that the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint': ss 36(1), 52(1)(b)(iii).

25 For a description of Australian state and territory privacy legislation, see Danuta Mendelson, Anne Rees and Gabrielle Wolf, 'Medical Confidentiality and Patient Privacy' in Ben White, Fiona McDonald and Lindy Willmott (eds), *Health Law in Australia* (Thomson Reuters, 3rd ed, 2018) 395, 409–14.

26 *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17.

27 *Medical Board of Australia v Kemp* [2018] VSCA 168, [99] (Niall JA), citing *Hunter v Mann* [1974] QB 767, 772 (Boreham J).

28 For a discussion of these actions, see Mendelson, Rees and Wolf, above n 25, 403–7.

29 Kenneth D Mandl, Peter Szolovits and Isaac S Kohane, 'Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private' (2001) 322 *British Medical Journal* 283, 284; Julius Bourke and Simon Wessely, 'Confidentiality' (2008) 336 *British Medical Journal* 888, 888.

30 O'Brien and Chantler, above n 1, 37.

inappropriate disclosure of patients' health information could cause them financial and/or psychological harm.[31]

Patients' lack of assurance that the confidentiality of their health information will be maintained could have a harmful impact on individual and public health.[32] It may lead to patients' loss of trust in their healthcare providers and therefore make them reluctant to seek medical help and disclose their medical information unless their pain and/or discomfort becomes unbearable.[33] At this point, however, it could be too late for them to be treated successfully. If they fear disclosure of their sensitive health details, patients may also provide incomplete information to health practitioners and/or self-medicate.[34] In the case of some conditions and patient populations, patients already tend to refrain from seeking healthcare, perhaps due to embarrassment.[35] For instance, a 2018 report into 'HIV, Viral Hepatitis and Sexually Transmissible Infections in Australia' stated that, '[i]n 2017, there were an estimated 255 227 (159 672 in men, 95 556 in women) new chlamydia infections [a sexually-transmitted disease that, untreated, harms women's reproductive systems and can cause epididymitis in men] in people aged 15–29 years' in Australia, but 'the vast majority of infections in young people (15–29 years) remain undiagnosed and untreated'.[36] This statistic could rise if patients believe that the confidentiality of their health information will be substantially compromised in the MHR system.

III POTENTIAL BREACHES OF PATIENT CONFIDENTIALITY IN THE MY HEALTH RECORD SYSTEM

Outside the MHR system, patients can assume that the confidentiality of their health information is maintained to some extent by virtue of its fragmentation and storage in multiple, disparate locations, such as different medical practices, pathology laboratories and hospitals, in electronic and paper records.[37] Nevertheless, privacy breaches can occur and an individual with access to one of those repositories could potentially view the patients' information that they hold,

31 Randolph C Barrows and Paul D Clayton, 'Privacy, Confidentiality, and Electronic Medical Records' (1996) 3 *Journal of the American Medical Informatics Association* 139, 139.

32 Ofir Ben-Assuli, 'Electronic Health Records, Adoption, Quality of Care, Legal and Privacy Issues and Their Implementation in Emergency Departments' (2015) 119 *Health Policy* 287, 291.

33 Ibid 291; Barrows and Clayton, above n 31, 142; David Mechanic and Sharon Meyer, 'Concepts of Trust among Patients with Serious Illness' (2000) 51 *Social Science and Medicine* 657, 664; Mandl, Szolovits and Kohane, above n 29, 284; Alix Rolfe et al, 'Interventions for Improving Patients' Trust in Doctors and Groups of Doctors' (2014) 3 *Cochrane Database of Systemic Reviews* 4–5.

34 Ben-Assuli, above n 32, 291.

35 See, eg, J Carlisle et al, 'Concerns over Confidentiality May Deter Adolescents from Consulting Their Doctors: A Qualitative Exploration' (2006) 32 *Journal of Medical Ethics* 133, 133.

36 Skye McGregor et al, 'HIV, Viral Hepatitis and Sexually Transmissible Infections in Australia: Annual Surveillance Report' (Kirby Institute, 2018) 10, 13 <https://kirby.unsw.edu.au/sites/default/files/kirby/report/KI_Annual-Surveillance-Report-2018.pdf>.

37 Roy Schoenberg and Charles Safran, 'Internet Based Repository of Medical Records that Retains Patient Confidentiality' (2000) 321 *British Medical Journal* 1199, 1199; Mandl, Szolovits and Kohane, above n 29, 283.

but the repositories are unconnected with one another. Further, the content of each one is generally limited to information about patients that it or its health practitioners created or received in the course of treating them. By contrast, in the MHR system, a broad range of sensitive information about individuals from many different health practitioners and government sources can be duplicated, summarised, linked and uploaded into patients' MHRs, in certain instances without them explicitly agreeing to this occurring.[38] Moreover, a multitude of individuals and entities can potentially access this voluminous data.

In the MHR system, individuals' health information is still 'held in repositories across multiple locations'.[39] Yet at least one of those repositories – the National Repositories Service ('NRS') – can comprise aggregated and summarised information about patients.[40] Further, the repositories are required to 'maintain interoperability' with the MHR system,[41] so that patients' information held in all of the repositories is accessible online through the system and can be 'obtained' from them.[42] The Australian Digital Health Agency ('ADHA'), which since July 2016 has been the 'System Operator' that operates the MHR system,[43] explains that:

> A My Health Record is not a single document stored in a single database. Rather it is made up of a collection of documents stored in a secure network of connected registered repositories. We collect information held in registered repositories and display an index of available information about you in your My Health Record. If … a healthcare provider wishes to access a document held in a registered repository … we will call for the document from the registered repository and make it available to the healthcare provider.[44]

An individual MHR can include several documents that are copies or precises of information concerning the patient that is maintained by his/her health practitioners and typically would be viewed only by the patient's treating healthcare providers. A MHR may incorporate:

- a 'shared health summary', prepared by the patient's nominated doctor or nurse that notes his/her medical history, medication, allergies and adverse reactions to medication;

---

38 HealthConsult, 'Development of a Framework for Secondary Use of My Health Record Data' (Public Consultation Paper, Department of Health, 1 September 2017) 1 <https://www.health.gov.au/internet/main/publishing.nsf/Content/964591B00A3C9D72CA2582C70083A1CA/$File/Public%20Consultations%20Paper.pdf>: with respect to data produced by 'healthcare providers', 'the original information is retained within the system of the healthcare provider that delivered the service', but 'the [MHR] system contains either a copy or a summary of health information held by healthcare provider organisations'.

39 *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* (Cth) guideline 4.4.

40 Office of the Australian Information Commissioner, 'National Repositories Service: Implementation of Recommendations – My Health Record System Operator' (Assessment Report, September 2016) <https://www.oaic.gov.au/privacy-law/assessments/national-repositories-service-implementation-of-recommendations-my-health-record-system-operator>.

41 *My Health Records Rule 2016* (Cth) rr 31, 39, 56.

42 *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* (Cth) guideline 4.4; Office of the Australian Information Commissioner, above n 40, 5 [2.5].

43 *My Health Records Act 2012* (Cth) ss 4, 14; *My Health Records Regulation 2012* (Cth) reg 2.1.1.

44 Australian Digital Health Agency, *Privacy Policy* <https://www.myhealthrecord.gov.au/about/privacy-policy>.

- an 'event summary', which includes information about healthcare provided to the patient on a particular occasion that is relevant to his/her future care;
- a record of prescriptions that have been issued for the patient;
- pharmacists' records of medication dispensed to the patient;
- hospital discharge summaries;
- diagnostic imaging and pathology reports;
- health practitioners' referrals of the patient to other clinicians, seeking advice or care, which could include a summary of the patient's conditions, diagnoses, treatment and test results; and
- medical specialists' reports to referring clinicians about their assessment and treatment of the patient.[45]

Information concerning patients that is held by government agencies can also be included in patients' MHRs. The Chief Executive Medicare may provide to the System Operator to include in a patient's MHR: a Pharmaceutical Benefits Report about Pharmaceutical Benefits Scheme ('PBS') subsidised medication that has been dispensed to the patient; a Medicare or Department of Veterans' Affairs ('DVA') Benefits Report about the patient's visits to healthcare providers and claims information; and records relating to the patient in the Australian Immunisation Register and Australian Organ Donor Register.[46]

Subject to patients' 'express advice' not to upload certain records, a healthcare provider organisation (any individual or body that 'has conducted, conducts, or will conduct, an enterprise that provides healthcare') that is registered by the System Operator is 'authorised to upload to the [MHR] system any record that includes health information about a registered [HR]'.[47] Likewise, the Chief Executive Medicare can upload information about patients into the MHR system, unless the patients notify the System Operator that they do not want this information included in their MHRs.[48]

Patients may, however, be unaware of which information is in fact being uploaded to their MHRs and therefore unable to make an informed decision about whether they want to object to this occurring. A healthcare provider must not 'upload to a [MHR] repository a record that includes health information about a registered [HR] if the [HR] has advised that the record is not to be uploaded'.[49] Nevertheless, ADHA confirms that: 'there is no requirement for a

45 HealthConsult, above n 38, 5; Australian Digital Health Agency, *View a My Health Record* <https://www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/view-my-health-record>; Australian Digital Health Agency, *What's in a My Health Record*, above n 14.

46 *My Health Records Act 2012* (Cth) sch 1 cl 12(1); Explanatory Statement, My Health Records (National Application) Rules 2017 (Cth) attachment cl 7; HealthConsult, above n 38, 6; Australian Digital Health Agency, *What's in a My Health Record*, above n 14.

47 *My Health Records Act 2012* (Cth) s 5 (definitions of 'entity' and 'healthcare provider organisation'), sch 1 cl 9(1).

48 *My Health Records Act 2012* (Cth) sch 1 cls 12, 13(1); Australian Digital Health Agency, *Privacy Policy*, above n 44.

49 *My Health Records Act 2012* (Cth) s 45(d). See also Australian Digital Health Agency, *Understand when You Can View and Upload Information* <https://www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/understand-when-you-can-view-and-upload-information>.

healthcare provider to obtain consent on each occasion prior to uploading clinical information. There is also no requirement for a healthcare consumer to review clinical information prior to it being uploaded'.[50]

This system does not enable patients to provide valid, informed consent, as this phrase is generally understood, to healthcare providers to upload their health information to their MHRs. In addition to being competent to provide consent, for patients to provide such valid, informed consent, they would need to: receive and understand information about all of the details that are proposed to be incorporated into their MHRs; comprehend the possible ramifications of uploading this information to their MHRs, including who will be able to access it and the benefits and risks of doing so; and make voluntary decisions, free from pressure, about whether particular information should be uploaded to their MHRs.[51] The AMA does tell doctors that 'good medical practice involves advising the patient you will upload information to their [MHR]' and 'if the information is potentially sensitive and you consider the patient may have reservations about it being uploaded to the [MHR system] you should discuss the uploading with the patient'.[52] Nevertheless, this advice is not binding on doctors.

A further loss of patient confidentiality can occur in the MHR system through the inclusion of one patient's health information in another patient's MHR. A registered healthcare provider organisation has authority 'to upload to the MHR system a record in relation to a [HR] (the *patient*) that includes health information about another [HR] (the *third party*), if the health information about the third party is directly relevant to the healthcare of the patient' (presumably the healthcare provider determines the relevance of the information in this regard).[53] Unless MHR regulations prescribe otherwise, healthcare provider organisations have such power 'despite a law of a State or Territory that requires consent to the disclosure of particular health information'.[54] As patients have authority to view information in their own MHRs,[55] by doing so, they could access those other individuals' health information.

The Department of Health envisages that 'the [MHR] system will evolve with consumer and healthcare provider feedback' to encompass 'more and different clinical content'.[56] As the volume and nature of patients' information that is accessible in the MHR system increases, so, too, will the number of people who are able to access it. Many people might have access to the extensive

50 Australian Digital Health Agency, *Understand when You Can View and Upload Information*, above n 49; Danuta Mendelson, 'The European Union General Data Protection Regulation (EU 2016/679) and the Australian My Health Record Scheme – A Comparative Study of Consent to Data Processing Provisions' (2018) 26 *Journal of Law and Medicine* 23, 36–8.

51 See Barrows and Clayton, above n 31, 143; Danuta Mendelson, 'Historical Evolution and Modern Implications of the Concepts of Consent to, and Refusal of, Medical Treatment in the Law of Trespass' (1996) 17 *Journal of Legal Medicine* 1; Medical Board of Australia, above n 21, art 3.5.

52 Australian Medical Association, 'AMA Guide to Using the PCEHR' (June 2012) [4.5.3.2], [4.5.3.4] <https://ama.com.au/article/ama-guide-using-pcehr>.

53 *My Health Records Act 2012* (Cth) s 41(3A), sch 1 cl 9(2).

54 *My Health Records Act 2012* (Cth) sch 1 cl 9(3).

55 *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* (Cth) guideline 4.4.

56 HealthConsult, above n 38, 6.

information about patients that can be included in their MHRs through their involvement in managing its storage in the MHR system and assisting with the system's technical operation. Outside the MHR system, individuals and organisations that store patients' health information often engage third parties to help them manage their electronic records in particular, but the information that those third parties can access is necessarily restricted to the data that the individuals and organisations possess.

The System Operator stores 'personal information' about registered HRs, 'an index of available documents about [HRs], stored in registered repositories', and Medicare information about HRs.[57] In addition, the System Operator operates the NRS,[58] which holds 'key records about [HRs]', including the shared health summary, event summaries, 'key clinical documents uploaded by [patients'] healthcare providers', and information that patients upload in the form of '[HR]-only notes'.[59] There appears to be no limit on the number of 'private and public sector bodies' and individuals whom the System Operator can register to hold 'records of information included in [MHRs] for the purposes of the [MHR] system', and the Chief Executive Medicare must apply for such registration.[60] Another repository is the 'eRx Script Exchange Repository', which holds patients' 'prescriptions information'.[61]

One of the System Operator's functions, which it will likely require technical assistance to fulfil, is 'to establish and maintain an index service … [that] allows information in different repositories to be connected to registered [HRs]'.[62] In addition, the System Operator registers 'portal operators' to operate any 'electronic interface that facilitates access to the [MHR] system'.[63] Also registered by the System Operator are 'contracted service providers', who provide 'information technology [IT] services' or 'health information management services relating to the [MHR] system' to 'healthcare provider organisations' that the System Operator has registered, pursuant to contracts with those organisations.[64] Contracted service providers are permitted to access the MHR system only 'to the extent' that the healthcare provider organisations to whom they are 'linked' (via a contract) have 'instructed' them to do so.[65]

Unless patients actively restrict access to information in their MHRs, 'healthcare provider organisations' that the System Operator has registered and that provide those patients with healthcare can access this data online, 'anywhere

57 Australian Digital Health Agency, *Privacy Policy*, above n 44.
58 *My Health Records Act 2012* (Cth) ss 4, 15(i).
59 *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* (Cth) guideline 4.4; Australian Digital Health Agency, *Privacy Policy*, above n 44; *My Health Records Act 2012* (Cth) ss 4, 5 (definition of 'healthcare recipient-only notes'). HR-only notes may include advance care planning information: HealthConsult, above n 38, 6.
60 *My Health Records Act 2012* (Cth) ss 4–5 (definition of 'registered repository operator'), 38, 48–9; *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* (Cth) guideline 4.5.
61 Australian Digital Health Agency, *Privacy Policy*, above n 44.
62 *My Health Records Act 2012* (Cth) s 15(a)(i).
63 *My Health Records Act 2012* (Cth) ss 5, 49.
64 *My Health Records Act 2012* (Cth) ss 4, 5, 44, 49; *My Health Records Rule 2016* (Cth) r 34.
65 *My Health Records Rule 2016* (Cth) r 37(1).

at any time'.[66] If authorised to do so, these organisations simply 'call up' and 'view' information in a MHR repository, regardless of where it is located.[67] For instance, 'a healthcare provider organisation can view a pathology report for a [HR] that is located at a particular pathology lab, if that pathology lab is a registered repository operator'.[68]

A healthcare provider organisation is eligible for registration by the System Operator provided that it has a 'healthcare identifier' ('HI') (and 'complies with … requirements as are specified in the My Health Record Rules' and 'has agreed to be bound by the conditions imposed by the System Operator on the registration').[69] HIs are not only assigned to doctors, but also, inter alia, to other health practitioners that a registration authority has registered as a member of a health profession, such as dentists, chiropractors and optometrists.[70] Consequently, there is a potential risk that any one of an individual's healthcare providers could access information uploaded to the system by the patient's other healthcare providers. For example, an individual's podiatrist might be able to view a discharge summary prepared by clinicians at a mental health service that this patient attended. Likewise, it might be possible for all of an individual's healthcare providers to view his/her Medicare claims history.

The MHR system thus facilitates healthcare providers' access to information that, but for this system, they would not have had an opportunity to read because it does not form part of the records that they have created or received in the course of treating their patients. In fact, this data may be irrelevant to the present needs of patients whom they are treating, and could include documents that were never intended to be shared beyond a patient's immediate treating health practitioners, such as letters that medical specialists wrote exclusively for the eyes of their referring clinicians.

Even if information in patients' MHRs seems minimal, it can be the key to substantial, highly personal details about them. In a submission to the Senate Finance and Public Administration References Committee's inquiry into 'circumstances in which Australians' personal information has been compromised and made available for sale illegally on the "dark web"' (Senate inquiry), Future Wise provided the following example: 'if a person has on record a consultation with a doctor who works in a … drug dependency clinic … then it is not only the content of the consultation that is sensitive, but the fact that the consultation has occurred at all'.[71] Further, readers of patients' MHRs may connect information in them to other data that is available on the internet and

66 HealthConsult, above n 38, 1, 5; *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* (Cth) guidelines 4.4–4.5.

67 *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* (Cth) guideline 4.5.

68 *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* (Cth) guideline 4.5.

69 *My Health Records Act 2012* (Cth) s 43.

70 *Healthcare Identifiers Act 2010* (Cth) ss 9(1)(a), 9A(1)(a).

71 Future Wise, Submission No 9 to Senate Finance and Public Administration References Committee, *Inquiry into Circumstances in Which Australians' Personal Medicare Information Has Been Compromised and Made Available for Sale Illegally on the 'Dark Web'*, August 2017, 11.

thereby discover more personal details about those individuals. Future Wise also aptly observed, 'the power of data is in its aggregation'.[72]

Healthcare provider organisations that are permitted to access patients' MHRs can in turn authorise their employees to view those MHRs if they consider that they need to do so to perform their 'duties'.[73] ADHA confirms that such personnel could be 'clinicians', but also 'other staff' whom health organisations authorise 'to access the [MHR] system as part of their role in healthcare delivery',[74] such as 'administrative staff', who require access 'for the purposes of retrieving information from the system for use by [a] healthcare provider or uploading documents to the system'.[75] Further, those employees can access and view a patient's MHR outside of a consultation, that is, 'without the individual being present, provided that access is for the purpose of providing healthcare to the individual'.[76]

Outside the MHR system, healthcare providers are similarly free to determine which of their employees can access their patients' records and the number of such personnel could be high. For instance, in hospitals, where there is a 'team approach' to patient care, patients' records may be accessible to a range of health care providers, including doctors, nurses, pharmacists, and medical and nursing students, in addition to administrative staff.[77] Yet, in contrast to patients' MHRs, those organisations' records are largely confined to details that the organisations have created and received in the course of treating their patients.

It is relatively straightforward for healthcare provider organisations' employees to view information that is stored in the MHR system. They can access the MHR system through either the 'National Provider Portal', which the System Operator operates, or 'a local clinical information system'.[78] They can use the National Provider Portal if:

- a 'responsible officer' or 'organisation maintenance officer' in the healthcare provider organisation for which they work (who acts on behalf of the organisation regarding its participation in the MHR system) links them to the organisation (via a phone call or written application form) and authorises their access to the portal;
- they are registered with the Healthcare Identifiers Service ('a national system that uses a unique number to match healthcare providers' and their records to their patients); and

72 Ibid 13.

73 *My Health Records Act 2012 (Cth)* s 99(a); *My Health Records Rule 2016* (Cth) rr 27(1), 44(a); Australian Digital Health Agency, *Understand when You Can View and Upload Information*, above n 49.

74 Australian Digital Health Agency, *Understand when You Can View and Upload Information*, above n 49.

75 Australian Digital Health Agency, Submission No 4 to Senate Finance and Public Administration References Committee, *Inquiry into Circumstances in Which Australians' Personal Medicare Information Has Been Compromised and Made Available for Sale Illegally on the 'Dark Web'*, 28 August 2017, 3.

76 Australian Digital Health Agency, *Understand when You Can View and Upload Information*, above n 49.

77 Dodek and Dodek, above n 1, 847, 849.

78 Australian Digital Health Agency, Submission No 4, above n 75, 2.

- they apply for a 'National Authentication Service for Health Public Key Infrastructure' ('NASH PKI') certificate.[79]

Alternately, they can access the MHR system by entering log on details into a clinical information system onto which their employer has installed relevant software and their NASH PKI (for which the employer must have applied).[80] After accessing the system, it is possible to view information in a patient's MHR by inputting the patient's surname, sex and date of birth, and either his/her Medicare card number and individual reference number, DVA card number, or HI that is assigned to the patient by the 'service operator' (which is currently the Department of Human Services ('DHS')).[81] ADHA advises that, if healthcare providers do not have this information, they can still 'access the system through the use of other demographic information, such as address details as they are recorded in the Medicare database'.[82]

Other people who have similar capacity to access information in a patient's MHR (in addition to the patient) are: an individual acting on the patient's behalf as an 'authorised representative' (if the patient is under 14 years of age, or is between 14 and 17 years of age and nominates an authorised representative, or is incapable of 'making decisions' for himself or herself);[83] or a 'nominated representative' for the patient, who can 'do any thing' that legislation 'authorises' the patient to do, subject to the patient's wishes.[84] Outside the MHR system, people acting on behalf of patients may similarly be able to access their health information. For instance, the *Privacy Act 1988* (Cth) permits organisations that provide health services to disclose a patient's health information for a purpose other than the purpose for which it was collected (to provide healthcare) to a 'responsible person' for the patient (such as a relative or guardian) in various circumstances.[85] Yet, as MinterEllison observed in their 2011 Privacy Impact Assessment Report on the PCEHR system, 'there is a risk that authorised representative/s of adult [patients] will, through their access to the PCEHR, gain information they normally would not be able to, such as health

79 Department of Human Services, *Healthcare Identifiers Service for Health Professionals* <https://www.humanservices.gov.au/organisations/health-professionals/services/medicare/healthcare-identifiers-service-health-professionals>; Australian Digital Health Agency, Submission No 4, above n 75, 2. See also *My Health Records Rule 2016* (Cth) r 4 (definitions of 'organisation maintenance officer' and 'responsible officer'); *Healthcare Identifiers Act 2010* (Cth) ss 5 (definitions of 'organisation maintenance officer' and 'responsible officer'), 9A(7)–(8).

80 Australian Digital Health Agency, Submission No 4, above n 75, 3.

81 Ibid 3; *Healthcare Identifiers Act 2010* (Cth) ss 9AA, 9; Department of Human Service, *Healthcare Identifiers Service for Health Professionals*, above n 79; Australian Digital Health Agency, *My Health Record Provider Portal Demonstration* <https://www.digitalhealth.gov.au/files/assets/cup-articulate/using-the-provider-portal/providerPortal/index.html>.

82 Australian Digital Health Agency, Submission No 4, above n 75, 3.

83 *My Health Records Act 2012* (Cth) s 6, as amended by *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth) sch 1 cls 1BA–1DA.

84 *My Health Records Act 2012* (Cth) ss 7(1)–(2), 62.

85 *Privacy Act 1988* (Cth) ss 6AA (definition of 'responsible person'), 16B(5), sch 1 cls 6.1, 6.2(c).

information about the [patient] unrelated to a current decision about their healthcare'.[86]

In certain situations, information in patients' MHRs can lawfully be disclosed to third parties, beyond the patients, their representatives and healthcare providers, in order to fulfil purposes other than providing healthcare to the patients, and sometimes without the patients' consent.[87] Outside the MHR system, health practitioners are required by law to breach patient confidentiality in particular circumstances, too. Nevertheless, those health professionals would not possess, and thus be incapable of disclosing, the same wealth of information about patients that can be collated in their MHRs. In addition, as noted below, there are situations in which patient information is required to be disclosed that only apply to the MHR system.

For instance, in two circumstances that are deemed to constitute cases of 'serious threat', a so-called 'participant in the [MHR] system' – namely, the System Operator, registered healthcare provider organisations, repository operators, portal operators and contracted service providers[88] – can disclose 'health information' in patients' MHRs (except for HR-only notes and records that have been removed from their MHRs).[89] The participants may disclose information in these circumstances irrespective of patients' expressed wishes to limit access to their MHRs to certain nominated representatives and healthcare provider organisations and/or to restrict access to particular records in their MHRs.[90] The first circumstance is where the participant 'reasonably believes' that it is 'necessary' to do so 'to lessen or prevent a serious threat to an individual's life, health and safety' and 'it is unreasonable or impracticable to obtain the [HR's] consent' to the disclosure.[91] The second is where the participant 'reasonably believes' that the disclosure is 'necessary to lessen or prevent a serious threat to public health or public safety'.[92] These provisions resemble sections of the *Privacy Act 1988* (Cth) and state and territory health records legislation that similarly permit organisations to disclose patients' health information in these circumstances.[93] Yet no one organisation would have all of the information about patients that can be amassed in their MHRs to disclose.

The participants in the MHR system can also disclose 'health information' in a patient's MHR 'for the purpose of the management or operation of the [MHR] system', provided that 'the [HR] would reasonably expect the participant to …

86 MinterEllison, 'Privacy Impact Assessment Report: Personally Controlled Electronic Health Record' (Report, Department of Health and Ageing, 15 November 2011) 60 [5.1.15(a)] <https://www.myhealthrecord.gov.au/sites/default/files/personally_controlled_electronic_health_record_pcehr_privacy_impact_asse.pdf?v=1520886932>.

87 *My Health Records Act 2012* (Cth) pt 4 div 2 sub-div B.

88 *My Health Records Act 2012* (Cth) s 5 (definition of 'participant in the My Health Record system').

89 *My Health Records Act 2012* (Cth) s 64(3); *My Health Records Rule 2016* (Cth) rr 7(2)(c), 8(2)(c).

90 *My Health Records Rule 2016* (Cth) r 6 note 3.

91 *My Health Records Act 2012* (Cth) s 64(1)(a); *My Health Records Rule 2016* (Cth) rr 6(2)(b)(ii), 7.

92 *My Health Records Act 2012* (Cth) s 64(2); *My Health Records Rule 2016* (Cth) rr 6(2)(b)(ii), 8.

93 See, eg, *Privacy Act 1988* (Cth) s 16A(1), sch 1 cls 6.1, 6.2(c); *Health Records and Information Privacy Act 2002* (NSW) sch 1 cl 11(1)(c).

disclose the health information for that purpose'.[94] This is a novel provision that does not apply outside the MHR system, and relevant legislation provides no guidance about how patients' expectations in this regard must be ascertained and by whom, and to whom the information can be disclosed.[95] Further, the System Operator (though not the other participants) must comply with a court or tribunal order to disclose health information in a patient's MHR in proceedings relating to either the *My Health Records Act 2012* (Cth), 'unauthorised access to information through the [MHR] system', or 'the provision of indemnity cover to a healthcare provider', even if the patient does not consent to this disclosure.[96] In addition, the System Operator must comply with a judicial officer's order to disclose health information in a patient's MHR to 'an entity that is: an agency or a State or Territory authority, within the meaning of the *Privacy Act 1988*', which could include a Minister or 'a body … established or appointed for a public purpose by or under a law of a State or Territory'.[97]

The participants in the MHR system are authorised to disclose health information in patients' MHRs 'in response to a request by the System Operator for the purpose of performing a function or exercising a power of the System Operator'.[98] Amongst the System Operator's functions, whose performance may depend on the participants disclosing patients' health information, and that could result in third parties accessing that information, is 'to prepare and provide [though not to private health insurers] de-identified data, and, with the consent of the [HR], health information, for research or public health purposes'.[99] Privacy legislation also permits organisations to disclose patients' health information for research that is relevant to public health or is otherwise in the public interest.[100] Yet, outside the MHR scheme, no individual or entity would have access to the extensive information about patients that can be accessible through their MHRs. The legislation provides for the appointment of a 'data custodian' – the Australian Institute of Health and Welfare – inter alia to de-identify data in the MHR system,[101] and it, in turn, will require access to patients' health information to do so. A greater infringement of patient confidentiality could, however, occur

94 *My Health Records Act 2012* (Cth) s 63(a).

95 Danuta Mendelson and Gabrielle Wolf, 'Health Privacy and Confidentiality' in Ian Freckelton and Kerry Peterson (eds), *Tensions and Traumas in Health Law* (Federation Press, 2017) 266, 273.

96 *My Health Records Act 2012* (Cth) ss 69(1)(b)(ii)–(iii), (3)–(4).

97 *My Health Records Act 2012* (Cth) s 69A, as inserted by *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth) sch 1 cl 12; *Privacy Act 1988* (Cth) ss 6, 6C(3).

98 *My Health Records Act 2012* (Cth) s 63(b).

99 *My Health Records Act 2012* (Cth) s 15(ma), as amended by *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth) sch 2 cl 2; *My Health Records Act 2012* (Cth) s 16, as inserted by *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth) sch 1 cl 1E.

100 See, eg, *Privacy Act 1988* (Cth) s 16B(3); *Health Records and Information Privacy Act 2002* (NSW) sch 1 cl 11(1)(f).

101 *My Health Records Act 2012* (Cth) s 109A(2), as inserted by *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth) sch 2 cl 14; *My Health Records Act 2012* (Cth) s 5 (definition of 'data custodian'), as amended by *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth) sch 2 cl 1. Schedule 2 of the *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth), which refers to the position of data custodian, is yet to commence, but it must commence by 11 December 2019: *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth) s 2(1).

through re-identification of this information (that is, matching anonymised data with the patients to whom it relates).

The Department of Health engaged HealthConsult to 'develop a Framework for the secondary use of data held in the [MHR] system' (providing healthcare is considered the primary use of this data).[102] The 'Data Governance Board' (the 'Board') will use the Framework 'when making decisions about granting access to, and making available, MHR system data for secondary use'.[103] According to the Framework, this Board is empowered to enable a large range of bodies, in a variety of contexts, to use MHR data. The Framework states that 'any Australian-based entity (except insurance agencies) can apply to access MHR system data for secondary use'.[104] HealthConsult envisaged that de-identified information from patients' MHRs could legitimately be provided to academic researchers as well as to those who use it for 'public health purposes' that also happen to serve commercial ends, such as 'for development of pharmaceuticals'.[105] The Framework provides another example where the Board could deem that commercial organisations' proposed use of MHR data is 'consistent with "research and public health purposes"': their development of new medical devices.[106] The Framework states that MHR system data could 'provide a more comprehensive picture of "real-world behaviour" … in regard to product consumption'.[107]

If de-identified data from patients' MHRs is given to researchers, and especially to commercial entities, there is a risk that this information could be matched with other datasets to re-identify the original information.[108] The Framework states that 'the Board will ensure that contemporary de-identification methods and techniques are appropriately applied before any data is made accessible to applicants'.[109] It also promises that 'the Board will ensure that the risk of a breach of privacy for an individual is reduced to an acceptable level by minimising the risks associated with each application for secondary use and

102 HealthConsult, above n 38, 1.

103 Department of Health, *Framework to Guide the Secondary Use of My Health Record System Data* (May 2018) 3 <http://www.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79BCA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf>. Note that *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth) sch 2 pt 7 div 1 establishes the 'Data Governance Board'. Schedule 2 of the *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth), which will establish the Data Governance Board, is yet to commence, but it must commence by 11 December 2019: *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth) s 2(1).

104 Department of Health, above n 103, 5.

105 HealthConsult, above n 38, 3.

106 Department of Health, above n 103, 7, 62.

107 Ibid 59.

108 MinterEllison, 'Privacy Impact Assessment Report: Personally Controlled Electronic Health Record' (Report, 20 May 2015) 79–80 <https://www.myhealthrecord.gov.au/sites/default/files/pcehr_opt_out_pia_-_2015.pdf?v=1520887003>; Chris Culnane, Benjamin Rubinstein and Vanessa Teague, 'Health Data in an Open World: A Report on Re-identifying Patients in the MBS/PBS Dataset and the Implications for Future Releases of Australian Government Data' (University of Melbourne, 18 December 2017) 3 <https://arxiv.org/ftp/arxiv/papers/1712/1712.05627.pdf>.

109 Department of Health, above n 103, 39.

recommending penalties where applicable'[110] (those penalties might be additional to existing penalties for unauthorised disclosure of health information in the MHR system, which are discussed in Part IV below).[111] Nevertheless, it is unclear who determines the level of risk that is acceptable, and patients may have different views from health practitioners or the Board about which level is acceptable.

Moreover, the relative ease with which re-identification of de-identified data can occur has been demonstrated on many occasions internationally.[112] University of Melbourne researchers, who demonstrated the possibility of 're-identifying supplier numbers' in a 'de-identified data release' of Medicare information, consider that 'sensitive unit-record level data, particularly when that data contains detailed information about each individual, cannot be securely de-identified without substantially degrading the data' (that is, by 'removing most of the information' from it).[113] Consequently, for the information in the MHR system to be useful to any external party, it would need to be de-identified to such a minimal extent that there would be a substantial likelihood of it being re-identified.

IV MECHANISMS TO MINIMISE BREACHES OF PATIENT CONFIDENTIALITY IN THE MY HEALTH RECORD SYSTEM

Outside the MHR system, health practitioners are principally accountable for ensuring that their patients' health information is not revealed to third parties inappropriately. Within the MHR system, health practitioners continue to bear this responsibility for safeguarding the confidentiality of their patients' health information, but they share it with the other participants and, particularly under the opt-out model, with patients themselves. The dispersion of this responsibility amongst so many individuals and entities makes it difficult to monitor compliance with it, and measures that have been created to do so may be inadequate to minimise the erosion of patient confidentiality sufficiently. Moreover, the default position that patients' confidentiality is compromised unless patients explicitly act to change this circumstance heightens the chance of disclosure of sensitive information, especially where patients are vulnerable. In any event, unless patients decline from participating in the MHR system altogether, their capacity to prevent access to and disclosure of their information may be limited and there are circumstances in which their wishes in this regard can be overridden.

---

110 Ibid 6, 51.

111 See *My Health Records Act 2012* (Cth) ss 59–60.

112 MinterEllison, '2015 Privacy Impact Assessment Report', above n 108, 79–80; Ira S Rubinstein and Woodrow Hartzog, 'Anonymization and Risk' (2016) 91 *Washington Law Review* 703.

113 Chris Culnane, Ben Rubinstein and Vanessa Teague, Submission No 5 to Senate Finance and Public Administration References Committee, *Inquiry into Circumstances in Which Australians' Personal Medicare Information Has Been Compromised and Made Available for Sale Illegally on the 'Dark Web'*, 2–3.

Patients will be able to maintain the confidentiality of their health information to some extent if they choose not to be involved in the MHR system. Pursuant to the opt-out model, patients who already have a HI – which is assigned to all individuals who are enrolled in Medicare or who have a DVA file number, and to others who apply for a HI – will have MHRs created for them if they have not opted out (unless they fall within certain exceptions).[114] Those patients could have elected not to be registered by the System Operator by notifying it, within six months of the commencement of the opt-out period, of this decision (the original notice period of three months was extended).[115] Patients can also, at any time, request the System Operator to cancel or suspend their registration in the system.[116]

Even if patients chose to opt-out of the MHR system, ADHA may already have gathered information about them. The Explanatory Statement to the *My Health Records (National Application) Rules 2017* (Cth) clarifies that their application of the opt-out model to all HRs 'triggers the authority for the System Operator to collect information about people who are not registered in the [MHR] system as part of preparation for the implementation of opt-out'.[117] The System Operator is empowered to collect 'identifying information' about patients.[118] This could include patients' names, telephone numbers, addresses, email addresses, dates of birth, Medicare and DVA file numbers and, 'if information relating to the identity of the [HR] has been, or is to be, verified using a particular form of identification document (such as a driver's licence or passport), details of that document'.[119] It is unclear where this information is stored and how it is managed if the patient to whom it pertains elected not to be registered.

If patients do not opt-out, they may be able to maintain the confidentiality of their health information to a certain degree. Patients can set 'advanced access controls' that restrict the nominated representatives and healthcare provider organisations who can access their MHRs, and their access to particular records within them.[120] The System Operator can establish controls that enable only a

114 *Healthcare Identifiers Act 2010* (Cth) ss 9AA, 9(1)(b); Explanatory Statement, My Health Records (National Application) Rules 2017 (Cth) attachment cls 5–6: 'the System Operator will not register any person who previously had a [MHR] and cancelled it', who was part of the opt-out trials and opted out, or who was part of the trials and did not opt-out, but has since then cancelled his/her MHR.

115 *My Health Records Act 2012* (Cth) sch 1 cl 5; *My Health Records (National Application) Rules 2017* (Cth) rr 6(1)–(3); Department of Health, *My Health Record: National Opt-Out*, above n 12. HRs who did not yet have a HI when the opt-out period commenced needed to notify the System Operator of their election to opt-out at the time that they applied to be assigned a HI or to enrol in Medicare, if they wished to opt-out: *My Health Records (National Application) Rules 2017* (Cth) rr 6(4)–(5).

116 *My Health Records Act 2012* (Cth) s 51(1); Explanatory Statement, My Health Records (National Application) Rules 2017 (Cth) attachment cl 6.

117 Explanatory Statement, My Health Records (National Application) Rules 2017 (Cth) attachment cl 5. See *My Health Records (National Application) Rules 2017* (Cth) r 5.

118 *My Health Records Act 2012* (Cth) sch 1 cl 8(1) item 1.

119 *My Health Records Act 2012* (Cth) ss 5 (definition of 'identifying information'), 9(3); *My Health Records Regulation 2012* (Cth) reg 1.1.7.

120 *My Health Records Act 2012* (Cth) ss 15(b)(i), (c); *My Health Records Rule 2016* (Cth) r 4 (definition of 'advanced access controls').

healthcare provider organisation that is involved in a patient's care to access the patient's MHR if the patient gives or requests the System Operator to give the organisation a 'record code'.[121] Similarly, these controls can prevent healthcare provider organisations from accessing records within a patient's MHR unless the patient gives or requests the System Operator to give the organisation a 'document code in relation to the record'.[122] Further, as noted above, a healthcare provider organisation must not upload to the MHR system a record that includes health information about a patient if the patient expressly advises it not to do so.[123]

There are, however, limits to patients' control over access to information in their MHRs. For instance, a patient cannot prevent a healthcare provider organisation from accessing records that it has uploaded to the patient's MHR (the organisation can access those records 'without the need to use the [HR's] document code').[124] It appears, too, that patients are unable to prevent healthcare provider organisations who are involved in their care from accessing 'shared health summaries and [HR]-entered health summaries' in their MHRs.[125] In addition, in several of the circumstances discussed in Part III of this article, information in patients' MHRs can be disclosed to third parties irrespective of those patients' advanced access controls. The *My Health Records Act 2012* (Cth) discusses the participants' authority to disclose health information in patients' MHRs 'for management of [MHR] system', 'in the case of a serious threat', if 'authorised by law', 'for indemnity cover', and 'in relation to unlawful activity', under the heading 'collection, use and disclosure other than in accordance with access controls'.[126]

In its 2011 and 2015 Privacy Impact Assessment Reports on the PCEHR system, MinterEllison highlighted how, even if patients set advanced access controls, those controls might not actually reflect their wishes regarding access to their information. MinterEllison also identified obstacles that patients could face in setting access controls. Patients 'may not understand their own settings' and therefore 'expose themselves to risks they thought they had mitigated', and/or '"set and forget" who else can see their [MHR]'.[127] They may only realise that their access controls are not set in accordance with their preferences after their information has been viewed.[128] Other patients may be unable to set access controls without substantial assistance if they do not understand how to do so, are illiterate and/or not 'computer literate', lack 'access to a computer or the

121 *My Health Records Rule 2016* (Cth) r 6(1)(a).
122 *My Health Records Rule 2016* (Cth) rr 6(1)(c), (2)(a).
123 *My Health Records Act 2012* (Cth) s 45(d), sch 1 cl 9(1).
124 *My Health Records Rule 2016* (Cth) r 6(2)(b)(i).
125 *My Health Records Rule 2016* (Cth) r 6(2)(a).
126 *My Health Records Act 2012* (Cth) pt 4 div 2 sub-div B; *My Health Records Act 2012* (Cth) s 70 (heading), substituted by *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth) cl 13.
127 MinterEllison, '2011 Privacy Impact Assessment Report', above n 86, 54.
128 Culnane, Rubinstein and Teague, above n 113, 3.

Internet', do not speak English, or 'have an impairment or disability' that affects their 'ability to access' the MHR system.[129]

In addition, some patients may not set access controls because they do not appreciate the ramifications of neglecting to do so and, specifically, who can view their information and the details they can read.[130] If a patient does not set advanced access controls, 'default access controls' that are established and maintained by the System Operator apply.[131] Those controls 'permit all registered healthcare provider organisations involved in the care of a registered [HR] to access the [HR's] [MHR]'.[132] A healthcare provider organisation is only removed from the 'access list of the registered healthcare provider organisations that are permitted to access' the patient's MHR 'if the organisation has not accessed the [HR's] [MHR] for a period of three years'.[133] Outside the MHR system, healthcare providers can continue to access their records concerning patients for whom they have provided healthcare without obtaining those patients' consent to them doing so. Yet they generally do not have access to information about their patients that they did not receive or generate in the course of treating them, which could be accessible from patients' MHRs. Importantly, the default access controls will not reflect patients' consent to waiving the confidentiality of all of the information that is potentially available in their MHRs to all of the healthcare providers who are involved in their care. To provide such consent, patients would need to indicate on each occasion that those healthcare providers seek to access specific details in their MHRs whether they have waived confidentiality in them. As Brennan J explained in *Commonwealth v Verwayen*, a 'right [such as a right to confidentiality] is waived only when the time comes for its exercise and the party for whose sole benefit it has been introduced knowingly abstains from exercising it'.[134]

Even where default access controls apply, patients still carry the onus of minimising intrusions into their confidentiality. The default access controls that the System Operator creates must 'permit registered [HRs] to effectively remove records from their [MHR]'.[135] Patients may not, however, have an opportunity to remove records before others have read them. Further, many patients may not consider during healthcare consultations whether they want to object to health practitioners uploading certain information to their MHRs if those practitioners do not inform them that they have the right to do so (which, as discussed above, they are not legally obliged to do).

In addition, if patients do not opt-out of the MHR system, but do not want the information that the Chief Executive Medicare can provide to the System Operator (outlined in Part III of this article) included in their MHRs, they must

129 MinterEllison, '2015 Privacy Impact Assessment Report', above n 108, 58; MinterEllison, '2011 Privacy Impact Assessment', above n 86, 55.

130 MinterEllison, '2015 Privacy Impact Assessment Report', above n 108, 68; Mendelson and Wolf, 'Health Privacy and Confidentiality', above n 95, 275.

131 *My Health Records Act 2012* (Cth) ss 4, 15(b)(ii).

132 *My Health Records Rule 2016* (Cth) r 5(a).

133 *My Health Records Rule 2016* (Cth) rr 5(b), (d).

134 (1990) 170 CLR 394, 427.

135 *My Health Records Rule 2016* (Cth) r 5(e).

notify the System Operator of their wishes in this respect.[136] A patient can make this election between the time that he/she is registered and the first occasion on which his/her MHR is accessed.[137] If the patient does not do so, details of patients' 'last two years of MBS' ('Medical Benefits Schedule') and 'PBS claims', 'organ and/or tissue donation decisions' and 'immunisations administered' to them,[138] 'will, by default, automatically be included in the person's [MHR] … the first time someone accesses a [MHR]', which could be the patient's health practitioner, rather than the patient.[139] The patient may subsequently decide that they do not want the Chief Executive Medicare's information included in their MHRs, but this election will only relate to 'new information', so they will need to 'choose to remove' such information that has already been included in their MHRs.[140]

Once a healthcare provider organisation is permitted, under default or advanced access controls, to access a patient's MHR or certain records within it, the patient cannot place any restrictions on which individuals within those organisations, or other organisations that are connected with them, can share this access. Outside the MHR system, a patient similarly lacks control over which individuals within these organisations and their networks can access their information, but those people are unable to view the extensive information about patients that can be accessible from their MHRs. In the MHR scheme, there is some oversight of organisations' decisions about which individuals have access to patients' MHRs, but the extent to which this will protect patient confidentiality is uncertain.

Healthcare provider organisations' maintenance officers must give the System Operator lists of 'individuals who are authorised to access the [MHR] system via or on behalf of the organisation using the provider portal'.[141] Since it does not appear that the System Operator has power to override the organisations' authorisations, the provision of this information to the System Operator does not guarantee protection of patient confidentiality.[142] Healthcare provider organisations are also required to 'ensure that their [IT] systems, which are used by people to access the [MHR] system via or on behalf of [them], employ reasonable user account management practices including: restricting access to those persons who require access as part of their duties'.[143] Yet it would be extremely difficult for the System Operator (or another authority) to ascertain the 'duties' of each individual whom every healthcare provider organisation

136 *My Health Records Act 2012* (Cth) sch 1 cls 12(2), 13(1).

137 *My Health Records (National Application) Rules 2017* (Cth) r 7(5); Explanatory Statement, My Health Records (National Application) Rules 2017 (Cth) attachment cl 7.

138 Australian Digital Health Agency, *Privacy Policy*, above n 44; Ariel Bogle, 'My Health Record: Your Questions Answered on Cybersecurity, Police and Privacy', *ABC News Science* (online), 15 July 2018 <http://www.abc.net.au/news/science/2018-07-15/my-health-record-questions-answers-security-privacy-police/9959622>.

139 Explanatory Statement, My Health Records (National Application) Rules 2017 (Cth) attachment cl 7.

140 Ibid.

141 *My Health Records Rule 2016* (Cth) r 27(1).

142 Mendelson and Wolf, 'Health Privacy and Confidentiality', above n 95, 275.

143 *My Health Records Rule 2016* (Cth) r 44(a).

permits to access a patient's MHR, and decide whether he/she actually requires this access.

If a registered healthcare provider organisation is part of a 'network' (a group of healthcare provider organisations that are part of, or superior or subordinate to, one another),[144] the 'seed organisation' (the organisation at the apex of the network, which is superior to the other organisations)[145] determines which of the network organisations can access patients' MHRs.[146] Its responsible officer and/or maintenance officer must establish and maintain 'access flags' – 'an [IT] mechanism made available by the System Operator to define access to a [HR's] [MHR]' – for the organisations in the network.[147] The access flags need to balance 'reasonable [HR] expectations about the sharing of health information as part of providing healthcare to the [HR]; and arrangements within the organisation for access to health information collected by the organisation'.[148] The System Operator can ask a seed organisation 'to make reasonable changes' to its access flags if it considers that they 'have been assigned in a manner that is inconsistent with [those] principles' and the organisation 'must not unreasonably refuse to comply' with such a request.[149] Nevertheless, relevant legislation provides no guidance about how the seed organisation or the System Operator should ascertain patients' expectations about the sharing of their information and weigh such expectations against the organisation's arrangements for access to information that it collects. Healthcare provider organisations may act on the assumption, which could be inaccurate, that patients would be content for them to make information in their MHRs accessible to all of the organisations in their network in case the patients require treatment by any one of them.

The MHR system also relies extensively on healthcare provider organisations and the other participants to prevent breaches of patient confidentiality. The system's security is thus only as robust as the participants' compliance with and competence at fulfilling their obligations. Like healthcare provider organisations, contracted service providers and repository and portal operators must develop 'user account management practices' that limit access to the MHR system through their IT systems to 'those persons who require access as part of their duties'.[150] All of these participants must monitor 'people using their [IT] systems to access the [MHR] system' to 'ensure' that they 'do not record, store or retain a copy of a [HR's] record code or document code for the purposes of accessing the [HR's] [MHR], or a record in the [HR's] [MHR], in the future'.[151] They also need to make certain that their IT systems have 'password and/or other access mechanisms that are sufficiently secure and robust given the security and privacy

144 *My Health Records Rule 2016* r 9 note; *Healthcare Identifiers Act 2010* (Cth) ss 6, 9A(4).
145 *Healthcare Identifiers Act 2010* (Cth) ss 6, 9A(5).
146 *My Health Records Rule 2016* (Cth) r 28.
147 *My Health Records Rule 2016* (Cth) rr 4 (definition of 'access flag'), 9(c).
148 *My Health Records Rule 2016* (Cth) r 10(1).
149 *My Health Records Rule 2016* (Cth) rr 10(3), (5).
150 *My Health Records Rule 2016* (Cth) rr 4 (definition of 'operator'), 49(a), 61(a).
151 *My Health Records Rule 2016* (Cth) rr 45, 50, 63(1). This rule 'does not apply to portal operators to the extent they operate a portal that provides access to the [MHR] system solely to [HRs]': r 63(2).

risks associated with unauthorised access to the [MHR] system'.[152] In addition, their responsibilities entail confirming that their IT systems '[ensure] that the user accounts of persons no longer authorised to access the [MHR] system … prevent access to the [MHR] system',[153] and '[suspend] a user account that enables access to the [MHR] system as soon as practicable after becoming aware that the account or its password or access mechanism has been compromised'.[154]

Further, those participants 'must have a written policy', which they 'communicate' and 'ensure … remains readily accessible, to all [their] employees', and 'enforce … in relation to all [their] employees' and, in the case of healthcare provider organisations, also in relation to 'any healthcare providers to whom the organisation supplies services under contract'.[155] The policy needs to detail 'training' that they will provide to 'employees before they are authorised to access the [MHR] system, including in relation to how to use the [MHR] system … responsibly, the legal obligations on … individuals using the [MHR] system and the consequences of breaching those obligations'.[156] This policy must also cover 'the physical and information security measures that are to be established and adhered to by … people accessing the [MHR] system',[157] as well as 'mitigation strategies to ensure [MHR] system-related security risks can be promptly identified, acted upon and reported'.[158]

Nevertheless, a participant's policy need not address any of these requirements if, in its 'reasonable opinion', they are 'not applicable' to it due to its 'limited size'.[159] Moreover, while it appears that the System Operator may be capable of scrutinising the other participants' adherence to their policies, it is not explicitly required to do so. The participants 'must ensure that the policy … is drafted in such a manner that the [participant's] performance can be audited against the policy to determine if [it] has complied with the policy'.[160] They also need to provide a copy of the policy to the System Operator in response to a written request to do so,[161] and one of the System Operator's functions is 'to establish and maintain an audit service that records activity in respect of information in relation to the [MHR] system'.[162]

Despite the potential authorisation of many individuals to access patients' MHRs, it is difficult to ensure that they do not read information that is accessible from them when they have no clinical reason to do so.[163] It is difficult to prevent those who have access to patients' records outside the MHR system from reading

152 *My Health Records Rule 2016* (Cth) rr 44(c), 49(c), 61(c).
153 *My Health Records Rule 2016* (Cth) rr 44(d), 49(d), 61(d).
154 *My Health Records Rule 2016* (Cth) rr 44(e), 49(e), 61(e).
155 *My Health Records Rule 2016* (Cth) rr 42(1)–(3), 47(1)–(3), 59(1)–(3).
156 *My Health Records Rule 2016* (Cth) rr 42(4)(b), 47(4)(b), 59(4)(b).
157 *My Health Records Rule 2016* (Cth) rr 42(4)(d), 47(4)(c), 59(4)(c).
158 *My Health Records Rule 2016* (Cth) rr 42(4)(e), 47(4)(d), 59(4)(d).
159 *My Health Records Rule 2016* (Cth) rr 42(5), 47(5), 59(5).
160 *My Health Records Rule 2016* (Cth) rr 42(6)(a)(i), 47(6)(a)(i), 59(6)(a)(i).
161 *My Health Records Rule 2016* (Cth) rr 43(1)–(2), 48(1)–(2), 60(1)–(2).
162 *My Health Records Act 2012* (Cth) s 15(g).
163 Sebastian Haas et al, 'Aspects of Privacy for Electronic Health Records' (2011) 80 *International Journal of Medical Informatics* e26, e27.

their contents without a proper purpose for doing this. Yet they would not have access to the extensive information that patients' MHRs could comprise, and often not to details that would be irrelevant to the conditions for which they or their employers are treating the patients. Contracted service providers must give the System Operator the HIs of linked healthcare provider organisations that have instructed them to access or disclose records from the MHR system each time they do so.[164] Yet this would not assist the System Operator in determining whether employees of contracted service providers have inappropriately viewed records in patients' MHRs. Likewise, there appears to be no technological mechanism for guaranteeing that health practitioners read only those details in patients' MHRs that are relevant to their treatment of the patients at the time that they are consulting them. ADHA states that its 'Cyber Security Centre continually monitors the [MHR] system for evidence of unauthorised access [to it]'.[165] Yet, as Future Wise advised the Senate inquiry, 'the greatest risk to the privacy of [MHR] holders' is 'improper access by authorised users'.[166] The wealth of data about patients in their MHRs may prompt more improper accessing of these records than might otherwise occur in relation to patients' health records outside the system, to the patients' detriment. Patients' MHRs may be alluring for 'reasons' including 'curiosity, perversity or financial or political gain', and it is conceivable that improper access to them may lead to 'ruined careers, public ridicule, social rejection and economic devastation for patients and their families'.[167]

Patients might be able to detect improper access to their MHRs. The System Operator must 'establish and maintain mechanisms that enable each registered [HR] to obtain electronic access to a summary of the flows of information in relation to his or her [MHR]' and, if patients apply to the System Operator for it, to 'a complete record' of those 'flows of information'.[168] According to ADHA, the system keeps a record of each occasion on which a patient's MHR is accessed, and patients can view this 'Access History' log or 'a real time log of every access to their [MHR] by a provider organisation'.[169] Patients can also receive an automatic notification when healthcare provider organisations access their MHRs for the first time, and can request the System Operator to establish advanced access controls that permit them 'to be alerted by means of an electronic communication when their [MHR] is accessed by a third party'

164 *My Health Records Rule 2016* (Cth) r 37(2).

165 Australian Digital Health Agency, Submission No 4, above n 75, 4.

166 Future Wise, above n 71, 9. See also Brian Randell, 'A Computer Scientist's Reactions to NPfIT' (2007) 22 *Journal of Information Technology* 222, 228.

167 Dodek and Dodek, above n 1, 850–1.

168 *My Health Records Act 2012* (Cth) ss 15(g)–(h).

169 Australian Digital Health Agency, Submission No 4, above n 75, 5; Australian Digital Health Agency, *See Who Has Accessed Your Record* <https://www.myhealthrecord.gov.au/for-you-your-family/howtos/see-who-has-accessed-your-record>; Australian Digital Health Agency, *Fact Check: Security of My Health Record* <https://www.digitalhealth.gov.au/news-and-events/news/fact-check-security-of-my-health-record>.

generally.[170] Nevertheless, many patients may not elect to receive these notifications or monitor access to their MHRs (which could be an onerous task, especially for vulnerable patients) unless they have reason to suspect that someone may view records in their MHRs for a purpose unrelated to providing healthcare to them. Moreover, this is yet another example of patients' responsibility for maintaining the confidentiality of their information in the MHR system, which represents an inadequate means of protecting it.

Intentional and inadvertent breaches of the MHR system's security may also compromise patient confidentiality. Although mechanisms have been developed to detect and respond to such contraventions in the MHR system, they would not prevent them from occurring. As well as the Cyber Security Centre's scrutiny of the MHR system, the participants and former participants are required to report any possible unauthorised disclosure of information in patients' MHRs, or events or circumstances that may compromise the security or integrity of the system, which could involve them.[171] If 'the System Operator considers that the security, integrity or operations of the [MHR] system have been, or may be, compromised, the System Operator may suspend access to the [MHR] system'.[172] Such a risk might arise if 'there is a security problem with the [IT] systems of a participant' or a participant 'has failed to maintain interoperability' with the MHR system.[173] Yet the System Operator's actions may be undertaken too late to preclude a significant infringement of patient confidentiality.[174] In such circumstances, patients could also complain to the Australian Information Commissioner 'about an act or practice that may be an interference with [their] privacy' under the MHR system,[175] but the Commissioner cannot reverse the patients' loss of confidentiality (the *My Health Records Act 2012* (Cth) provides that '[a] contravention of this Act is also an interference with privacy for the purposes of the *Privacy Act 1988*, and so can be investigated under that Act').[176]

The legislation prescribes severe penalties for deliberate breaches of patients' confidentiality, but they are unlikely to deter everyone. Civil and criminal sanctions can be imposed on a person for unauthorised use or disclosure of health information in a patient's MHR that he/she obtained by using or accessing the MHR system where he/she knew or was 'reckless as to the fact' that the use or disclosure was unauthorised under the *My Health Records Act 2012* (Cth).[177] Where that person discloses the information to another person and the second person discloses the information, knowing that the disclosure was unauthorised or reckless about whether it was unauthorised, the second person commits an

170 Australian Digital Health Agency, *Fact Check: Security of My Health Record*, above n 169; *My Health Records Rule 2016* (Cth) r 6(1)(d).

171 *My Health Records Act 2012* (Cth) s 75.

172 *My Health Records Rule 2016* (Cth) r 17(1).

173 *My Health Records Rule 2016* (Cth) rr 17(2)(a), (c), 31.

174 Mendelson and Wolf, 'Health Privacy and Confidentiality', above n 95, 276–7.

175 *Privacy Act 1988* (Cth) s 36(1).

176 *My Health Records Act 2012* (Cth) s 4.

177 *My Health Records Act 2012* (Cth) s 59. Penalties for unauthorised collection, use and disclosure of health information in patients' MHRs have recently been increased: see *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth) sch 1 cls 6A–E.

offence and is liable to penalties too.[178] Unless reckless, unintentional or accidental disclosure of health information in patients' MHRs does not attract a penalty, however.[179] Such a disclosure might occur, for example, if an employee neglects to close a computer screen with information from a patient's MHR visible on it and leaves the computer unattended due to an oversight or in an emergency, thereby enabling others to view it.[180]

It is probable that the penalties will be ineffective in dissuading some people who are enticed to access and disclose information in the MHRs of patients whom they know or who have a high public profile, and assume that their improper actions will not be detected.[181] Computer scientist Brian Randell notes:

> The larger the system, the more people involved, the easier it will be, for example, for an unscrupulous reporter or private investigator to find a weak link in the form of a legitimate user who can be fooled into committing, or bribed to commit, an act which will breach the system's privacy rules … though [they] can be prosecuted should they be caught, lazy or corrupt insiders have little to fear from the law.[182]

Moreover, various features of the MHR system exacerbate the risk of unauthorised access to and disclosure of patients' health information.[183] For instance, there are many legitimate access points into the MHR system, each of which potentially provides access over the internet to records held by registered repository operators.[184] ADHA asserts that 'any software that connects to the system undergoes ongoing checks to ensure that it conforms to the system requirements and has authority to access the information'.[185] Yet it would be extremely difficult for the System Operator to make certain that every access point into the MHR system is secured adequately.[186] A recent observation by the American Healthcare Industry Cybersecurity Task Force may be pertinent to the MHR system: 'if the health care system is connected, but insecure, this connectivity could betray patient safety, subjecting them to unnecessary risk and forcing them to pay unaffordable personal costs'.[187] MinterEllison forecasted that:

> The likelihood and level of security risk to PCEHR system data security will increase under an Opt-Out Model due to the large number of individuals, as well as the richness of the volume of information. In particular, the registration of almost all Australians will increase the 'honeypot' value of the PCEHR system.[188]

178 *My Health Records Act 2012* (Cth) s 60.
179 HealthConsult, above n 38, 19.
180 Barrows and Clayton, above n 31, 142; Bourke and Wessely, above n 29, 889.
181 Mendelson and Wolf, 'Health Privacy and Confidentiality', above n 95, 277.
182 Randell, above n 166, 225.
183 Mendelson and Wolf, 'Health Privacy and Confidentiality', above n 95, 275–6.
184 eHealth Privacy Australia, Submission No 8 to Senate Finance and Public Administration References Committee, *Inquiry into Circumstances in Which Australians' Personal Medicare Information Has Been Compromised and Made Available for Sale Illegally on the 'Dark Web'*, 31 August 2017, 4–6.
185 Australian Digital Health Agency, Submission No 4, above n 75, 5.
186 eHealth Privacy Australia, above n 184, 6.
187 Health Care Industry Cybersecurity Task Force, 'Report on Improving Cybersecurity in the Health Care Industry' (2 June 2017) 1 <https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf>.
188 MinterEllison, '2015 Privacy Impact Assessment Report', above n 108, 74.

MinterEllison envisaged various 'risk scenarios' under the opt-out model, including 'one person impersonating another in order to gain access to someone's PCEHR', and 'organised criminals … circumventing controls in order to access multiple individuals' records'.[189]

The reality of the risk of unauthorised disclosure of health information in patients' MHRs, and the government's inability to provide meaningful assurances about the system's security, are illuminated by events that occurred in 2017. *The Guardian Australia* exposed that Medicare data about Australians managed by DHS was being illegally sold on the darknet.[190] In its submission to the Senate inquiry, DHS emphasised that 'the Medicare card alone does not provide access to personal health information'.[191] Yet the criminal vendors of the Medicare data would have been able to view patients' health information if they had access to the MHR system and entered into it a patient's Medicare card number, together with the patient's surname, sex and date of birth.[192] Once stolen, patients' health information could be used for 'fraud, identity theft … and disruption of hospital systems and patient care'.[193]

ADHA has stated that it 'takes a proactive, privacy by design approach to managing the development and operation of the [MHR] system'.[194] Privacy by design is a 'methodology that enables privacy to be "built in" to the design and architecture of information systems, business processes and networked infrastructure' in order 'to ensure that privacy is considered before, at the start of, and throughout the development and implementation of initiatives that involve the collection and handling of personal information'.[195] Canadian Information and Privacy Commissioner Ann Cavoukian developed 'The 7 Foundational Principles' for 'privacy by design', as follows:

1. 'Proactive not Reactive; Preventative not Remedial': 'The Privacy by Design approach … anticipates and prevents privacy invasive events *before* they happen' and 'aims to *prevent* them from occurring';
2. 'Privacy as the Default': 'ensuring that personal data are automatically protected in any given IT system or business practice … No action is required on the part of the individual to protect their privacy – it is built into the system, *by default*';
3. 'Privacy *Embedded* into Design': 'Privacy by Design is embedded into the design and architecture of IT systems and business practices … The

189 Ibid.

190 Paul Farrell, 'The Medicare Machine: Patient Details of "Any Australian" for Sale on Darknet', *The Guardian Australia* (online), 4 July 2017 <https://www.theguardian.com/australia-news/2017/jul/04/the-medicare-machine-patient-details-of-any-australian-for-sale-on-darknet>.

191 Department of Human Services, Submission No 7 to Senate Finance and Public Administration References Committee, *Inquiry into Circumstances in Which Australians' Personal Medicare Information Has Been Compromised and Made Available for Sale Illegally on the 'Dark Web'*, 4.

192 See Australian Digital Health Agency, *My Health Record Provider Portal Demonstration*, above n 81.

193 Health Care Industry Cybersecurity Task Force, above n 187, 6. See also Farrell, above n 190.

194 Australian Digital Health Agency, Submission No 4, above n 75, 4.

195 Office of the Victorian Information Commissioner for Privacy and Data Protection, 'Privacy by Design: Effective Privacy Management in the Victorian Public Sector' (Background Paper, 2018) <https://ovic.vic.gov.au/wp-content/uploads/2018/07/Privacy-by-Design-Background-Paper.pdf>.

result is that privacy becomes an essential component of the core functionality being delivered';

4. 'Full Functionality – Positive-Sum, not Zero-Sum': 'Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner';
5. 'End-to-End Security – Lifecycle Protection': 'Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved … This ensures that all data are securely retained, and then securely destroyed at the end of the process';
6. 'Visibility and Transparency': 'Privacy by Design seeks to assure all stakeholders that … the business practice or technology … is in fact, operating according to the stated promises and objectives';
7. 'Respect for User Privacy': 'Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options'.[196]

It is unclear how ADHA is implementing these principles given that the architecture of the MHR system does not meaningfully reflect many of them. There are insufficient measures in the MHR system to prevent intrusions into patients' confidentiality. Relevant legislation, described above, suggests that patients need to take action in order to protect their health information in their MHRs. Privacy does not seem to be a core component of the MHR system's design. Patients' interests appear not to be prioritised in this system. As patients' privacy is seemingly not adequately embedded into the system before their information is collected, it may not be preserved throughout the lifecycle of this data. The System Operator is currently required to retain records that include health information in patients' MHRs and are uploaded to the NRS for '30 years after the death of the [HR]; or if the System Operator does not know the date of death of the [HR] – 130 years after the date of birth of the [HR]', unless the HR or someone else requests it to cancel the HR's registration, in which case the System Operator must do so and then destroy these records (though it can retain the patients' names and HIs).[197] Storing patients' health information for such a long period of time might not only be unnecessary, but it could also heighten the risk of improper access to and disclosure of it. These periods of time far exceed the duration for which legislation in the Australian Capital Territory, New South Wales and Victoria requires health service providers to retain their health records (namely, for seven years after the service was last provided to the patient or, if

196 Ann Cavoukian, 'Privacy by Design – The 7 Foundational Principles – Implementation and Mapping of Fair Information Practices' (Document, Information and Privacy Commissioner of Ontario, May 2010) Appendix A, 6 <http://www.ontla.on.ca/library/repository/mon/24005/301946.pdf>.

197 *My Health Records Act 2012* (Cth) s 17(3), as inserted by *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth) sch 1 cl 6; see also ss 17(1)–(2), 51(1).

the patient was under 18 years of age when the information was collected, until the patient turns 25).[198]

ADHA may seek to assure stakeholders that patient confidentiality is maintained in the MHR system, but such pledges carry little weight given that the MHR system appears to lack 'strong privacy defaults'. While, to some degree, as Cavoukian proposes, the MHR system '[empowers] data subjects to play an active role in the management of their own data', it also makes them responsible for ensuring that the confidentiality of their health information is not breached and gives them little capacity to prevent 'misuses' of their information.[199] Further, in certain circumstances, their actions to impede access to and disclosure of their health information in their MHRs can be overridden.

V MAINTAINING PATIENT CONFIDENTIALITY IN AN ELECTRONIC HEALTH RECORDS SYSTEM

The major potential advantage of an electronic health records system can also pose the greatest threat to patient confidentiality: unification of up-to-date health information about patients and availability of it at the point of care, wherever that may be.[200] This is particularly pertinent to the MHR system. Another irony is that the MHR system makes patients responsible for protecting the confidentiality of their health information and, as a consequence of them attempting to do so, their health practitioners may have an incomplete, and thus inaccurate, record of their health details when they need it most. It is vital that the designers and developers of an electronic health records system find robust means of protecting patient confidentiality, while enabling health practitioners to access the information they require to provide optimal healthcare.

Proponents of the MHR system claim that it has several benefits. Principally, they assert that the system enables sharing of patients' health information between their healthcare providers, which they believe will improve patients' health outcomes.[201] They maintain that health practitioners will be able to make well-informed decisions regarding treatment of patients quickly and in coordination with each other, and ensure that patients are not given medication to which they may react adversely or subjected unnecessarily to repeat diagnostic tests and other investigatory procedures, which will save costs.[202] Further, they argue that, by facilitating patients' access to their health information, the system

198 *Health Records (Privacy and Access) Act 1997* (ACT) sch 1 PP 4.1(3)(b); *Health Records and Information Privacy Act 2002* (NSW) s 25; *Health Records Act 2001* (Vic) sch 1 HPP 4.2(b).

199 Cavoukian, above n 196, 5.

200 Barrows and Clayton, above n 31, 146; Mandl, Szolovits and Kohane, above n 29, 283–4; Schoenberg and Safran, above n 37, 1200.

201 Statement of Compatibility with Human Rights, My Health Records (National Application) Rules 2017 (Cth); Australian Digital Health Agency, Submission No 4, above n 75, 2.

202 Statement of Compatibility with Human Rights, My Health Records (National Application) Rules 2017 (Cth); Australian Digital Health Agency, Submission No 4, above n 75, 2; Brendan Murphy and Meredith Makeham, 'Letter to the Editor' (2017) 24 *Journal of Law and Medicine* 576, 576–7, n 7.

helps them to recall their medical history (which they will not need to repeat to multiple health practitioners) and make better decisions about their healthcare.[203]

These are undeniably worthy objectives. They are especially important where patients consult many health practitioners at different facilities to treat the same conditions, and each practitioner may not have all the relevant details about the patients' conditions and the treatment they have received.[204] Yet it appears that patient confidentiality is sacrificed in the attempt to achieve these aims in the MHR system. One of the key means of seeking to counter the erosion of patient confidentiality under this scheme is to empower patients to control access to their information. Although this is superficially appealing, it potentially thwarts fulfilment of the goals of the MHR system because it makes the information in patients' MHRs inherently unreliable. As David Markwell highlights, '[p]atients' control of records … may prevent professionals from accessing the information they need in order to fulfil … their responsibilities'.[205]

To substantiate the claim that relevant legislation protects patients' privacy in the MHR system, the Statement of Compatibility with Human Rights for the *My Health Records (National Application) Rules 2017* (Cth) refers to patients' choices to: opt-out of the system; suspend or cancel their registration; set access controls; ask health practitioners not to upload information to their MHRs; request that the Chief Executive Medicare's data not be included in their MHRs; and remove documents from their MHRs.[206] It is, however, precisely because these options are available to patients that their health practitioners cannot assume that the information in their MHRs is comprehensive.[207] Consequently, patients' MHRs can be, at best, useless and, at worst, misleading in a clinical context. Giving patients this authority can result in health practitioners lacking accurate and complete medical information and therefore providing inefficient, delayed or inappropriate healthcare,[208] the very situations that it was intended the MHR system would prevent arising. Indeed, the AMA has advised doctors, 'it is safest to assume the information in a patient's PCEHR is not a completely accurate record of the patient's clinical history or current health status, so all information should be verified from other sources of patient information, and ideally, with the patient'.[209] This recommendation begs the question: what is the purpose of the MHR system? If one of the principal purposes of the system is to generate data for research, this function will also be undermined if patients choose to deny access to information in their MHRs for such uses (the

203 Statement of Compatibility with Human Rights, My Health Records (National Application) Rules 2017 (Cth); Murphy and Makeham, above n 202, 576.

204 Ben-Assuli, above n 32, 288; Mandl, Szolovits and Kohane, above n 29, 284.

205 David Markwell, 'Commentary: Open Approaches to Electronic Patient Records' (2001) 322 *British Medical Journal* 286, 286.

206 Statement of Compatibility with Human Rights, My Health Records (National Application) Rules 2017 (Cth).

207 Mendelson and Wolf, 'My [Electronic] Health Record', above n 3, 292–3.

208 Schoenberg and Safran, above n 37, 1203.

209 Australian Medical Association, above n 52, [5.3.3].

Framework confirms that 'individual consumers who have a MHR will be able to opt out of the use of their MHR system data for secondary purposes').[210]

Designing a national electronic health records system that can facilitate health practitioners' swift access to detailed, relevant health information about patients, especially in emergencies, without compromising patient confidentiality is extremely challenging. Expanding the number of individuals who have access to the system can proportionally increase the threat to patient confidentiality.[211] Trisha Greenhalgh et al note, '[e]ven the simplest nationally shared electronic record is in reality technically very complex'.[212] Moreover, Randell observes, 'no complex IT system is completely reliable and secure', and 'one can (with difficulty) achieve any two of (a) high security, (b) sophisticated functionality, and (c) great scale – but achieving all three is currently (and may well remain) beyond the state of the art'.[213]

In general, following Cavoukian's 'The 7 Foundational Principles' for 'privacy by design' in developing an electronic health records system would be a critical starting point for minimising its potential erosion of the paradigm of patient confidentiality. This process would, however, likely entail an elimination or reversal of several elements of the current MHR system. For instance, it might require reverting to an opt-in model. Patients may need to provide valid, informed consent both to the uploading of each detail of their health information to the system and to health practitioners accessing specific records held in the system on each occasion that they seek to do so. It could be crucial that information about patients is neither aggregated nor stored in repositories that are accessible over the internet.[214] It might be preferable to contain 'minimal information' in silos, which are unconnected from one another and are 'under appropriate control'.[215] Randolph Barrows and Paul Clayton observe, '[w]ith remote access to distributed health data, or the pooling of health data from multiple sites in a central repository, the potential for loss of information privacy is greater than in isolated [electronic medical records] systems'.[216]

Perhaps no one user of the system would be permitted to view all of a patient's records,[217] and, instead, as submitters to the Senate inquiry suggested, 'only those who really need access to a person's record get only those parts of it that they need to see'.[218] It might be best if this is the default position, varied only with patients' explicit agreement. Consistent with Future Wise's recommendation to the Senate inquiry, the system could collect just the 'minimum necessary set of data' and ensure it is 'stored in a secure way for the

210 Department of Health, above n 103, 19.
211 Haas et al, above n 163, e26.
212 Trisha Greenhalgh et al, 'Introducing a Nationally Shared Electronic Patient Record: Case Study Comparison of Scotland, England, Wales and Northern Ireland' (2013) 82 *International Journal of Medical Informatics* e125, e134.
213 Randell, above n 166, 228, 230.
214 eHealth Privacy Australia, above n 184, 6.
215 Randell, above n 166, 228.
216 Barrows and Clayton, above n 31, 139.
217 eHealth Privacy Australia, above n 184, 6.
218 Culnane, Rubinstein and Teague, above n 113, 3.

minimum possible time, with access granted to only those with a legitimate need to access it'.[219] Together with their principal healthcare providers, patients could determine precisely 'what degree of authentication is required to satisfy need to know criteria for each clinical data item' before the system enables access to a record on the basis that the practitioner must read it to provide healthcare to the patient.[220] The only information from a patient's medical history that may need to be retained in an electronic health records system are details that are relevant for the patient's care in a future emergency.[221]

It might be impossible to create an electronic health records system on a national level that sufficiently protects patient information owing to the 'huge user population involved'.[222] Regardless of its size, to develop any electronic health records system that prioritises data security and patient confidentiality, medical specialists, lawyers, and privacy software engineers and designers may need to work closely together.[223]

VI CONCLUSION

Most Australians have been, currently are and/or will be patients. Therefore, since the opt-out period for the MHR system commenced on 16 July 2018, the government imposed on a majority of the population the need to make important decisions. For those of us who cherish the confidentiality of our health information, electing not to participate in the scheme may be the only viable choice. If we acquiesce, unwittingly or otherwise, to our MHR registration, we cannot be assured that the information we provide to our healthcare providers in the course of the therapeutic relationship will remain with them, and that only relevant details will be disclosed with our valid, informed consent for the purpose of treating us.

In response to growing public concern about the potential for loss of patient confidentiality in the MHR system, in December 2018, the Federal Parliament passed the *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth), following an inquiry by the Senate Community Affairs References Committee into the MHR system.[224] Some breaches of patient confidentiality that might otherwise have arisen under the MHR system will be prevented owing to the passage of this Act and other breaches might also be prevented if recommendations for amendments to the MHR system in the Senate Committee's Final Report,[225] delivered in October 2018, are implemented. For instance, the *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth) amends the *My Health Records Act 2012* (Cth) to prohibit the System

219 Future Wise, above n 71, 6.
220 Schoenberg and Safran, above n 37, 1200.
221 Ibid 1199–1200.
222 Randell, above n 166, 229.
223 Ibid 224.
224 Owen Griffiths, Department of Parliamentary Services (Cth), *Bills Digest*, No 30 of 2018–19, 16 October 2018, 7–10, 23.
225 Senate Community Affairs References Committee, Parliament of Australia, *My Health Record System* (2018).

Operator from disclosing patients' health information in their MHRs to law enforcement and government agencies unless they have an order from a judicial officer requiring the System Operator to do so.[226] In addition, the Senate Committee recommended applying record codes to patients' MHRs by default and preventing third parties from accessing patients' MHRs without their 'explicit permission', though these suggestions have not yet been implemented.[227]

Yet the *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth) and the Senate Committee's Final Report do not address all of the fundamental flaws in the design of the MHR system that threaten to undermine the traditional paradigm of patient confidentiality within the therapeutic relationship. As discussed above, these weaknesses include the following: the MHR system enables the linking and aggregation of a high volume of sensitive health information; the access points into the MHR system and thus the people who could access patients' MHRs are possibly countless; the system lacks sufficient means for preventing or reducing breaches of patient confidentiality; the extensive data in patients' MHRs can legitimately be disclosed in certain circumstances; control of clinical records is removed from clinicians and the institutions that support them; and the system is vulnerable to cyber hacking.

The ostensible potential benefits of the MHR system will not outweigh the damage that could ensue from the system's erosion of patient confidentiality. Although many patients would value an electronic health records system that enables accurate health information about them to be 'readily accessible to those who need' it to treat them, they will also be extremely concerned to preserve its confidentiality.[228] Any loss of confidentiality of their health information may undermine patients' trust in the health records system and even in their health practitioners. In Randell's words, '[t]rust is gained slowly and can be lost abruptly'.[229] Also, 'once lost', trust 'may be difficult to re-establish'.[230] As noted above, without trust in their health practitioners and the health records system, patients may be less candid with their practitioners, thereby diminishing the accuracy and comprehensiveness of information they provide to them. They might also be less willing to undergo testing and treatment. This could have adverse implications for individual and public health.

---

226 *My Health Records Act 2012* (Cth) s 69A, inserted by *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth) sch 1 cl 12; Explanatory Memorandum, My Health Records Amendment (Strengthening Privacy) Bill 2018 (Cth) 1, sch 1 items 10–12.

227 Senate Community Affairs References Committee, above n 225, 66, 68.

228 Rhona MacDonald, 'Commentary: A Patient's Viewpoint' (2001) 322 *British Medical Journal* 287, 287; Ben-Assuli, above n 32, 291.

229 Randell, above n 166, 230.

230 Mechanic and Meyer, above n 33, 668.