

The Senate

Community Affairs
References Committee

My Health Record system

October 2018

© Commonwealth of Australia 2018

ISBN 978-1-76010-848-9

Secretariat

Ms Jeanette Radcliffe (Committee Secretary)

Ms Kate Gauthier (Principal Research Officer)

Ms Hannah Dibley (Senior Research Officer)

Mr Michael Kirby (Senior Research Officer)

Mr Michael Finch (Research Officer)

Ms Carol Stewart (Administrative Officer)

PO Box 6100
Parliament House
Canberra ACT 2600

Phone: 02 6277 3515

Fax: 02 6277 5829

E-mail: community.affairs.sen@aph.gov.au

Internet: www.aph.gov.au/senate_ca

This document was produced by the Senate Community Affairs Committee Secretariat and printed by the Senate Printing Unit, Parliament House, Canberra.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Australia License.



The details of this licence are available on the Creative Commons website: <http://creativecommons.org/licenses/by-nc-nd/3.0/au/>

MEMBERSHIP OF THE COMMITTEE

45th Parliament

Members

Senator Rachel Siewert, Chair	Western Australia, AG
Senator Lucy Gichuhi (from 10 September 2018) Deputy Chair (from 13 September 2018)	South Australia, LP
Senator Slade Brockman, Deputy Chair (to 10 September 2018)	Western Australia, LP
Senator the Hon Kristina Keneally	New South Wales, ALP
Senator Steve Martin	Tasmania, NATS
Senator Louise Pratt	Western Australia, ALP
Senator Murray Watt	Queensland, ALP

Participating members for this inquiry

Senator Richard Di Natale	Victoria, AG
Senator Lisa Singh	Tasmania, ALP

TABLE OF CONTENTS

Membership of the Committee	iii
Abbreviations	vii
List of Recommendations	ix
Chapter 1	
Introduction	1
What is MHR?	1
What are the expected benefits of MHR?	3
Development of the MHR system	5
What structures are currently in place to guard against misuse?	8
Structure of the report.....	9
Conduct of the inquiry.....	9
Notes on references	10
Chapter 2	
Is My Health Record secure?	11
Is the design of the system secure?.....	11
Additional security protections for individuals	18
Who else could find out what is in MHR?	24
How else could information in the MHR system be used?	27
Chapter 3	
Using My Health Record.....	31
Populating a MHR.....	31
Default access controls	32
Clinical use	37

Chapter 4

Transitioning from opt-in to opt-out	45
Why adopt an opt-out system?	45
Supporting individuals to actively engage with the MHR system	50

Chapter 5

Conclusion and recommendations	65
System utility at the expense of patient privacy and security	65
Supporting individuals and practitioners to engage with the MHR system	69
Ongoing parliamentary oversight of the MHR system	70

Coalition Senators' Dissenting Report

Additional Comments by Coalition Senators	76
---	----

Labor Senators' Additional Comments

Appendix 1

Submissions and additional information received by the Committee	79
--	----

Appendix 2

Public hearings	87
-----------------------	----

ABBREVIATIONS

ACHWA	Aboriginal Health Council of Western Australia
ACTU	Australian Council of Trade Unions
ADHA	Australian Digital Health Agency
AHPA	Allied Health Professions Australia
AMA	Australian Medical Association
AMA(NSW)	Australian Medical Association (NSW)
APS	Australian Psychological Society
Bill	My Health Records Amendment (Strengthening Privacy) Bill 2018
CALD	culturally and linguistically diverse
CHF	Consumers Health Forum of Australia
CIS	clinical information system
committee	Community Affairs References Committee
Culnane, Rubinstein and Teague	Dr Chris Culnane, A/Prof Benjamin Rubinstein and Dr Vanessa Teague
DHS	Department of Human Services
DOH	Department of Health
DVA	Department of Veteran's Affairs
Evaluation	Siggins Miller, <i>Evaluation of the Participation Trials for the My Health Record</i> , November 2016
FECCA	Federation of Ethnic Communities Councils of Australia
LCA	Law Council of Australia
Legislation Committee	Senate Community Affairs Legislation Committee
MBS	Medicare Benefits Schedule
MHR	My Health Record

NAPWHA	National Association for People with HIV Australia
OAIC	Office of the Australian Information Commissioner
Orygen	Orygen, The National Centre of Excellence in Youth Mental Health
PBS	Pharmaceutical Benefits Scheme
PCEHR	Personally Controlled Electronic Health Records
PCEHR Bill	Personally Controlled Electronic Health Records Bill 2011
PHRN	Population Health Research Network
PIP	Practice Incentives Program
PLNSW	Positive Life NSW
QNMU	Queensland Nursing and Midwifery Union
RAC	Record Access Code
RACGP	Royal Australian College of General Practitioners
RACP	Royal Australian College of Physicians
RANZCP	Royal Australian and New Zealand College of Psychiatrists
RANZCR	Royal Australian and New Zealand College of Radiologists
RDAA	Rural Doctors Association of Australia
RFDS	Rural Flying Doctor Service
Royle Review	Richard Royle, Dr Steve Hambleton and Andrew Walduck, <i>Review of the Personally Controlled Electronic Health Record</i> , December 2013
Secondary Use Framework	<i>Framework to guide the secondary use of My Health Record system data</i>

LIST OF RECOMMENDATIONS

Recommendation 1

5.12 The committee recommends that record access codes should be applied to each My Health Record as a default and that individuals should be required to choose to remove the code. The committee further recommends that the ability to override access codes in the case of an emergency should only be available to registered healthcare providers for use in extraordinary and urgent situations.

Recommendation 2

5.15 The committee recommends that the Australian Government amend the *My Health Records Act 2012* to protect the privacy of children aged 14 to 17 years unless they expressly request that a parent be a nominated representative.

Recommendation 3

5.16 The committee recommends that the Minister for Health amend the My Health Record Rule 2016 to extend the period for which a My Health Record can be suspended in the case of serious risk to the healthcare recipient, such as in a domestic violence incident.

Recommendation 4

5.19 The committee recommends that data which is likely to be identifiable from an individual's My Health Record not be made available for secondary use without the individual's explicit consent.

Recommendation 5

5.21 The committee recommends that the current prohibition on secondary access to My Health Record data for commercial purposes be strengthened to ensure that My Health Record data cannot be used for commercial purposes.

Recommendation 6

5.23 The committee recommends that no third-party access to an individual's My Health Record be permissible, without the explicit permission of the patient, except to maintain accurate contact information.

Recommendation 7

5.25 The committee recommends that the Australian Government amend the *My Health Records Act 2012* and the *Healthcare Identifiers Act 2010* to ensure that it is clear that an individual's My Health Record cannot be accessed for employment or insurance purposes.

Recommendation 8

5.26 The committee recommends that access to My Health Records for the purposes of data matching between government departments be explicitly limited only to a person's name, address, date of birth and contact information, and that no other information contained in a person's My Health Record be made available.

Recommendation 9

5.28 The committee recommends that the legislation be amended to make explicit that a request for record deletion is to be interpreted as a right to be unlisted, and as such, that every record is protected from third-party access even after it is deleted, and that no cached or back-up version of a record can be accessed after a patient has requested its destruction.

Recommendation 10

5.32 The committee recommends that the Australian Digital Health Agency revise its media strategy to provide more targeted comprehensive education about My Health Record.

Recommendation 11

5.36 The committee recommends that the Australian Digital Health Agency identify, engage with and provide additional support to vulnerable groups to ensure that they have the means to decide whether to opt out, whether to adjust the access controls within their My Health Record and how to do this.

Recommendation 12

5.37 The committee recommends that the Australian Government commit additional funding for a broad-based education campaign regarding My Health Record, with particular regard to communicating with vulnerable and hard to reach communities.

Recommendation 13

5.38 The committee recommends that the Australian Government extend the opt-out period for the My Health Record system for a further twelve months.

Recommendation 14

5.45 The committee recommends that the My Health Record system's operator, or operators, report regularly and comprehensively to Parliament on the management of the My Health Record system.

Chapter 1

Introduction

1.1 The My Health Record (MHR) system is an electronic health record system that commenced operation in July 2012.¹ Although the system was originally designed on an opt-in basis, in May 2017 the government announced that the MHR system would transition to an opt-out system.² Members of the Australian public were originally given a three-month period to elect to opt-out. The deadline to opt-out was later extended to a four-month period concluding on 15 November 2018.³

1.2 In July and August 2018, concerns were raised in the media by medical commentators, general practitioners, IT professionals and journalists about the utility and security of the MHR system and whether members of the public should exercise their right to 'opt-out' of the new system.⁴

1.3 In this inquiry, the Community Affairs References Committee (committee) has considered the views of a wide range of stakeholders to assess whether the MHR system is working and how it can be improved to make MHR a more effective tool to support patients and improve healthcare delivery.

What is MHR?

1.4 MHR is an online folder of summary documents relating to a healthcare recipient's health that can be controlled by the individual. MHR can be used to record information such as allergies, blood test results or medical conditions a person has been diagnosed with.⁵

1.5 Some witnesses described MHR as being like a 'drop box' for health records: it provides a central place where copies of documents relating to a recipient's healthcare can be stored electronically, but the contents of and access to that box can be controlled by the healthcare recipient.⁶

1 Australian Digital Health Agency (ADHA), *Submission 31*, p. 3.

2 Department of Health (DOH) and Department of Human Services (DHS), *Submission 22*, p. 5.

3 DOH and DHS, *Submission 22*, p. 5.

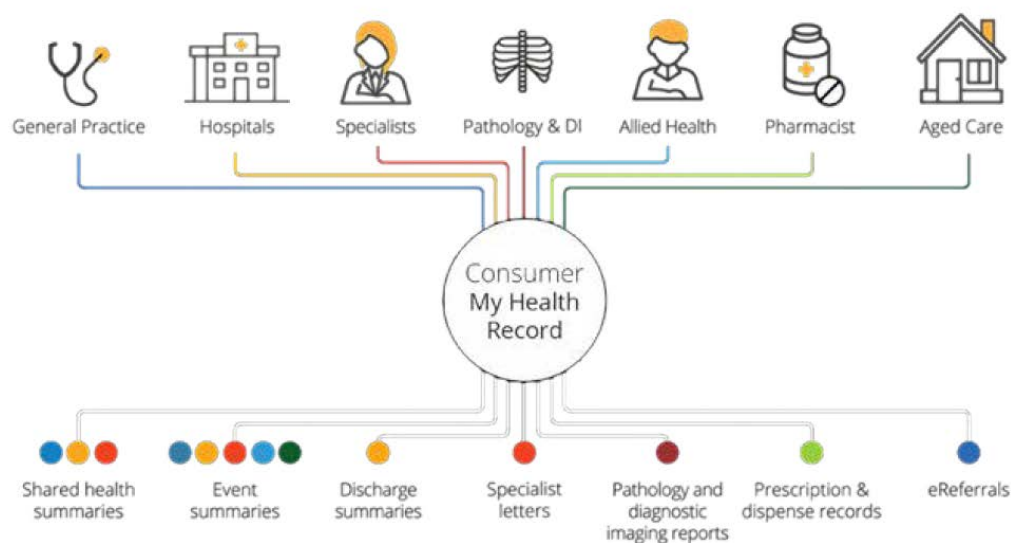
4 See for example: Ben Grubb and Jennifer Duke, 'Breach "inevitable" in digital health records – Serious concerns raised over federal government's digital health record system', *The Age*, 16 July 2018, p. 1; David Ellery, 'Why I have opted out', *The Canberra Times*, 18 July 2018, p. 15; Owen Evans, 'Shades of grey in IT dark side', *The Age*, 23 July 2018, p. 19; Dana McCauley, 'Millions to opt out of My Health Record as backlash builds – Criticisms of the scheme continue to mount and doctors threaten a boycott to protect their patients' privacy', *Sydney Morning Herald* (online), 25 July 2018.

5 ADHA, *What is in a My Health Record?*, <https://www.myhealthrecord.gov.au/for-you-your-family/what-is-my-health-record> (accessed 24 August 2018).

6 Ms Leanne Wells, Chief Executive Officer, Consumers Health Forum of Australia (CHF), *Committee Hansard*, 19 September 2018, p. 7; Mr Grahame Grieve, Principal, Health Intersections Pty Ltd, *Committee Hansard*, 17 September 2018, p. 13.

Figure 1: How does MHR work?

How does My Health Record work?



Source: Department of Health (DOH) and Department of Human Services (DHS), *Submission 22*, p. 2.

1.6 When a healthcare recipient first accesses their MHR, it is likely to be blank. When the healthcare recipient first visits their general practitioner, nurse or pharmacist, two years' worth of Medicare information and Pharmaceutical Benefits Scheme data will be uploaded to the healthcare recipient's MHR, unless this function has been turned off by the healthcare recipient prior to the visit.⁷

1.7 Over time, other documents including a summary of the individual's health, hospital discharge summaries, medication information, referral letters and test results can also be uploaded to the central depository.⁸

1.8 Once the health care recipient has registered, they can access their MHR via the online portal or via a mobile phone application.⁹

1.9 A key feature of the MHR is that the individual can control who can access their health information. A healthcare recipient is able to set a Record Access Control, which will protect their entire record, or they are able to set a Document Access Control, which will restrict access to a particular document in their record.¹⁰ Health

⁷ ADHA, *Submission 31*, [p. 27].

⁸ ADHA, *What is in a My Health Record?*, <https://www.myhealthrecord.gov.au/for-you-your-family/what-is-my-health-record> (accessed 24 August 2018).

⁹ Dr Nathan Pinski, Chair, RACGP Expert Committee, eHealth and Practice Systems, Royal Australian College of General Practitioners (RACGP), *Committee Hansard*, 11 September 2018, p. 40.

¹⁰ Mr Tim Kelsey, Chief Executive Officer, ADHA, *Committee Hansard*, 17 September 2018, pp. 35–36.

care recipients can then provide the necessary codes to the doctors they would like to have access to their MHR.¹¹

1.10 This facilitates the patient-centred flow of healthcare information whilst balancing the healthcare recipient's right to privacy.

What are the expected benefits of MHR?

1.11 Proponents of MHR point out that there are a multitude of potential benefits that may flow from having a personally controlled electronic health record.

1.12 The Australian Digital Health Agency (ADHA) advised the committee that 61 per cent of general practitioners and 79 per cent of pharmacists who have used MHR have already observed or experienced one or more actual benefits from use.¹² Some of these benefits are considered below.

Improved patient care, patient safety and medical communication

1.13 Submitters to the inquiry expect that MHR will lead to improved patient care, safety and medical communication.¹³ Future Wise advised the committee that the lack of interoperability between hospitals and general practitioners is a common source of medical error.¹⁴ MHR provides the ability for the hospital to attach discharge summaries, and event summaries and test results, such as pathology or diagnostic imaging, which may avoid these errors.¹⁵ MHR allows for information to be consolidated in one place, which may be convenient for both consumers and clinicians.¹⁶

Improved continuity of care between providers

1.14 MHR may also improve continuity of care for health care recipients when visiting different health care professionals.¹⁷

1.15 The Australian Bureau of Statistics data indicated that in 2016 almost 4 million Australians saw more than three different health practitioners for the same

11 Mr Kelsey, *Committee Hansard*, 17 September 2018, p. 36.

12 *Submission 31*, p. 4.

13 Future Wise, *Submission 15*, pp. 3, 5; People with Disabilities ACT Inc, *Submission 18*, p. 2; Rural Doctors Association of Australia (RDAA), *Submission 28*, p. 4; Multiple Sclerosis Australia, *Submission 32*, p. 4; Carers WA, *Submission 36*, p. 1; Positive Life NSW (PLNSW) and National Association for People with HIV Australia (NAPWHA), *Submission 44*, p. 3.

14 Future Wise, *Submission 15*, pp. 3, 5.

15 ADHA, *What is in a My Health Record?*, <https://www.myhealthrecord.gov.au/for-you-your-family/whats-in-my-health-record> (accessed 21 September 2018).

16 *Submission 31*, p. 4; Western Queensland PHN, *Submission 35*, p. 2; Queensland Nursing and Midwifery Union (QNMU), *Submission 41*, p. 3; Federation of Ethnic Communities Councils of Australia (FECCA), *Submission 45*, p. 2.

17 DOH and DHS, *Submission 22*, p. 6; Royal Australian and New Zealand College of Psychiatrists (RANZCP), *Submission 30*, p. 2; *Submission 32*, p. 4; Western Queensland PHN, *Submission 35*, p. 2; QNMU, *Submission 41*, p. 3; FECCA, *Submission 45*, p. 2.

condition.¹⁸ People with Disabilities ACT Inc noted that research conducted by the Australian Institute of Health and Welfare found that 17 per cent of people with disabilities who saw three or more health professionals reported issues caused by a lack of communication between them.¹⁹ MHR can allow an individual to share their health summary securely with each of their healthcare providers to support better continuity of care between providers.²⁰

Reduced need to recite medical history

1.16 By having a consolidated electronic health record, there may be less need for patients, who could be quite unwell, to explain their medical history to multiple practitioners.

1.17 Submitters noted that a centralised health record would obviate the need for health care recipients with complex symptoms and medications, to explain all of their symptoms and history when they attend an emergency room or see a new doctor.²¹ Similar benefits could also be gained by people with lower English language proficiency, people with intellectual disabilities or consumers who move between states or see practitioners in multiple locations.²²

Empower health care recipients

1.18 MHR may assist to empower health care recipients to more fully participate in their own healthcare.

1.19 Currently, health recipients often do not get to see their own health records. Consumers Health Forum of Australia noted that there is already an information asymmetry that exists between health care recipients and health professionals. By allowing health care recipients to see their own health records and to control access to them, they may be empowered to play a more active part in their own health care.²³

Reduce adverse drug events because of medication errors

1.20 Adverse drug events are common. Each year 230 000 adverse medication events lead to hospitalisation.²⁴ MHR has the capacity to reduce those errors by

18 ADHA, *Submission 31*, p. 3.

19 People with Disabilities ACT Inc, *Submission 18*, p. 2.

20 QNMU, *Submission 41*, p. 3; Doctors Reform Society, *Submission 29*, [p. 1].

21 RDAA, *Submission 28*, p. 4; Multiple Sclerosis Australia, *Submission 32*, p. 3.

22 People with Disabilities ACT, *Submission 18*, p. 2; RDAA, *Submission 28*, p. 4; RANZCP, *Submission 30*, p. 2; Multiple Sclerosis Australia, *Submission 32*, p. 3; Institute for Healthcare Transformation, Deakin University, *Submission 37*, p. 2.

23 CHF, *Submission 16*, p. 12; DOH and DHS, *Submission 22*, p. 6; *Submission 32*, p. 3; *Submission 37*, p. 2.

24 Dr Chris Moy, Member, AMA Federal Council; Chair, Federal Ethics and Medico-Legal Committee, Australian Medical Association (AMA), *Committee Hansard*, 11 September 2018, p. 32; ADHA, *Submission 31*, p. 3; Pharmaceutical Society of Australia, *Submission 46*, p. 4; AMA, *Submission 79*, p. 7; Medicines Australia, *Submission 81*, p. 2; Bayer Australia, *Submission 89*, p. 1; Health Workers Union, *Submission 96*, p. 7.

having available a list of medications that have been prescribed to the health care recipient and, if health summary has been uploaded, a more complete picture of the patient's health that may inform the medications pharmacists or doctors may prescribe.²⁵

Public health research

1.21 Information from healthcare recipients who do not elect to 'Withdraw Participation' may have their de-identified data used for public health research purposes.²⁶ The data MHR contains, when aggregated, may provide researchers with ability to more comprehensively understand the use, cost and effectiveness of health services and the outcomes that healthcare recipients are achieving as a result of those services.²⁷ A healthcare recipient can nominate not to have their data used for secondary use purposes by selecting the 'withdraw participation' button in their MHR.²⁸

Development of the MHR system

1.22 The MHR system has been in development for some time.

1.23 In 2009 the National Health and Hospitals Reform Commission recommended that 'by 2012 every Australian should be able to have a personal electronic health record that will at all times be owned and controlled by that person'.²⁹

1.24 To enable individuals to have a personal electronic health record, a system was required to assign all Australians with an identifying number that would be unique to them to ensure that the correct health information was assigned to the correct person. In 2010, the *Healthcare Identifiers Act 2010* was passed for that purpose.³⁰

1.25 In 2011, the Personally Controlled Electronic Health Records Bill 2011 (PCEHR Bill) was introduced to establish the legal framework for a national electronic health records system. The PCEHR Bill was referred to the Senate

25 Dr Moy, *Committee Hansard*, 11 September 2018, p. 32; Future Wise, *Submission 15*, p. 5; Australian Council of Trade Unions (ACTU), *Submission 17*, p. 2; RANZCP, *Submission 30*, p. 2; ADHA, *Submission 31*, p. 3; Allied Health Professions Australia, *Submission 33*, [p. 4]; Pharmaceutical Society of Australia, *Submission 46*, p. 2.

26 ADHA, *Submission 31*, p. 33.

27 Population Health Research Network (PHRN), *Submission 4*, p. 2; ACTU, *Submission 17*, p. 2; Institute for Healthcare Transformation, Deakin University, *Submission 37*, p. 2.

28 ADHA, *Submission 31*, p. 33.

29 The Hon. Nicola Roxon MP, Minister for Health, *House of Representatives Hansard*, 23 November 2018, p. 13576; National Health and Hospitals Reform Commission, *A Healthier Future for All Australians*, Final Report, June 2009, p. 34 (Recommendation 115).

30 DOH and DHS, *Submission 22*, p. 4; *Healthcare Identifiers Act 2010*, s. 3. Medicare numbers were not sufficient for this purpose because multiple people can be assigned the same Medicare number and a Medicare number is not fixed throughout a person's life.

Community Affairs Legislation Committee (Legislation Committee) for inquiry and report.³¹ In that report, the Legislation Committee made three recommendations:

- that the review of the Act explicitly consider whether the Secretary of the Department of Health was the appropriate person to be the system operator;
- that the review of the Act consider the opt-in design and consider the feasibility of transitioning to an opt-out system; and
- that the Bill be passed.³²

1.26 The then Government made a number of amendments in response to concerns raised during the committee's inquiry and the Bill was passed by the Parliament.³³

1.27 In 2013 a review of the Personal Electronic Health Record system was conducted by Mr Richard Royle, Dr Steve Hambleton and Mr Andrew Walduck (Royle Review).³⁴ The Royle Review made 38 recommendations including renaming the system MHR and transitioning to an opt-out system.³⁵ Legislation was introduced to give effect to the change of name in 2015.³⁶

2016 MHR participation trials

1.28 In 2016 DOH commissioned four trial sites: two opt-in sites—covering a number of general practices in Perth, Western Australia, and at the Ballarat Hospital in Victoria—and two opt-out trial sites in the North Queensland and the Nepean Blue Mountains Primary Health Network areas.³⁷

1.29 The evaluation of those trials found that there was evidence to support 'the stakeholder consensus that opt-out should be the participation model into the future'.³⁸ It found that there were statistically significant increases in: individual awareness of the MHR, individual and healthcare provider recall of communication about the MHR; individual registration and use of the MHR system; healthcare provider

31 *Journals of the Senate*, No. 72, 25 November 2011, p. 1961.

32 Community Affairs Legislation Committee (Legislation Committee), Personally Controlled Electronic Health Records Bill 2011 [Provisions]; Personally Controlled Electronic Health Records (Consequential Amendments) Bill 2011 [Provisions], March 2012, pp. 11, 18, 31.

33 [Supplementary Explanatory Memorandum](#), Personally Controlled Electronic Health Records Bill 2011, p. 1, <https://www.legislation.gov.au/Details/C2011B00258/Supplementary%20Explanatory%20Memorandum/Text> (accessed 21 September 2018); *Journals of the Senate*, No. 92, 19 June 2012; *House of Representative Votes and Proceedings*, No. 116, 21 June 2012, p. 1597. The Act was renamed the My Health Records Act 2012 in 2015.

34 Richard Royle, Dr Steve Hambleton and Andrew Walduck, *Review of the Personally Controlled Electronic Health Record*, December 2013 (Royle Review).

35 Royle Review, pp. 15–16 (Recommendations 1, 13).

36 *Health Legislation Amendment (eHealth) Act 2015*, sch. 2.

37 Siggins Miller, *Evaluation of the Participation Trials for the My Health Record*, November 2016 (Evaluation).

38 Evaluation, p. xi.

organisations registered to use the MHR system, health provider document uploads to and viewings of MHRs.³⁹

1.30 Two other findings from the trials are notable. First, once the benefits of MHR were explained, focus group participants 'said that their concerns about security and privacy, or about the fact that a My Health Record had been created, disappeared'.⁴⁰ The second is that the focus group participants strongly suggested that a 'bigger emphasis on awareness and education' would be required for a national change.⁴¹

1.31 These trials and their evaluation have guided some aspects of the national rollout of MHR, such as the communication strategy.⁴²

Opt-out model

1.32 In 2015, Parliament provided an option for the Minister for Health to make rules to provide for a national opt-out model after consulting with the relevant Ministerial Council comprising representatives of the state and territory governments.⁴³

1.33 In May 2017, the Australian Government announced that it would transition to an opt-out model as part of the 2017–18 Budget.⁴⁴ The rule giving legal effect to that announcement was made on 30 November 2017.⁴⁵

1.34 The period to allow individuals to opt-out of the MHR system commenced on 16 July 2018 and it will conclude on 15 November 2018.⁴⁶

Opting out

1.35 There are a number of ways an individual can elect to opt-out.

1.36 To opt out, an individual needs to verify their identity by producing their Medicare Card or Department of Veteran's Affairs (DVA) card and either their driver licence, passport or ImmiCard.

1.37 Under the current system there is the ability to request cancellation of their registration in the MHR system.⁴⁷

39 Evaluation, p. xi.

40 Evaluation, p. vi.

41 Evaluation, p. vii.

42 Ms Tania Rishniw, First Assistant Secretary, Portfolio Strategies Division, DOH, *Committee Hansard*, 17 September 2018, p. 39.

43 *Health Legislation Amendment (eHealth) Act 2015*, sch. 1, item 106.

44 DOH and DHS, *Submission 22*, p. 5.

45 [My Health Records \(National Application\) Rules 2017](#), r. 5.

46 DOH and DHS, *Submission 22*, p. 5. The opt-out date was originally designated as 15 October but on 9 August it was extended by a month to 15 November 2018. See [My Health Records \(National Application\) Amendment \(Extension of Opt-out Period\) Rules 2018](#).

47 *My Health Records Act 2012*, s. 51(2).

1.38 The Parliament is currently considering the My Health Records Amendment (Strengthening Privacy) Bill 2018 (Bill). This Bill would allow for a person to request deletion of records that are held about them in the MHRs system.⁴⁸

Current participation in the system

1.39 The Chief Executive of the ADHA, Mr Tim Kelsey, told the committee that, as at 12 September 2018, approximately 900 000 people have opted out, and that the opt-out rate is three percent.⁴⁹ The committee heard that it was not possible to provide accurate data as there are a number of channels available to people to opt-out of the system: internet, telephone and on paper. Ms Caroline Edwards from DOH explained that the paper returns will not be processed until after the opt-out period.⁵⁰ Mr Kelsey advised the committee:

Maybe the salient figures would be 6.1 million currently have a My Health Record. Since the start of opt out 181,000 have opted in. So we've had roughly 900,000 opting out, your correct, but at the same time 181,000 people have opted in to the system, since opt out, obviously wanting to take advantage of the benefits ahead of opt out being realised later this year. What we're saying is that the total number of 6.1 million incorporates those who have opted in since the start of opt out.⁵¹

1.40 Mr Kelsey also advised the committee that the ADHA had anticipated significantly higher levels of opt out than it was currently seeing and that the opt-in rates are very much higher than the rates seen over the previous six years.⁵²

What structures are currently in place to guard against misuse?

1.41 There are a number of structures and penalties in place to guard against misuse of data contained in a MHR.

1.42 Under the *My Health Records Act 2012*, there are heavy penalties for the unauthorised use, collection or disclosure of health information. The criminal penalty is up to two years imprisonment and/or \$25 200 for an individual or \$126 000 for bodies corporate. The civil penalty is up to \$126 000 for an individual or \$630 000 for a body corporate.⁵³

1.43 Knowingly breaching restricted data may lead to a criminal penalty under the *Criminal Code Act 1995*.⁵⁴

48 My Health Records Amendment (Strengthening Privacy) Bill 2018 (Bill), schedule. 1, item 6.

49 Mr Kelsey, *Committee Hansard*, 17 September 2018, pp. 33–34.

50 Ms Caroline Edwards, Deputy Secretary, DOH, *Committee Hansard*, 17 September 2018, p. 33.

51 *Committee Hansard*, 17 September 2018, p. 37.

52 *Committee Hansard*, 17 September 2018, p. 37.

53 DOH and DHS, *Submission 22*, p. 13.

54 DOH and DHS, *Submission 22*, p. 13.

1.44 The Office of the Australian Information Commissioner is empowered under the *My Health Records Act 2012* and the My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016 to investigate breaches to the My Health Records Act and to address them through conciliation, education or enforcement actions, including enforceable undertakings, injunctions or civil penalties.⁵⁵

1.45 There are also a number of information technology measures that protect the MHR system from unauthorised access. These are considered in greater detail in the next chapter.

Structure of the report

1.46 This report is organised into five chapters.

1.47 **Chapter 2** considers concerns about the privacy and security of the MHR.

1.48 **Chapter 3** considers concerns that have been raised by submitters about using the MHR system.

1.49 **Chapter 4** will consider the reasons the opt-out model was adopted, why some groups are advocating for a return to opt-in and concerns people have raised about their experiences trying to opt-out.

1.50 **Chapter 5** will contain the committee's conclusions and recommendations.

Conduct of the inquiry

1.51 The Senate referred the MHR system inquiry to the committee on 15 August 2018 for inquiry and report by 8 October 2018.⁵⁶ On 19 September 2018, the Senate agreed to extend the time for reporting to 12 October 2018.⁵⁷ The committee received further extensions on 12 October and 17 October 2018 to finalise its report.⁵⁸ The committee reported to the Senate on 18 October 2018.

1.52 While the committee was conducting this inquiry, the Legislation Committee was conducting an inquiry into the My Health Records Amendment (Strengthening Privacy) Bill 2018. On 28 August 2018 the committee and the Legislation Committee agreed to share evidence relevant to each inquiry. A statement was placed on each committee's website to that effect.⁵⁹

55 My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016.

56 *Journals of the Senate*, No. 108, 15 August 2018, pp. 3471–3472.

57 *Journals of the Senate*, No. 120, 19 September 2018, p. 3823.

58 *Journals of the Senate*, No. 122, 15 October 2018, p. 3869; *Journals of the Senate*, No. 124, 17 October 2018, p. 3961.

59 Community Affairs References Committee, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Community_Affairs (accessed 18 September 2018).

1.53 In accordance with its usual practice, the committee advertised the inquiry on its website and wrote to 57 individuals and organisations inviting submissions by 14 September 2018. The committee continued to accept submissions after that date.

1.54 The committee received 118 submissions from individuals and organisations. A list of submissions received by the committee is available at Appendix 1 and copies of public submissions can be accessed via the committee's website.

1.55 The committee held three public hearings in Canberra on 11 September, 17 September and 20 September 2018. A list of the witnesses who appeared at each hearing is available at Appendix 2.

1.56 The committee thanks all the individuals and organisations who submitted to the inquiry and appeared as witnesses.

Notes on references

1.57 References in this report are to Committee Hansard are to proof transcripts. Page numbers may vary between the proof and official transcripts.

Chapter 2

Is My Health Record secure?

2.1 Throughout this inquiry, submitters have raised concerns about the security of the My Health Record system (MHR). This chapter will consider the design of the system and the protections it includes, what individuals can do to enhance the privacy of their own records and whether those protections are sufficient to protect vulnerable members of the community. The chapter will then examine whether the record can be legitimately accessed by employer nominated doctors or law enforcement agencies and what secondary or tertiary purposes MHR data could be used for.

Is the design of the system secure?

2.2 Submitters and witnesses to the inquiry expressed concerns about the risks of unauthorised access to MHR data. Submitters who raised these concerns commonly referred to the way the system was designed.

Centralised database

2.3 There are two broad ways of designing a data management system: the first is a distributed or federated model where data is stored in decentralised repositories.¹ The second model is a centralised repository or database. MHR is a form of centralised database.²

2.4 Mr Grahame Grieve from Health Intersections explained the difference between a centralised database like MHR and a distributed system:

In a centralised database, all the information flows up to the central repository and then out of it. It's like a hub-and-spoke model with public transport: everyone goes to the city to get anywhere. Whereas a distributed system means you go directly to the source of the information and hold it there.³

2.5 Mr Grieve explained to the committee that there is a balance that needs to be managed between utility and privacy when considering which model should be adopted:

As you build a single repository, you have the benefits of scale and the problems of broad access. That's why there's space for multiple scales of repository to choose the optimal point for a particular context. For some

1 Dr Nathan Pinski, Chair, RACGP Expert Committee eHealth and Practice Systems, Royal Australian College of General Practitioners (RACGP), *Committee Hansard*, 11 September 2018, p. 45; Australian Privacy Foundation, *Submission 1*, p. 30; Dr Andrew Magennis, *Submission 57*, pp. 4–5.

2 Mr Paul Power, *Committee Hansard*, 11 September 2018, p. 18; Centre for Digital Business, *Submission 2*, p. 2.

3 Mr Grahame Grieve, Principal, Health Intersections Pty Ltd, *Committee Hansard*, 17 September 2018, p. 12.

people there is an issue that we want everybody's medications to be available for drug-to-drug interaction testing. On the other hand, making everyone's medications available for that has privacy concerns...⁴

2.6 As an example of the clinical benefits that can come from having a centralised database with lower privacy restrictions, Mr Kelsey from the Australian Digital Health Agency (ADHA) explained that the Northern Territory's experience with its e-health record indicated that having no privacy restrictions meant that clinicians could obtain the information that they needed at the time it was needed and that citizens could obtain the clinical benefits of having an electronic health record without needing to engage with it.⁵

Risk of external unauthorised access

2.7 Some submitters raised concerns that having broad access to a centralised database makes it hard to secure. The Centre for Digital Business described the design of MHR as 'a centralised database with widespread access at the edge'.⁶ That means that the data for MHR is held in a centralised database but that a large number of healthcare providers are granted access to records in the database. Most submitters considered that there would be approximately 900 000 health practitioners who would have access to the central repository.⁷

2.8 The Centre for Digital Business explained that having so many potential access points was a potential source of vulnerability for the system if those access points could not be properly secured:

A system is only as resilient as its weakest link. Even if "military grade" security applies to the centralised database... securing access at the edge involving some 900,000 individuals in a great variety of environments, is a far greater almost impossible challenge.⁸

2.9 A number of other submitters and witnesses, such as information technology specialists Dr Robert Merkel and Mr Paul Power, were also concerned that keeping the log-in mechanisms and passwords of 900 000 health practitioners secure may be a challenge.⁹

4 Mr Grieve, *Committee Hansard*, 17 September 2018, p. 13.

5 Mr Tim Kelsey, Chief Executive Officer, Australian Digital Health Agency (ADHA), *Committee Hansard*, 17 September 2018, p. 41.

6 Centre for Digital Business, *Submission 2*, p. 2.

7 Mr Power, *Committee Hansard*, 11 September 2018, p. 18; Centre for Digital Business, *Submission 2*, p. 5; Dr Thinus van Rensburg, *Submission 8*, [p. 2]; Information and Privacy Commission NSW, *Submission 43*, p. 1; Women's Legal Service NSW, *Submission 48*, p. 2; Dr David G More, *Submission 54*, p. 3.

8 Centre for Digital Business, *Submission 2*, p. 5.

9 Mr Power, *Committee Hansard*, 11 September 2018, p. 18; Dr Robert Merkel, *Committee Hansard*, 11 September 2018, p. 22.

2.10 This concern is particularly acute in health professions where existing practices can be lax.¹⁰ The Information and Privacy Commission of New South Wales told the committee that poor information practices, such as passwords being kept next to access terminals, keeping systems logged in for faster access, failing to limit access to only essential staff and using generic logins, were becoming more common.¹¹

2.11 Against that backdrop, the Centre for Digital Business considered that the security challenge facing MHR was 'practically unresolvable'.¹²

2.12 The ADHA advised the committee that healthcare organisations must connect to the network through conformant software with a secure and encrypted connection that requires two-factor identification in addition to any local authentication process.¹³

2.13 Concerns that the system may not be able to be secured at the health practitioners' point of access was given greater prominence because a centralised database is also potentially a more substantial target for cyber-criminals because it contains a large amount of valuable data.¹⁴

2.14 Medical data is considered to be valuable to health recipients and to clinicians,¹⁵ but it is also potentially valuable for commercial and identity fraud purposes.¹⁶ Some witnesses described the aggregation of valuable data in one database as a 'honey pot' that may attract criminals.¹⁷

2.15 Dr Merkel told the committee that he believed that the number of people with legitimate access increased the possibility of a successful attack by criminals because it was inevitable that not all of the health practitioners will be able to keep their accounts secure:

...if you have that many people with legitimate access, the odds of somebody electronically impersonating that person by stealing their passwords and gaining access to their account—the other things you need to get on the system—it's inevitable that criminals will find ample people

10 Dr Thinus van Rensburg, *Submission 8*, [p. 1].

11 Information and Privacy Commission NSW, *Submission 43*, p. 2.

12 Centre for Digital Business, *Submission 2*, p. 6.

13 ADHA, *Submission 31*, p. 8.

14 Mr Grieve, *Committee Hansard*, 17 September 2018, p. 14; Professor Chris Bain, *Committee Hansard*, 11 September 2018, p. 28; Doctors Reform Society, *Submission 29*, [p. 2]; Positive Life NSW and National Association of People with HIV Australia, *Submission 44*, p. 5.

15 Professor Kerry Phelp, *Committee Hansard*, 11 September 2018, p. 3; Dr Thomas Rechnitzer, *Submission 56*, [p. 3].

16 Name withheld, *Submission 9*, [p. 2]; Future Wise, *Submission 15*, p. 11; Maurice Blackburn Lawyers, *Submission 25*, p. 10.

17 Mr Paul Shetler, *Committee Hansard*, 17 September 2018, pp. 3, Ms Olga Ganopolsky, Chair, Privacy Law Committee, Business Law Section, Law Council of Australia (LCA), *Committee Hansard*, 17 September 2018, p. 28.

who, for whatever reason, have not kept their accounts secure. This is what hackers do. They're very skilled at it.¹⁸

2.16 Dr Merkel said that it may also be reasonable to assume that some of the groups who may seek to attack a central database will have sophisticated operations:

Some of those individuals and organisations are extremely well resourced, skilled and determined, so the data in My Health Record needs to be extremely well protected. And, while the core system may well indeed be well protected, my understanding is that hundreds of thousands of health practitioners will have access to My Health Record information, and the log-in mechanisms for some of the ways you can get in and access that data are considerably less hacker-resistant than they should be.¹⁹

2.17 Some submitters considered that if the central database is breached, the attacker is likely to obtain broad access to the database.²⁰

2.18 For this reason, some submitters favoured a federalised or decentralised model.²¹ One of the benefits of a decentralised model is that less information is contained in each system, making the risk of disruption or unauthorised access smaller.²²

2.19 However, the committee heard that when the MHR system was first designed, a federated model was not really possible and the system that exists is limited by those initial design choices:

The design of the system and the standards it is based on were state of the art in 2007. Although a more distributed design was initially planned, it is now, unfortunately, a centralised national database of static summary documents. This was an inevitable consequence of the technical standards used at the time...²³

2.20 Professor Chris Bain, a digital health expert, told the committee that whilst a distributed model might be preferable from a technical perspective, it is not the model that currently exists and it would be a substantial investment to change it:

Some people have put forward technical architectures where the information isn't actually held all in one place. You might have demographic data held in one repository, general practice data held in another repository and hospital data held in another repository and you bring it together in a virtual view, if you like, but it never actually sits in

18 Dr Merkel, *Committee Hansard*, 11 September 2018, p. 22.

19 *Committee Hansard*, 11 September 2018, p. 19.

20 Dr Bernard Robertson-Dunn, Chair, Health Committee, Australian Privacy Foundation, *Committee Hansard*, 11 September 2018, p. 13; Dr Merkel, *Committee Hansard*, 11 September 2018, p. 22.

21 Dr Robertson-Dunn, *Committee Hansard*, 11 September 2018, p. 13.

22 Dr Robertson-Dunn, *Committee Hansard*, 11 September 2018, p. 14; Mr Shetler, *Committee Hansard*, 17 September 2018, p. 3.

23 Health Intersections, *Submission 14*, [p. 2].

one large database. There are arguments for that, but we don't have that in front of us at the minute.²⁴

Protecting the system

2.21 The ADHA accepts that the system needs to be able to protect Australia's health information for the system to have legitimacy:

The Agency understands that healthcare information is some of the most private information people have, and that the success of Australia's digital health program is reliant on secure digital operations and respecting people's rights to privacy.²⁵

2.22 The ADHA advised the committee that it is aware that certain safeguards are vulnerable and so it has developed a security design called 'defence in depth'.²⁶ This security design employs a range of security measures that operate simultaneously to protect the data that has been entrusted to it. This includes comprehensive security monitoring, process and technology security controls, security assurances and a dedicated security operations management team.²⁷

2.23 The ADHA informed the committee that the system has been certified and accredited under the Australian Government Information Security Manual and the Protecting Security Policy Framework by an independent assessor.²⁸

2.24 The ADHA also notes that there are stringent penalties and criminal penalties attached to the misuse of MHR information.²⁹

2.25 Future Wise noted that this is an important area to get right because medical privacy, once breached, cannot be restored:

Privacy of medical confidentiality is a one-way door; penalties and sanctions may serve as deterrents, or as compensation for the loss of privacy, but neither give individuals their privacy back if it is breached.³⁰

Is MHR less secure than the existing system?

2.26 In determining how much weight to afford to the above concerns, some submitters stressed that they should be considered against the status quo that exists for the current circulation of medical information.

2.27 A lack of interoperability between clinical systems means that Australian health practitioners still largely rely on transmitting documents by fax.³¹ Dr Chris

24 *Committee Hansard*, 11 September 2018, p. 29.

25 ADHA, *Submission 31*, pp. 13–14.

26 ADHA, *Submission 31*, p. 8.

27 ADHA, *Submission 31*, p. 8.

28 ADHA, *Submission 31*, p. 8.

29 ADHA, *Submission 31*, p. 10.

30 Future Wise, *Submission 15*, p. 11.

Moy from the Australian Medical Association explained that fax is not a very private or effective method of communicating important health information:

...I get a call in the middle of a consultation, I have other patients in front of me, I try to rustle together a few bits of information and I fax it away. This isn't particularly private, because I don't know whether it ends up where it is [needed], and it's absolutely no use if I'm not there after hours.³²

2.28 Dr Moy told the committee that he believed it was important for the discussion about privacy to start from an understanding of the vulnerabilities in the current system:

The problem is that the current debate so far has not been an apple versus apple situation. Really, we've had a debate about My Health Record versus this sort of mythical utopia of perfect privacy: it's not been a debate about My Health Record versus the sad reality of this fax land and all the harm that goes with it.³³

2.29 The current system is vulnerable to unauthorised access. One submitter noted that:

In 2018 there has been well-publicised disciplinary action against healthcare workers in South Australia and Western Australia for inappropriately accessing individual records to which they had no clinical need to access, highlighting the importance of the "insider threat" to privacy.³⁴

2.30 With the current procedures for handling medical records, healthcare recipients have no way of knowing who has viewed, accessed or shared components of their health information.³⁵

2.31 Proponents of MHR note that the new system will have an electronic audit trail that means that the healthcare recipient can see who has accessed their information. The ADHA noted that these audit logs are updated in real time and that healthcare recipients can elect to be notified when someone accesses their record:

Every access to every health record is logged in an audit trail and immediately visible to the consumer. A consumer can elect to get a text message or email when a new healthcare provider accesses the record or when certain things happen to the record such as a new shared health summary being uploaded, or when someone 'breaks the glass' to access their record.³⁶

31 Prof Phelps, *Committee Hansard*, 11 September 2018, p. 4; Dr Chris Moy, Member, AMA Federal Council; Chair, Federal Ethics and Medico-Legal Committee, Australian Medical Association (AMA), *Committee Hansard*, 11 September 2018, p. 32.

32 *Committee Hansard*, 11 September 2018, p. 32.

33 *Committee Hansard*, 11 September 2018, p. 32.

34 Future Wise, *Submission 15*, pp. 10–11 (footnotes omitted).

35 ADHA, *Submission 31*, p. 31.

36 *Submission 31*, p. 28.

2.32 Professor Chris Bain noted that where people have inappropriately accessed records, an electronic audit trail means that the offenders can be caught and punished:

it's very clear and visible to the patient, most importantly, who's accessing it. Patients, unless they go through a whole lot of rigmarole...will struggle to know who in any given hospital has looked at their records and whether it was just the treating team or others who sniffed around. We've had examples in South Australia of people who were caught out because they sniffed around. That's only because there's an electronic system and an audit trail.³⁷

2.33 However, some submitters, such as the Office of the Australian Information Commissioner noted that these audit logs only show access at the organisational level.³⁸ This means that if a healthcare recipient wants to know who within the organisation access their record they need to contact the organisation concerned.³⁹

2.34 Separate arrangements apply for the System Operator which, in most cases, can track access at the individual practitioner level.⁴⁰ Some submitters noted that it would be desirable for consumers to be able to have access logs at an individual level.⁴¹

Committee view

2.35 The committee understands that there are potential security vulnerabilities associated with having a centralised database with broad access. The committee acknowledges that having a system that is able to be accessed by such a large number of health practitioners provides opportunities for external unauthorised access by actors who may wish to take advantage of the data for their own purposes.

2.36 However, the committee also acknowledges that there are some clinical benefits to the model that has been adopted. A centralised database provides clinicians with the ability to access information as it is required, unless the healthcare recipient has activated one or more of the privacy settings.

2.37 While a federated model may have been preferable if the system was to be designed today. The committee acknowledges that a substantial investment has been made in the current system and that fundamentally redesigning the system would involve additional investment.

2.38 The committee notes that the ADHA has undertaken considerable work to secure the information held within the MHR system. However, the committee notes

37 *Committee Hansard*, 11 September 2018, p. 28.

38 Dr van Rensberg, *Submission 8*, [p. 1]; Office of the Australian Information Commissioner (OAIC), *Submission 26*, p. 9, QNMU, *Submission 41*, p. 7; Office of the Information Commissioner Queensland, *Submission 98*, [p. 1].

39 *Submission 26*, p. 9.

40 *Submission 26*, p. 9.

41 *Submission 98*, [p. 1].

that the system may become a more substantial target as the number of records held within the system increases.

Additional security protections for individuals

2.39 MHR was designed to be a system that could be controlled by the healthcare recipient. To add to the security of their records, healthcare recipients can apply a number of privacy settings to their MHR.

2.40 These privacy controls include a record access control, which protects the entire record, a document access code, to restrict access to a particular document, or a healthcare recipient could set up an email alert when a new organisation first accesses the healthcare recipient's record.⁴² The Health Workers Union told the committee that restricted controls only appear to apply to organisations, and that individual health providers are 'exempt' from those settings.⁴³

2.41 Applying a record access code would mean that the code would have to be provided every time the MHR was accessed.⁴⁴ Similarly, the document access code would need to be provided each time the document was accessed.⁴⁵

Security and vulnerable groups

2.42 For some groups there are serious security concerns that do not appear to be able to be addressed by the current privacy settings. These apply especially to young people and women and children who have experienced family violence.

Young people aged 14–17 years

2.43 Until a person is 18 years old, a person with parental responsibility can be an Authorised Representative.⁴⁶ The Authorised Representative is empowered under the *My Health Records Act 2012* to do anything that the healthcare recipient would be able to do.⁴⁷ This includes seeing all of the young person's clinical information except from their Medicare Benefits Schedule (MBS) and Pharmaceutical Benefits Scheme (PBS) data.⁴⁸ A person ceases to have an authorised representative when they turn 18 or they satisfy the System Operator that they want to manage their own MHR and can demonstrate that they are able to do so. Under ADHA policy, this requires the young person to obtain a letter from a health professional or a court.⁴⁹

42 Mr Kelsey, *Committee Hansard*, 17 September 2018, pp. 35–36.

43 Health Workers Union, *Submission 96*, p. 13.

44 Mr Kelsey, *Committee Hansard*, 17 September 2018, p. 36. The My Health Records Rule 2016, r. 45 provides that a healthcare provider organisation may not retain a copy of the record code or access code for future use.

45 My Health Records Rule 2016, r. 45.

46 *My Health Records Act 2012*, s. 6; ADHA, *Submission 31*, p. 28.

47 *My Health Records Act 2012*, s. 6(7).

48 *Submission 31*, p. 28.

49 *Submission 31*, p. 28.

2.44 Some submitters expressed concern that these settings may restrict the ability of young people aged 14 to 17 to confidentially access healthcare.

2.45 Dr Robert Walker, a general practitioner from the Lindisfarne Clinic who runs a clinic at a high school in Tasmania, told the committee that he no longer believed that he could guarantee the absolute confidentiality of clinical work.⁵⁰ In his submission, Dr Walker explained that many students are unaware they may have a MHR or that their parents may be able to see parts of their record, such as pathology tests or pharmacy dispensing records, unless they had taken control of their own record.⁵¹

2.46 Dr Walker noted that while most parents are supportive, disclosure of certain information could be detrimental to the student if the parent is not supportive:

Most parents are supportive but not always. There are risks of poor outcomes if confidential data appears on a teenager's MyHR for others to view. Students will be frightened and may not seek help in times of crisis. Imagine the risks they face when their sexuality or their mental health issues are exposed to unforgiving parents or religious orders! Some may be injured or become homeless and self-harm is a constant concern.⁵²

2.47 One 17 year old told the committee that they were unaware that a record had been created for them and that their parents were able to see the information that was added to it:

I live away from home because my mother and I don't get along. I didn't know I needed to take control of My Health Record to stop her from seeing and controlling all of my personal information in My Health Record and talking to my doctor.⁵³

2.48 A number of submitters and witnesses noted that there may be legitimate reasons to seek medical advice, such as obtaining mental health or sexual health information that a young person may prefer their parent did not know about.⁵⁴

2.49 To ensure that young people in this age group are aware of the MHR and what it means for them, a number of submitters recommended that the ADHA specifically tailor communications to target this demographic.⁵⁵

50 Dr Robert Walker, *Submission 55*, [p. 1].

51 *Submission 55*, [pp. 1, 2].

52 *Submission 55*, [p. 2].

53 Consumers of Mental Health WA, *Submission 64*, p. 4.

54 Women's Legal Service Queensland, *Submission 19*, p. 5; Maurice Blackburn Lawyers, *Submission 25*, p 5.

55 Royal Australian and New Zealand College of Psychiatrists (RANZCP), *Submission 30*, p. 5; Pharmaceutical Society of Australia Ltd, *Submission 46*, p. 7; Australian Association of Social Workers, *Submission 49*, p. 4; Orygen, The National Centre of Excellence in Youth Mental Health (Orygen), *Submission 63*, p. 3; Consumers of Mental Health WA, *Submission 64*, p. 4; Aboriginal Health Council of Western Australia, *Submission 91*, p. 5.

2.50 The ADHA advised the committee that specific material has been developed to communicate information about MHR to young people and their parents which had been reviewed by young people in coordination with Orygen Youth Health.⁵⁶ The ADHA also noted that it had engaged heavily with social media, reaching 127 million social media accounts with over 127 000 pieces of content in accordance with feedback received during the 2016 participation trials.⁵⁷

2.51 Orygen, The National Centre of Excellence in Youth Mental Health (Orygen) explained that, as an organisation, it facilitated feedback on two draft information sheets but that some of its other concerns have not been addressed to its satisfaction.⁵⁸ In particular, Orygen was not satisfied that timely and age-appropriate information has been provided about opting out during the opt-out period.⁵⁹

2.52 The Australian Privacy Commissioner, Ms Angelene Falk, advised the committee that she has asked the ADHA and the Department of Health (DOH) to conduct additional consultation with a view to striking the right balance between utility of the record and the privacy of people in the affected age group:

There have also been issues raised regarding the access by parents to younger people's My Health Record parents after age 14 and concerns relating to individuals at risk from family violence. I've asked the agency and the department to give further consideration to these issues during the opt-out period and to consult with affected stakeholders as to whether these settings continue to strike the right balance between the utility of the record and the protection of privacy. Strategies to address issues affecting vulnerable people may include further education and engagement. Consideration may also be given to whether further adjustments are required to these default settings.⁶⁰

Women and children in family violence situations

2.53 Submitters raised serious concerns that the system may be vulnerable to unauthorised access, including by individuals who might have parental responsibility for a child and may have been perpetrators of family violence.⁶¹

2.54 The Law Council of Australia (LCA) explained that it may be possible for a person's former partner to become an Authorised Representative on a child's MHR because the broad definition of parental responsibility in family law legislation includes:

56 ADHA, *Submission 31*, p. 28.

57 *Submission 31*, p. 12.

58 Orygen, *Submission 63*, p. 2.

59 *Submission 63*, pp. 2–4.

60 Ms Angelene Falk, Australian Information Commissioner and Privacy Commissioner, Office of the Australian Information and Privacy Commissioner, *Committee Hansard*, 17 September 2018, p. 33.

61 Mr Morry Bailes, President, LCA, *Committee Hansard*, 17 September 2018, p. 27; Maurice Blackburn Lawyers, *Submission 25*, p. 6.

...a person who merely has an order that a child spend time with that person. Frequently, a parent may retain parental responsibility for a child whilst simultaneously being subject to an interim or final parenting order made under the Family Law Act 1975 or the law of a state or territory.⁶²

2.55 As noted above, an Authorised Representative can see all of the clinical information except for MBS and PBS data.

2.56 In particular, submitters were concerned that an individual may use the right of access they may have as the parent of a child to obtain access to data that may disclose or narrow down the possible residential address of their former partner and child.⁶³

2.57 Submitters noted that potentially identifying information may range from the name of a pharmacy or doctor that the child attended to letters from specialists or other document that are uploaded to the MHR may include the actual residential address of the former partner and child.⁶⁴

2.58 One submitter who had left a violent partner explained to the committee that her child's MHR may disclose their location. The submitter noted that the shared health summary includes an address field and that the activity log reveals that the name of the only medical centre in suburb and the name of the doctor that opened the record.⁶⁵ The submitter's experiences of the navigating the system are set out in the case study below.

62 Mr Bailes, *Committee Hansard*, 17 September 2018, p. 27.

63 National Council of Single Mothers and their Children, *Submission 13*, [p. 1]; Information and Privacy Commission NSW, *Submission 43*, p. 3; Womens Legal Service NSW, *Submission 48*, p. 2; Consumers of Mental Health Western Australia, *Submission 64*, p. 6; Australian Psychological Society, *Submission 73*, p. 3; AMA, *Submission 79*, p. 15; Rape and Domestic Violence Services Australia, *Submission 94*, [p. 1].

64 Western Queensland PHN, *Submission 35*, p. 2.

65 Name withheld, *Submission 62*, [p. 2].

Case Study—Escaping family violence

I am a separated parent, who has escaped family violence. As far as I am aware, my ex-partner does not know where I currently live. However, that may now have been compromised by the establishment of a My Health Record for my son, because under the current legislation, my ex-partner will be permitted to access all information in my son's record, including documents that reveal our location – even if I try to remove them from the system...

I was shocked to learn that my son's My Health Record includes information that identifies our location. Specifically:

- The activity log reveals which medical centre established the record. There is only one medical centre in our small suburb. It is across the road from my son's school, just a few blocks from our house. This effectively gives away our location.
- A shared health summary names the practitioner who authored it (and whom google reveals is working in that same medical centre). This information remained even when I tried to permanently remove that shared health summary from the record.
- The same shared health summary included a form field detailing our home address. Fortunately for me, it was an outdated address. However, it does raise the question of why an address has been included at all.

Currently, the only way to restrict his access to the record is to get an order for sole parental responsibility. However, this process could take months or even years, and going to court is not guaranteed to result in such an order...

Without an order naming the child, the maximum period the digital health agency can suspend my son's record is one month. This is patently inadequate time to secure an order for sole parental responsibility, or to add a child to a family violence order should the defendant choose to challenge it. So, this offers very little protection to victims of Family Violence. Furthermore, even though I have been told that my son's record is currently suspended, I am still able to access it.⁶⁶

2.59 Submitters with experience of domestic violence noted that many perpetrators of domestic violence are controlling and may have access to all of their partner's passwords and constantly monitor where they go and what information they access.⁶⁷

2.60 Women's Legal Service Queensland told the committee that these tendencies meant that the system could inadvertently place women and their children in danger:

We believe the "opt-out" requirement is particularly dangerous if victims are unaware they have active My Health Records, the types of information

66 Name withheld, *Submission 62*, pp. 1–2.

67 Women's Legal Service Queensland, *Submission 19*, p. 2; Women's Legal Service NSW, *Submission 48*, p. 2; Women's Legal Service NSW, *Submission 48*, p. 2; Gold Coast Domestic Violence Integrated Response, *Submission 93*, p. 14.

contained on these records, and the potential for perpetrators to access this information. It is not uncommon for highly dangerous perpetrators to constantly monitor women's lives including who she communicates with, where she goes and her access to information. Perpetrators often have access to (and in fact demand) access to all such accounts including her passwords, controlling every aspect of her life. The media and controversy around the roll out has not only alerted victims to potential safety concerns but will also inadvertently alert perpetrators to a new possible way to enhance control over their victims and children.⁶⁸

2.61 They noted that some of the information in a MHR could potentially be used to escalate physical or verbal abuse toward the victim.⁶⁹

2.62 To ensure that all members of the community remain safe, many submitters called for a greater level of education to be provided to the community.⁷⁰

2.63 The LCA suggested that one way to fix the problem might be to amend the definition of 'parental responsibility' in the *My Health Records Act 2012* to read that 'the child is to spend unsupervised time with the person'.⁷¹ According to the LCA, this amendment would have the effect that a person who was subject to a restraining order or personal protection order that prevented them from spending time with the child would not be considered to have 'parental responsibility'.⁷²

2.64 The DOH considered that the concern had been addressed by the privacy settings that are already in the MHR system:

That's why there are all sorts of mechanisms for people to go in and change the access environment in their records. But we are very interested in what the Law Council and others have to say and we are always interested in hearing these things and we are continually reviewing those settings and so on.⁷³

2.65 The ADHA also explained that it had processes in place to suspend the account of a child if there were concerns about family violence:

Practically speaking, the agency has operational processes in place to respond to those situations so that a consumer—potentially a mother fleeing a violent situation—could contact us and raise concern about safety for herself or the child. The ex-partner would not be able to see the mother's

68 Women's Legal Service Queensland, *Submission 19*, p. 2.

69 Women's Legal Service Queensland, *Submission 19*, p. 2; Women's Legal Service NSW, *Submission 48*, p. 2; Gold Coast Domestic Violence Integrated Response, *Submission 93*, p. 14; Rape and Domestic Violence Services Australia, *Submission 94*, [p. 1].

70 Consumers Health Forum of Australia (CHF), *Submission 16*, p. 19; RANZCP, *Submission 30*, p. 5; AMA, *Submission 79*, p. 15.

71 Mr Bailes, *Committee Hansard*, 17 September 2018, p. 27.

72 Mr Bailes, *Committee Hansard*, 17 September 2018, p. 27.

73 Ms Caroline Edwards, Deputy Secretary, Department of Health (DOH), *Committee Hansard*, 20 September 2018, p. 3.

record but could see the child's. We would immediately suspend that record in terms of stopping the authorised representatives from accessing it. We do that immediately and then we undertake an investigation to ensure that any sort of access is not putting the child at risk and those records can remain suspended while there's any risk of that occurring.⁷⁴

2.66 However, as the above case study demonstrates, those restrictions appear to apply for a period of 30 days, which may not be enough time to find a more permanent solution.

Committee view

2.67 The committee is concerned by the possibility that the MHR system may jeopardise the ability of young people and women to confidentially seek medical advice without posing further risks to their physical or emotional wellbeing.

2.68 The committee notes that young people aged between 14 and 17 years may have legitimate reasons to seek medical advice and may prefer that their parents did not know about it.

2.69 The committee notes that the Australian Information Commissioner and Privacy Commissioner and others have called on the ADHA to revise its strategy for engaging with young people and how the default settings are currently configured.

2.70 The committee is deeply concerned about the prospect that perpetrators of domestic violence may be able to legitimately gain access to the records of their children and potentially exploit that access to the potential detriment of their former partner and their children. The committee is not satisfied that women and children are adequately protected and believes that further work is required to ensure that MHR is not used by perpetrators to gain access to records. The committee notes the recommendation of the LCA as one way this issue may be addressed. The committee understands that the ADHA is conducting work to improve its response in this area. The committee urges them to continue with that work and to engage more fully with providers of domestic violence services.

Who else could find out what is in MHR?

Employer nominated doctors

2.71 Some submitters raised concerns that an employer nominated health practitioner could obtain access to the healthcare recipient's MHR and potentially disclose information that the healthcare recipient would prefer was kept confidential in the context of a pre-employment medical or workers compensation claim.⁷⁵

74 Ms Bettina McMahon, Chief Operating Officer, ADHA, *Committee Hansard*, 20 September 2018, p. 4.

75 Mr Christopher Watts, Social Policy Advisor, Australian Council of Trade Unions (ACTU), *Committee Hansard*, 17 September 2018, p. 17; Mr Trevor Gauld, Electrical Trades Union of Australia, *Committee Hansard*, 17 September 2018, p. 17.

2.72 While this might seem like a remote possibility, Ms Leigh Svendsen from the Health Services Union advised the committee that the union was aware of cases where health information has been passed on to an employer by a health practitioner.⁷⁶

2.73 The concern raised by unions and others was that the way the My Health Records Act is drafted may make it entirely permissible for that information to be passed to an employer.

2.74 The unions' concern is that access to information in the MHR is dependent upon the provision of 'health care' which is broadly defined in the Privacy Act 1988 to include 'assessing, maintaining, improving or managing the individual's health'.⁷⁷ Mr Christopher Watts from the Australian Council of Trade Unions noted that it was his interpretation that such a broad definition could include examinations of the individual for medical relating to a person's employment.⁷⁸

2.75 The DOH advised the committee that the information could not be used in that way because subsection 14(2) of the *Healthcare Identifiers Act 2010* prohibits a healthcare provider from disclosing a healthcare identifier as part of employing the healthcare recipient or examining the healthcare recipient in connection with a contract of insurance.⁷⁹

2.76 The joint submission from the DOH and the Department of Human Services (DHS) stated that it was not possible to access a MHR without collecting, using or disclosing a healthcare identifier.⁸⁰

2.77 However, some witnesses disagreed with the departments' assessment. Mr Thomas Ballantyne, a principal at Maurice Blackburn Lawyers told the committee that if the MHR could be accessed using the individual's Department of Veterans' Affairs file number or their Medicare number, then the restriction in the Healthcare Identifiers Act did not apply:

I think the key thing is effectively whether you need to use the healthcare identifier to access the My Health Record of a particular patient. I went again on the digital health portal—the training for providers—this morning, and it's clear that you can access a patient's My Health Record with their healthcare identifier or a Medicare number or a DVA number.

I think that, on plain reading of section 14 of the Healthcare Identifiers Act, it has to be the most likely outcome that, unless you use that particular number, the offence doesn't apply—the exclusion doesn't apply.⁸¹

76 Ms Leigh Svendsen, Senior National Industrial Officer, Health Services Union, *Committee Hansard*, 17 September 2018, p. 19.

77 Mr Gauld, *Committee Hansard*, 17 September 2018, p. 18.

78 Mr Watts, *Committee Hansard*, 17 September 2018, p. 18.

79 DOH and DHS, *Submission 22*, p. 17.

80 DOH and DHS, *Submission 22*, p. 17.

81 Mr Thomas Ballantyne, Head of the Victorian Medical Law Practice, Maurice Blackburn Lawyers, *Committee Hansard*, 17 September 2018, p. 29.

2.78 Other submitters, such as the Public Health Association of Australia and Unions NSW noted that employers may ask employees to consent to the release of information in their MHR.⁸² Under section 66 of the My Health Records Act, a participant may disclose for any purpose health information included in the MHR with consent of the healthcare recipient.

2.79 DOH and the ADHA have made clear that it was certainly not intended that the legislation would facilitate access to information contained in a MHR for any purpose other than the provision of health care to the recipient.⁸³

2.80 A number of submitters, including Maurice Blackburn Lawyers, have recommended that a provision similar to section 14(2) of the Healthcare Identifiers Act 2010 be added to the My Health Records Act to clarify the position.⁸⁴

Law enforcement

2.81 Some submitters raised concerns about whether information in a MHR could be used for law enforcement purposes.

2.82 Section 70 of the My Health Records Act currently provides that information may be disclosed for the purposes of law enforcement or the protection of revenue.

2.83 Whilst the committee was conducting this inquiry, the Community Affairs Legislation Committee (Legislation Committee) was conducting an inquiry into the My Health Records Amendment (Strengthening Privacy) Bill 2018 (Bill).

2.84 That Bill will, if passed, remove section 70 from the My Health Records Act and replace it with a requirement that a 'designated entity' may apply to a judicial officer for a warrant to obtain information in a MHR from the System Operator, other than 'healthcare recipient-only notes'.⁸⁵

2.85 Submitters to this inquiry endorsed the measures in the Bill directed at strengthening privacy provisions.⁸⁶

Committee view

2.86 The committee considers that the MHR system should only be used to provide access to information for the purpose of providing healthcare to the healthcare recipient. The committee considers that where there is doubt about whether information contained within the system may be used for that purpose, the legislation should be clarified to ensure that the integrity of the system is maintained.

82 Unions NSW, *Submission 80*, p. 4; Public Health Association of Australia, *Submission 97*, p. 7.

83 Mr Kelsey, *Committee Hansard*, 17 September 2018, p. 42; Ms Edwards, *Committee Hansard*, 17 September 2018, p. 42.

84 ACTU, *Submission 17*, p. 7; Victorian Trades Hall Council, *Submission 20*, [p. 2]; Maurice Blackburn Lawyers, *Submission 25*, p. 8; Unions NSW, *Submission 80*, p. 6.

85 My Health Records Amendment (Strengthening Privacy) Bill 2018, sch. 1, item 12.

86 See for example CHF, *Submission 16*, p. 17; Women's Legal Service Queensland, *Submission 19*, p. 6; QNMU, *Submission 41*, p. 7.

2.87 The committee notes the recommendation proposed by the unions and Maurice Blackburn Lawyers that to avoid doubt, a provision similar to section 14(2) of the *Healthcare Identifiers Act 2010* should be inserted into the My Health Records Act.

How else could information in the MHR system be used?

Secondary use

2.88 In addition to the provision of healthcare, MHR has the potential to provide information that could be used in public health research. This is known as secondary use.

2.89 Submitters broadly acknowledged that MHR data has the potential to have significant public health research benefits, including improving insights into population health issues and how people use the health system.⁸⁷

2.90 The default setting is that all people consent to the use of their information for secondary use. However, they may withdraw this consent by selecting the 'Withdraw Participation' button in their MHR.⁸⁸

2.91 Some submitters noted that this default setting was originally conceived of in the context of an opt-in model. On that basis, it was reasonable to assume that people who provided information made an informed choice when they consented to their information being placed in the MHR system and that it may include the secondary use of that data.

2.92 That informed consent is not necessarily true in an opt-out model. Some submitters considered that healthcare recipients should be asked to provide explicit consent to the secondary use of their data.⁸⁹

2.93 The LCA explained that the secondary use of data was at odds with privacy laws because the healthcare recipient had not provided consent for their data to be used in that way. Therefore, the LCA recommended that explicit consent should be obtained:

The secondary use of their data is at odds with the underlying principles in both Commonwealth and state privacy laws. These principles provide that a health entity that holds information about a patient can only use or disclose the information for the particular purpose for which it was collected, unless

87 Dr Linc Thurecht, Senior Research Director, Australian Healthcare and Hospitals Association, *Committee Hansard*, 11 September 2018, p. 8; Future Wise, *Submission 15*, p. 8; Federation of Ethnic Communities Councils of Australia, *Submission 45*, p. 3; National Rural Health Alliance, *Submission 66*, [p. 6]; Australian Genomics, *Submission 70*, p. 5; Medicines Australia, *Submission 81*, p. 1; Australian Healthcare and Hospitals Association, *Submission 86*, p. 6.

88 ADHA, *Submission 31*, p. 33.

89 Name withheld, *Submission 9*, [p. 2]; Dr Chris Culnane, A/Prof Benjamin Rubinstein and Dr Vanessa Teague (Culnane, Rubinstein and Teague), *Submission 59*, p. 1; Australian Genomics, *Submission 70*, p. 6.

the patient has explicitly consented to secondary use or disclosure. The Law Council therefore recommends the patient must provide explicit consent if their health information is obtained for a secondary purpose or disclosure.⁹⁰

2.94 Whilst it is not currently possible, the *Framework to guide the secondary use of My Health Record system data* (Secondary Use Framework) notes that in time a dynamic consent model will be explored to allow consumers to decide whether to participate in a research project on a case-by-case basis.⁹¹

2.95 Whether healthcare recipients would be prepared to provide consent may depend on the nature of the research projects under consideration.

2.96 Consumers Health Forum of Australia told the committee that its research has found that consumers are more likely to give permission to projects if they understand how their data is going to be used and what benefits might flow from its use:

we believe there is a place for secondary use of de-identified—that's a key word—My Health Record data. On the whole, so do consumers. Our research shows that Australians want ownership and control of their own health data and want to give consent when it is used by governments, private companies and researchers. The same research also found that consumers are more likely to give permission if they understand how their data will be used and the benefits that will come from its use. There is a level of comfort among the majority of consumers in data being used to support health providers to improve care or make better policy. But consumers are significantly less willing to share their data if it's to be used for commercial gain.⁹²

2.97 To ensure social license for the use of secondary data there is a need to make sure that the data is used in a manner that the community would feel comfortable with.⁹³

2.98 To ensure that secondary data is used appropriately, the DOH has developed the Secondary Use Framework which sets out the guiding principles for the use of secondary data from the MHR system. The principles detail the governance model, consumer control of data, applications and access to secondary data, the process for requesting and accessing data, linkage privacy protection, making data available, assurance processes and risk mitigation.⁹⁴

90 Mr Bailes, *Committee Hansard*, 17 September 2018, p. 27. See also Positive Life NSW (PLNSW) and National Association of People with HIV Australia (NAPWHA), *Submission 44*, p. 6.

91 Department of Health, *Framework to guide the secondary use of My Health Record system data* (Secondary Use Framework), May 2018, p. 19.

92 Ms Leanne Wells, Chief Executive Officer, CHF, *Committee Hansard*, 17 September 2018, p. 7.

93 Australian Genomics, *Submission 70*, p. 5.

94 Secondary Use Framework, pp. 4–6.

2.99 The Secondary Use Framework was developed after public consultation and was supported by submitters to the inquiry.⁹⁵ In particular, submitters were supportive of the principles that prohibited insurance agencies from applying for data and that prohibited the release of data for 'solely commercial purposes'.⁹⁶

2.100 DOH and DHS advised the committee that two examples that would be prohibited were access to data for direct marketing to consumers or for the assessment of insurance premiums or claims.⁹⁷

2.101 Some submitters raised concerns that secondary data, if it was released, may be re-identified.⁹⁸

2.102 Whilst the DOH understood the concern, it noted that the linkage and data custodian arrangements administered by the Australian Institute of Health and Welfare are stringent and different from a previous case where Medicare data was re-identified by some Melbourne based researchers.

2.103 The researchers who conducted the re-identification, Dr Chris Culnane, Associate Professor Benjamin Rubinstein and Dr Vanessa Teague told the committee that, while they welcomed the approach to not publish MHR data as open data, they did not consider that would be sufficient to prevent re-identification of datasets.⁹⁹

2.104 These researchers told the committee that they believed that the technical difficulty of finding patients was low and that 'the presence of the identifiable MBS-PBS data for 10% of the population is now a resource that an attacker could leverage in My Health Record identification'.¹⁰⁰

2.105 The Privacy Commissioner told the committee that valuable lessons had been learned from the previous experience and that the Secondary Use Framework has been drafted to take account of those lessons:

Only to note that that matter was the subject of an investigation by my office, and we did find that there was a breach of the Privacy Act. What it brings to light, of course, is that with de-identified information there needs to be very strict safeguards around that information. In that case, it was

95 Ms Tania Rishniw, First Assistant Secretary, Portfolio Strategies Division, DOH, answers to questions on notice, 17 September 2018 (received 20 September 2018); Australian Genomics, *Submission 70*, p. 5; RACGP, *Submission 74*, p. 5.

96 Secondary Use Framework, pp. 23, 27. Under principle 3.3 any Australian entity other than an insurance agency may apply to access secondary use data. Under principle 4.2 the Board will use a 'case and precedent' approach when determining what is 'solely commercial use' of data.

97 DOH and DHS, *Submission 22*, p. 18.

98 Name withheld, *Submission 9*, [p. 3]; Future Wise, *Submission 15*, p. 9; Rural Doctors Association of Australia, *Submission 28*, p. 3; Royal Australian and New Zealand College of Radiologists, *Submission 47*, [p. 6]; Australian Medical Association (NSW) (AMA(NSW)), *Submission 68*, [p. 5]; Joshua Badge, *Submission 113*, p. 8.

99 Culnane, Rubinstein and Teague, *Submission 59*, p. 1.

100 Culnane, Rubinstein and Teague, *Submission 59*, p. 2.

around making information publicly available. That's not what is envisaged by the secondary use framework as I understand it.¹⁰¹

Third party access

2.106 Some submitters were concerned at the prospect that MHR data could be made available, either now or in the future, to insurers or other commercial parties.¹⁰²

2.107 These submitters raised concerns that while the Secondary Use Framework currently prohibited access by third parties, the Secondary Use Framework would only be in place in the short term, noting that health insurer access may be prioritised in the first review.¹⁰³

2.108 Some submitters considered that a legislative amendment may be required to ensure that insurers would not be able to access the data and to ensure that their data is permanently protected from such interests.¹⁰⁴

Committee view

2.109 The committee considers that there is great potential for data in the MHR system to be used for population health research purposes, however, the committee also recognises concerns that personal data be used for commercial purposes.

2.110 The committee notes that the current Secondary Use Framework does not permit secondary data to be used for 'solely commercial purposes'. The committee considers that this prohibition is appropriate but notes that there is public interest in a more permanent solution being found to ensure that a healthcare recipient's MHR data is only used for the purposes for which it was originally intended.

101 Ms Falk, *Committee Hansard*, 17 September 2018, p. 50.

102 Future Wise, *Submission 15*, p. 13; CHF, *Submission 16*, p. 18; RANZCP, *Submission 30*, p. 5; Western Queensland PHN, *Submission 35*, p. 3; QNMU, *Submission 41*, p. 6; Pharmaceutical Society of Australia, *Submission 46*, p. 7; Dr David G More, *Submission 54*, p. 3; National Rural Health Alliance, *Submission 66*, [p. 7]; AMA (NSW), *Submission 68*, [pp. 6–7]; Australian Genomics, *Submission 70*, p. 9; Australian Healthcare and Hospitals Association, *Submission 86*, p. 10; Breast Cancer Network Australia, *Submission 110*, [p. 9]; Joshua Badge, *Submission 113*, p. 9.

103 AMA, *Submission 79*, p. 16.

104 Dr Pinski, *Committee Hansard*, 11 September 2018, p. 42; Name withheld, *Submission 9*, [p. 3]; Doctors Reform Society, *Submission 29*, [p. 3]; PLNSW and NAPWHA, *Submission 44*, p. 8; National Rural Health Alliance, *Submission 66*, [p. 7]; RACGP, *Submission 74*, p. 5; AMA, *Submission 79*, p. 17.

Chapter 3

Using My Health Record

3.1 Throughout the inquiry, submitters and witnesses provided evidence which emphasised that My Health Records need to be usable for both healthcare recipients and healthcare providers if the My Health Record (MHR) system is to operate effectively.

3.2 A MHR will be created for every Australian by the end of 2018 unless they chose to opt-out.¹ Following a 'trigger' event, a healthcare recipient's MHR will commence being populated with health information. Unless a healthcare recipient has requested otherwise, the MHR system's default access controls will be applied to their MHR. These controls, in part, enable healthcare providers to access MHR information for the purpose of providing healthcare.

3.3 This chapter considers the population of healthcare recipients' MHRs with health information following a trigger event, and the default access settings that will be applied to those MHRs when created by the System Operator. The chapter considers healthcare providers' use of MHRs, and, in particular, the balance which exists between MHR information being usable in clinical settings and the privacy controls afforded to healthcare recipients.

Populating a MHR

3.4 When a registered healthcare recipient's MHR is created it will be empty.² A MHR will start to be populated with certain health information when a healthcare recipient first interacts with the health system, or when they first log on to the MHR system to access their record.³ The Royal Australian College of General Practitioners (RACGP) described this activation of healthcare recipients empty MHRs as 'trigger events'.⁴ Following a trigger event, two years' worth of a healthcare recipient's Medicare Benefits Schedule (MBS) and Pharmaceutical Benefits Scheme (PBS) data will be uploaded to their MHR, unless the recipient has applied a control that prevent this from occurring.⁵

3.5 The Australian Digital Health Agency (ADHA) outlined some of the health information which will be uploaded following a trigger event:

...certain types of documents then start flowing into the record – medicine prescription and dispense records, hospital discharge summaries, pathology test results and diagnostic imaging reports, specialist letters, event

1 Australian Digital Health Agency (ADHA), *Submission 31*, pp. 1, 5.

2 ADHA, *Submission 31*, p. 27.

3 ADHA, *Submission 31*, p. 27.

4 Royal Australian College of General Practitioners (RACGP), *Submission 74*, p. 3.

5 ADHA, *Submission 31*, p. 27; Australian Manufacturing Workers' Union, *Submission 105*, [p. 2].

summaries and a curated shared health summary by a consumer's GP. Medicare data such as the Australian Immunisation Register, Organ Donor Register and MBS/PBS data also go into the record.⁶

3.6 Some submitters raised concerns that many healthcare recipients are not aware of what the MHR system's trigger events for populating a MHR are.⁷ Some submitters considered that healthcare recipients should have more notice before this data is uploaded. It was argued that more should be done to alert healthcare recipients to this.⁸ For example, Dr Nathan Pinskiier, Chair, Expert Committee – eHealth and Practice Systems, RACGP suggested that:

The consumer may not always be aware of that, so we believe that the system should be strengthened so that the consumer is made aware that when the trigger event occurs it's actually occurring: 'I see you have a shell record. I see that nothing's been uploaded to it yet. Sending up a shared health summary, an event summary, a pathology request—whatever—will create the trigger event.' A positive consent flag should then get entered into the system, and the consumer should be advised that they should log on to their My Health Record through MyGov and the consumer portal and consider whether they want to strengthen their controls.⁹

3.7 The Health Workers Union expressed concern that, following a trigger event, PBS and MBS data may be uploaded for people who may not have voluntarily registered for a MHR, or for people who do not have a level of digital literacy that would allow them to access their MHR to amend their default access controls to prevent the upload.¹⁰

3.8 The committee notes evidence from the ADHA that healthcare recipients' past health information, such as older tests and medical reports, will not be available in new MHRs.¹¹

Default access controls

3.9 The MHR system's consumer privacy controls are mandated by the My Health Record Rule 2016, which, in part, specifies the default access controls applicable to MHRs when created by the System Operator.¹² The default access controls which must be enabled by the System Operator are as follows:

6 ADHA, *Submission 31*, p. 27.

7 Dr Nathan Pinskiier, Chair, Expert Committee – eHealth and Practice Systems, RACGP, *Committee Hansard*, 11 September 2018, p. 42; RACGP, *Submission 74*, p. 3.

8 Dr Pinskiier, *Committee Hansard*, 11 September 2018, p. 42.

9 Dr Pinskiier, *Committee Hansard*, 11 September 2018, p. 42.

10 Health Workers Union, *Submission 96*, p. 16.

11 ADHA, *Submission 31*, p. 31.

12 Department of Health (DOH) and Department of Human Services (DHS), *Submission 22*, p. 10.

-
- (a) permit all registered healthcare provider organisations involved in the care of a registered healthcare recipient to access the healthcare recipient's My Health Record;
 - (b) include an access list of the registered healthcare provider organisations that are permitted to access the healthcare recipient's My Health Record because the organisation is involved in the care of the registered healthcare recipient;
 - (c) permit registered healthcare recipients to view the access list for their My Health Record;
 - (d) remove a healthcare provider organisation from the access list for a healthcare recipient's My Health Record if the organisation has not accessed the healthcare recipient's My Health Record for a period of three years;
 - (e) permit registered healthcare recipients to:
 - (i) effectively remove records from their My Health Record; and
 - (ii) authorise the System Operator to restore records which have previously been effectively removed; and
 - (f) permit registered healthcare provider organisations that uploaded records to a healthcare recipient's My Health Record to access those records, but only by request to the System Operator, if the healthcare provider organisation is no longer on the access list for the healthcare recipient's My Health Record.¹³

3.10 RACGP observed that the default access controls of a MHR '...effectively allow any healthcare provider with access to My Health Record to view, upload and download from a consumer's My Health Record for the purposes of providing healthcare.'¹⁴ RACGP recommended that consumers be prompted to review their access controls on activation of their MHR.¹⁵

3.11 Submitters expressed concern that the level of access to MHR information enabled by the default access controls was too extensive. For example, Maurice Blackburn Lawyers submitted that whilst the default access settings allowing all registered MHR healthcare providers to access recipients' MHRs may have been appropriate in an opt-in system, '...the same cannot be said of an out-out system.'¹⁶ The Australian Council of Trade Unions similarly suggested that, given the MHR system had transitioned from an opt-in to an opt-out system, the default access

13 My Health Record Rule 2016, Part 2, Division 1.

14 RACGP, *Submission 74*, p. 3.

15 RACGP, *Submission 74*, p. 3.

16 Maurice Blackburn Lawyers, *Submission 25*, p. 4.

controls should provide greater protection to individuals who may not be aware that a MHR is being created for them.¹⁷

3.12 The NSW Privacy Commissioner urged further consideration be given to the default settings applied to MHRs:

Consideration should be given to altering the default settings to ensure that individual privacy is protected. Access to health information should remain limited until the individual record holder chooses to allow a healthcare provider to have access to their health information.¹⁸

3.13 Considering the impact the MHR system may have on vulnerable groups, the NSW Privacy Commissioner informed the committee that the setting of access controls will be central to managing the risk of inappropriate access to MHR information and, given this, default privacy settings should be set at the highest level.¹⁹ Positive Life NSW (PLNSW) and National Association of People with HIV Australia (NAPWHA) explained sharing sensitive health information with all members of their healthcare teams via the default settings applied to MHRs would particularly effect people living with HIV, or people who inject or use drugs. PLNSW and NAPWHA suggested this could potentially expose people who may not have the capacity to adjust their MHR privacy settings to an unnecessary risk of disclosure.²⁰

3.14 Similarly, the Federation of Ethnic Communities' Councils of Australia recommended:

...default settings for the MHR should be set at maximum security and privacy with a prompt that offers individuals the choice to allow for their health data to be shared with others including caregivers and medical professionals should they wish.²¹

3.15 Several other submitters expressed support for strengthening the default privacy settings applied to healthcare recipients' MHRs.²²

3.16 Some submitters noted that MHRs included other privacy controls which were not enabled by default. For example, the Consumers Health Forum of Australia pointed out that healthcare recipients are able to set an access control so that they are notified when their MHR has been accessed, however this control is not applied by

17 Australian Council of Trade Unions, *Submission 17*, p. 6.

18 NSW Privacy Commissioner, *Submission 43*, pp. 2–3.

19 NSW Privacy Commissioner, *Submission 43*, p. 3.

20 Positive Life NSW and National Association of People with HIV Australia, *Submission 44*, p. 10.

21 Federation of Ethnic Communities' Councils of Australia, *Submission 45*, p 1.

22 Dr Thomas Rechnitzer, *Submission 56*, p. 2; Dr Chris Culnane, A/Prof Benjamin Rubinstein, and Dr Vanessa Teague, *Submission 59*, p. 1; Mr Stephen Ma, *Submission 61*, [p. 3]; Consumers of Mental Health WA, *Submission 64*, pp. 12, 15–16.

default.²³ The ADHA informed the committee that the notification control was active in 136 644 MHRs, as at 2 September 2018.²⁴

3.17 To increase registered healthcare recipients' understanding of the MHR system's default access settings, and broader privacy implications and controls available, submitters and witnesses suggested that improved public information and education is necessary.²⁵ The need for better awareness of the MHR system's privacy implications are considered in further detail in Chapter 4.

Record access code

3.18 In response to the open nature of the MHR system's default access controls, some submitters suggested that the, currently optional, Record Access Code (RAC) control should be applied to healthcare recipients' MHRs by default.²⁶ Healthcare recipients are able to apply a RAC to the MHR to restrict a healthcare provider from accessing their MHR without a code managed by the recipient.²⁷ A 'limited access document control' can also be enabled by healthcare recipients to restrict healthcare providers' access to individual documents within their MHRs.²⁸ Ms Bettina McMahon, Chief Operating Officer, ADHA, informed the committee that, as at 2 September 2018, healthcare recipients had applied 16 848 RACs to their MHRs, and 4109 limited documents access codes.²⁹

3.19 Some submitters suggested that the use of a RAC could provide security benefits. For example, Dr Robert Merkel suggested that by using a RAC a healthcare recipient could reduce the potential for unauthorised access to their MHR:

...you can set a PIN on your My Health Record so that any new healthcare provider who wants to see your My Health Record needs to ask you what your PIN is, but that's not compulsory, and in the opt-out trial of the My Health Record system only a very small percentage of people set a PIN. That means that, if a hacker got access to a doctor's log-in credentials, for instance, they would be able to access the My Health Record of the vast majority of people, because they hadn't set an access code. If instead having an access code was the default rather than the exception, the range of

23 Consumers Health Forum Australia, *Submission 16*, p. 23; Queensland Nurses and Midwives' Union, *Submission 41*, pp. 7–8.

24 Ms Bettina McMahon, Chief Operating Officer, ADHA, *Committee Hansard*, 17 September 2018, p. 36.

25 Primary Health Networks, *Submission 75*, [p. 4]; Pharmaceutical Society of Australia, *Submission 46*, p. 7; Dr Pinski, *Committee Hansard*, 11 September 2018, p. 44.

26 Professor Kerry Phelps, *Committee Hansard*, 11 September 2018, p. 5; Dr Robert Merkel, *Committee Hansard*, 11 September 2018, p. 22; Victorian Trades Hall Council, *Submission 20*, [p. 3].

27 ADHA, *Submission 31*, p. 9.

28 Mr Tim Kelsey, Chief Executive Officer, ADHA, *Committee Hansard*, 17 September 2018, pp. 35–36; Law Council of Australia, *Submission 108*, p. 13.

29 Ms McMahon, *Committee Hansard*, 17 September 2018, p. 36.

people whom that hacker would be able to get access to would be very much reduced.³⁰

3.20 Mr Grahame Grieve, Principal, Health Intersections Pty Ltd, echoed the view that potential unauthorised access to the MHR information through a clinician portal could be negated through the use of a record code by default. However, Mr Grieve noted a potential side effect of this protection could be limitations to the accessibility of MHR information.³¹

3.21 The Australian Medical Association (AMA) expressed similar concerns:

A decision to impose maximum security settings as a default for all new My Health Records created by government under an opt out model, would mean all clinical information uploaded to the patient's My Health Record would remain invisible to the patient's treating healthcare providers unless the patient creates myGov account and opts into their Record to relax these privacy settings. The opt in approach has demonstrably failed in Australia to achieve a critical mass adoption necessary to create a self-sustaining My Health Record System with all the potential clinical benefits it offers.³²

3.22 The AMA suggested that the default application of record access codes to all MHRs would, in effect, cause the system to operate more on an opt-in basis.³³ RACGP suggested that there is a balance which exists between the two MHR system's privacy requirements and system utility.³⁴

Committee view

3.23 The committee recognises that MHRs will contain sensitive and confidential health information. As such, it is the committee's view that the MHR system's default access controls, which significantly impact how healthcare recipients' MHR information is used, require further consideration. The committee notes that following the creation of a MHR record by the System Operator, a trigger event will cause significant health information to be uploaded to the record. The committee also notes registered healthcare recipients may not be aware that they can vary the access controls for their MHRs, or may not have the ability to readily change those controls.

3.24 Many submitters expressed concern that the default access controls applied to healthcare recipients MHRs are too 'open'. Submitters stressed that more restrictive access controls should be applied to MHRs. The committee acknowledges the evidence from some submitters that restricted access controls are important for protecting vulnerable groups. The committee found this evidence particularly

30 Dr Robert Merkel, *Committee Hansard*, 11 September 2018, p. 20.

31 Mr Grahame Grieve, Principal, Health Intersections Pty Ltd, *Committee Hansard*, 17 September 2018, p. 15.

32 Australian Medical Association (AMA), *Submission 79*, p. 12.

33 Dr Chris Moy, Member, AMA Federal Council, Chair, Federal Ethics and Medico-Legal Committee, AMA, *Committee Hansard*, 11 September 2018, p. 39.

34 Dr Pinskiier, *Committee Hansard*, 11 September 2018, pp. 43–44.

compelling, and considers that the call for strengthened default access controls is justified.

Clinical use

3.25 After a healthcare recipient's MHR has been created, healthcare providers are able to commence using those records in the provision of healthcare, subject to the healthcare recipient's MHR access controls.

Access to patients' health information

3.26 MHRs have potentially significant clinical benefits through increasing clinicians' access to patients' health information to improve the quality of health care.³⁵ The AMA summarised some of the clinical benefits in its submission:

Many of the greatest failures in patient care and safety result when patients are required to move across the health system but their clinical information does not follow them.

The My Health Record (Record) has the potential to circumvent these limitations to ensure clinically important patient information is available at the point of care, irrespective of the health care setting and the location of the treating doctor. The result is better connected care, reduced medical harm from avoidable medication complications and allergic reactions.³⁶

3.27 Some submitters noted that an MHR could be a significant advance on the lack of information that practitioners may currently be contending with. Without an electronic health record, the AMA explained that emergency doctors are effectively 'flying blind' when treating the patient in front of them:

In plain terms, that's what they're doing, they're flying blind and they're giving medications... There are 230,000 medication events leading to hospitalisation in Australia every year, many due to lack of information.³⁷

3.28 The AMA also explained that for healthcare recipients who change doctors, it can be very difficult to obtain proper information about that patient.³⁸

3.29 Only 61 per cent of general practitioners, and 79 per cent of pharmacists, who have used the MHR system reported '...one or more actual benefits from use.'³⁹ The most common benefit reported by general practitioners was the ability to view information about a patient which was previously unknown, and 29 per cent of pharmacists reported having avoided a potential adverse medicines event through having access to patients' MHR information.⁴⁰

35 See for example: Medicines Australia, *Submission 81*, p. 2; University of New South Wales, *Submission 80*, p. 3; AMA NSW, *Submission 68*, [p. 2].

36 AMA, *Submission 79*, p. 1.

37 Dr Moy, *Committee Hansard*, 11 September 2018, pp. 31–32.

38 Dr Moy, *Committee Hansard*, 11 September 2018, p. 31.

39 ADHA, *Submission 31*, p. 4.

40 ADHA, *Submission 31*, p. 4.

3.30 The Royal Australian College of Physicians (RACP) highlighted the benefits of the MHR system's review function, which allows '...clinicians to read and review opinions and decisions made by other clinicians on the same patient'.⁴¹ Whilst noting imperfections of the MHR system, RACP suggested the review functionally is an improvement to the current system where there can be complete lack of visibility for clinicians who are not the patient's main consulting clinician. RACP commented:

...the review and information repository functions are one of the key characteristics of MHR that makes it an important building block for better integrated care. Even though interactive functionality of the MHR is currently limited, having this infrastructure in place can be an important first step for adding more sophisticated functionality to the platform later.⁴²

3.31 The benefits of improved access to clinical data through patients' MHRs may also assist patients in better understanding and engaging with their clinical care. As observed by the AMA:

Research indicates 40-80 per cent of medical information provided by healthcare practitioners is forgotten immediately by patients. If patients have access to their clinical data in their My Health Record, they are more likely to understand their health conditions, adhere to treatment advice and engage more actively with their treating clinicians in their ongoing care. This will also assist in increasing overall patient health literacy which will improve long term health outcomes and indeed improve prevention and education activities.⁴³

3.32 The Australian Healthcare and Hospitals Association submitted that MHRs, with active use and updating, have the potential to be very empowering for both clinicians and patients.⁴⁴

Issues

3.33 Submitters to the inquiry raised concerns regarding the utility of the MHR system in clinical settings.

Information comprehensiveness

3.34 A concern frequently raised by submitters was the issue of how comprehensive the information in healthcare recipients' MHRs will be, and the potential consequences of incomplete information in clinical settings. MHRs are designed to be personally controlled by healthcare recipients. This means that they can effectively hide or remove clinical records from their MHR. Submitters noted that the personally controlled nature of the record contains an inherent limitation, in that a

41 Royal Australian College of Physicians (RACP), *Submission 106*, p. 3.

42 RACP, *Submission 106*, p. 3.

43 *Submission 79*, p. 2.

44 Australian Healthcare and Hospitals Association, *Submission 86*, p. 5.

MHR can only be considered a component or summary of a person's broader health information.⁴⁵

3.35 The RACP submitted that the usefulness of the MHR system will ultimately depend on the quality and comprehensiveness of the information uploaded. RACP explained the elements of information comprehensiveness and the risks to patient safety that could arise from the potential incompleteness of patient records:

There are two dimensions to comprehensiveness. There is firstly the extent of coverage of the MHR (of both patients and clinicians). Secondly there is the question of the completeness of the patient record. However, there will realistically be limits on this comprehensiveness because some people may choose to opt-out. In addition, under current provisions, people are also able to limit which healthcare provider organisations can access their MHR or restrict access to selected part of their record. These choices must be respected as a matter of patient autonomy. However, the possible incompleteness of the patient record introduces some risks to patient safety if clinicians treat it as a complete record and use it as a substitute for having an appropriate conversation with the patient or pursuing further investigations as required.⁴⁶

3.36 Some submitters expressed concern that the MHR system's privacy controls available to registered healthcare recipients could adversely impact the completeness of their MHR. For example, the Australian Psychological Society (APS) submitted:

The reliability of health information held in MHR is further reduced by inconsistent approaches to uploading health information by providers and the ability for consumers to remove or restrict access to important information. There is currently no requirement for health providers to upload all clinical information to the MHR. Thus, a person's MHR may omit significant amounts of relevant information. This means that even in an emergency, treating practitioners cannot rely on the information contained in a MHR when making clinical decisions.⁴⁷

3.37 The AMA NSW, whilst acknowledging that patients have the fundamental right to determine what health information is included in their MHR and who can access it, suggested that a patient-controlled electronic system may lead to omissions of information which may undermine the usefulness of MHRs.⁴⁸ The University of Melbourne echoed this view, noting that whilst the privacy rationale for general practitioners' uploading of health information to MHRs only with patients' explicit consent is clear, incomplete information in MHRs is an inhibitor to the clinical utility of those records.⁴⁹

45 MIGA, *Submission 65*, p. 2.

46 RACP, *Submission 106*, pp. 3–4.

47 Australian Psychological Society (APS), *Submission 73*, p. 1.

48 AMA NSW, *Submission 68*, p. 3.

49 University of Melbourne, *Submission 82*, p. 2.

3.38 A number of other submitters noted that if an MHR is incomplete or out of date, the record's utility as a clinical tool is reduced.⁵⁰ Mr Paul Shetler, the former head of the Digital Transformation Office, questioned whether MHRs were being regularly updated. Based on a briefing he received in 2015, Mr Shetler told the committee that only a minority of healthcare recipients actually updated their records:

Of the 10 per cent of the Australians who had My Health Record, 10 per cent of them were having their health records updated with any kind of regularity. That was one per cent of the population⁵¹

Interface issues

3.39 To access the MHR system through a clinical information system (CIS), health providers need to:

- be using conformant software which has a secure and encrypted connection to the My Health Record system;
- be authorised to access the system by the healthcare provider organisation; and
- be providing healthcare to a patient of the practice who has had a record created on the local Clinical Information System (with patient name, Medicare card number, date of birth and gender as part of the local record).⁵²

3.40 The ADHA noted that healthcare provider organisations must be registered to access the MHR system, and indicated it was important providers use up-to-date version of their CIS.⁵³

3.41 Some submitters noted that the software currently used by clinicians may not be well-integrated with the MHR interface and that this may lead to information gaps in MHRs. For example, the APS said in its submission:

Currently, psychologists are unable to write data to the MHR as the MHR interface is not compliant with the practice software for psychologists. This means that essential health information will not be included in a person's MHR. The absence of this important health information dilutes the continuity of care for consumers and reduces the reliability of MHR.⁵⁴

3.42 The RACGP noted a similar concern that if a CIS used in a general practice was not the latest version, then the MHRs functions may not fully integrate with their

50 Australian Privacy Foundation, *Submission 1*, p. 31; Ms Bianca Phillips, Mr Shane Genziuk and Mr Jerome Owagage, *Submission 52*, [p. 3]; Dr David More, *Submission 54*, p. 4.

51 Mr Paul Shetler, *Committee Hansard*, 17 September 2018, p. 4.

52 ADHA, *Submission 31*, p. 10.

53 ADHA, *Submission 31*, p. 10.

54 APS, *Submission 73*, p. 1.

CIS. RACGP noted that such compatibility challenges pose significant barrier to adopting the MHR.⁵⁵

3.43 Dr Andrew Magennis, a general practitioner with extensive experience in medical software, noted that the MHR system is currently operating as a document management system, which, on viewing by a clinician, presents a list of documents which the clinician then has to open to determine contents and repeat this process with other documents until an understanding of the health context is determined.⁵⁶ This view aligned with that of an individual submitter, who noted that there does not appear a way for the data from a health-related document in their MHR can be summarised for the use of healthcare professionals.⁵⁷

3.44 The Australian Privacy Foundation was particularly critical of the document management capability in MHRs and suggested little clinically useful data would be included.⁵⁸

Break glass (override functionality)

3.45 Some submitters noted that access codes could inhibit practitioners from accessing information that could be clinically necessary. For that reason, MHR includes a 'break glass' feature that allows practitioners who are in emergency situations and need to access the information to do so.

3.46 The break glass functionality will, in an emergency situation, allow a healthcare provider to access the record or documents which a healthcare recipient had applied an access code to. The ADHA, the current System Operator, submitted that each break glass event would be investigated.⁵⁹

3.47 Consumers of Mental Health WA observed that provisions are not made to restrict which health professionals can use the break glass function.⁶⁰ Multiple Sclerosis Australia noted that healthcare recipients can elect to receive a message or email when the break glass function had been used.⁶¹ Dr Donald Rose, Summerdale Medical Practice, considered that the inability for healthcare recipients to block the break glass function from overriding a record access control is a major system flaw.⁶²

Additional administration and costs for healthcare providers

3.48 Some submitters expressed concern that the MHR system may lead to additional work that would be passed on to the healthcare provider, or that the

55 RACGP, *Submission 74*, p. 9.

56 Dr Andrew Magnennis, *Submission 57*, p. 2.

57 Mr Ian Bowie, *Submission 7*, [p. 2].

58 Australian Privacy Foundation, *Submission 1*, pp. 4, 5.

59 ADHA, *Submission 31*, [p. 27].

60 Consumers of Mental Health WA, *Submission 64*, p. 64.

61 Multiple Sclerosis Australia, *Submission 32*, p. 7.

62 Dr Donald Rose, Summerdale Medical Practice, *Submission 58*, p. 1.

provider would not be appropriately remunerated for the additional work that the MHR system requires. For example, MIGA commented that excessive administrative and time burdens can pose challenges for health providers using the MHR system:

...the investments needed by practitioners and healthcare organisations in time, finances and understanding to use My Health Record effectively are significant. The capacity to do this varies significantly across professionals and locations.⁶³

3.49 The Royal Australian and New Zealand College of Radiologists (RANZCR) noted that, at present, only a small number of radiologists are uploading clinical radiologists reports to MHRs and that this was due, in part, to costs.⁶⁴ RANZCR argued that, due to radiology providers treating a large number of patients, the '...administrative costs associated with digital health, while relatively minor per patient, can become burdensome and costly in aggregate.'⁶⁵

3.50 The Law Council of Australia (LCA) suggested that healthcare providers who assist patients with their MHR registration may not be able to bill Medicare for that time, and was conscious that, for some providers, MHRs could be perceived as a burden on their limited consulting time.⁶⁶ The LCA recommended:

The Inquiry consult further with health practitioners about assisting patients with their MHR in a way that provides health practitioners with reasonable remuneration for their expertise and time to do so.⁶⁷

3.51 Currently, the Practice Incentives Program (PIP) eHealth Incentive program provides financial incentives for general Practitioners who meet set targets for uploading shared health summaries to healthcare recipients' MHRs.⁶⁸ The PIP eHealth Incentive program does not, however, provide incentives for general practitioners to update healthcare recipients' MHR information.⁶⁹ Submitters noted that a similar incentive program is not in place for other health professions.⁷⁰ RACP recommended that provider readiness incentives should be provided to hospital and community-based specialist physicians.⁷¹

63 MIGA, *Submission 65*, p. 2.

64 Royal Australian and New Zealand College of Radiologists (RANZCR), *Submission 47*, [p. 2].

65 RANZCR, *Submission 47*, p. 2.

66 Law Council of Australia (LCA), *Submission 108*, p. 24.

67 LCA, *Submission 108*, p. 24.

68 ADHA, Practice Incentive Program (PIP) eHealth Incentive, <https://www.digitalhealth.gov.au/get-started-with-digital-health/pip-ehealth-incentive> (accessed 15 October 2018).

69 Mr Paul Power, *Committee Hansard*, 11 September 2018, p. 22.

70 Royal Australian and New Zealand College of Psychiatrists, *Submission 30*, p. 4; AMA, *Submission 79*, p. 13; Australian Dental Association, *Submission 107*, p. 7.

71 RACP, *Submission 106*, pp. 3, 7.

3.52 The Australian Association of Social Workers also expressed concern that the implementation of the MHR system may create a financial burden for accredited mental health social workers:

...the [Australian Association of Social Workers] shares the concerns of other allied Health professions that the cost of conformant software is prohibitive, especially for Accredited Mental Health social workers who are mainly in practice as sole operators or as part of small practices. Compared with the situation of general practices and other health services, social workers in private practice face significant financial burden in participating in My Health Record.

Committee view

3.53 The committee recognises that access to patient information is currently problematic for healthcare providers in clinical settings and that poor information can cause serious adverse impacts for patients' healthcare. In the committee's view, the MHR system provides an improvement to the information currently available to healthcare providers, which should improve the quality of care provided to healthcare recipients. The committee notes that some submitters anticipate MHRs will provide healthcare recipients with a better understanding of, and engagement with, their clinical care. The committee considers that MHRs, if managed correctly, can empower both healthcare providers and healthcare recipients.

3.54 However, the committee strongly believes that realising the benefits of MHRs in clinical use will involve overcoming some widespread issues. For example, the comprehensiveness of healthcare recipients' MHR information was a concern raised by many submitters during the inquiry. Healthcare providers submitted that, whilst healthcare recipients have a fundamental right to determine how their information is used, recipients using increased privacy controls in their MHRs can make providers' access, and contribution to, their MHR information difficult. Submitters stated that incomplete information in healthcare recipients' MHRs will reduce the clinical utility of those records.

3.55 Healthcare providers have also reported experiencing difficulty in accessing MHR information through their clinical information systems. Some submitters were concerned that healthcare providers face an administrative and cost burden in engaging with the MHR system. The committee believes that such issues could undermine the efficiency of the MHR system, and that the System Operator should take a lead role in investigating these issues. Where necessary, the System Operator should develop solutions which maximise the MHR system's benefits.

Chapter 4

Transitioning from opt-in to opt-out

4.1 A key principle of the My Health Record (MHR) system is that it will provide individuals with greater control and management of their health information.¹ In particular, the system is intended to enable consumers to access their own record, control what information is in it and which health care provider organisations can access it.²

4.2 As discussed in Chapter 1, the MHR system was originally designed as a voluntary opt-in system³ and, consistent with the idea of freedom of choice, individuals were free to decide whether they wished to have an electronic health record at all.⁴ However, following a period of review and evaluation, the Australian Government announced the decision to transition to an opt-out participation model, as part of the 2017-18 Budget.

4.3 This chapter will consider the basis for the decision to transition to an opt-out system and the impact this has had on individuals' ability to choose if and how to participate in the MHR system. The chapter considers the extent to which consumers have access to information to enable them to make an informed choice about whether to participate in the MHR system and, if so, how to exercise control over what records will be available in their MHR and who will be able to access those records.

Why adopt an opt-out system?

4.4 The announcement that the system would transition to an opt-out model of participation followed a period of review and consultation. In December 2013, a panel of health and IT experts tabled the report of the *Review of the Personally Controlled Electronic Health Record* (Royle Review).⁵ From March to October 2016, trials of different participation models were conducted in four regions across four states.⁶

4.5 Following completion of an evaluation of the trials and consultation with the Council of Australian Governments Health Council, the Australian Government decided to transition the MHR system to an opt-out model.⁷

1 Department of Health (DOH) and Department of Human Services (DHS), *Submission 22*, p. 2.

2 Australian Digital Health Agency (ADHA), *Submission 31*, p. 9.

3 DOH and DHS, *Submission 22*, p. 4.

4 The Hon. Nicola Roxon MP, Minister for Health, *House of Representative Hansard*, 23 November 2011, p. 13578.

5 Richard Royle, Dr Steve Hambleton and Andrew Walduck, *Review of the Personally Controlled Electronic Health Record* (Royle Review), December 2013, p. 4.

6 DOH, *Evaluation of My Health Record Participation Trials*, <http://www.health.gov.au/internet/main/publishing.nsf/content/ehealth-evaluation-trials>, (accessed 9 October 2018).

7 DOH and DHS, *Submission 22*, p. 9.

The need for a critical mass of participants

4.6 At the time of the Royle Review, the Personally Controlled Electronic Health Records (PCEHR) system had just over one million users, and while adoption and utilisation was slowly growing, it appeared to have plateaued despite efforts to increase consumer registration.⁸

4.7 Evidence to the Royle Review considered that the system would be more valuable and more practitioners would use the system if it had a broader participation base.⁹ A number of submitters expressed concern that an opt-in system would not generate the critical mass necessary to make the system a success.¹⁰

4.8 The Royle Review noted that without a critical mass of patients registered, medical practitioners had no incentive to use the system.¹¹ At the same time, medical practitioners expressed concern that the time required to assist patients to register under an opt-in system was a substantial impost on their time.¹² The Royle Review noted that without a clear understanding of the potential benefits there was limited motivation for both consumers and health practitioners to participate in the system.¹³

4.9 Submitters to the Royle Review considered that the problems of population and health practitioner usage could be eliminated if the system moved to an opt-out system.¹⁴ The Royle Review noted that, provided safety and security issues are addressed, the international experience suggested that an opt-out system would be well received and that the opt-out rate could be low.¹⁵

4.10 In its final report, the Royle Review recommended that the system should be transitioned to an opt-out model.¹⁶ The Royle Review stated that this recommendation was subject to the completion of minimum composite of records and the establishment of clear standards for compliance for clinical users.¹⁷

4.11 As noted in Chapter 1, the Department of Health (DOH) commissioned four trial sites in 2016 to trial both an opt-in and an opt-out model of participation. The report of the independent *Evaluation of the Participation Trials for the My Health Record* (Evaluation) states that the trials were designed to:

8 Royle Review, p. 6.

9 Royle Review, p. 28.

10 Royle Review, p. 28; Consumers Health Forum of Australia (CHF), *Submission 16*, p. 5.

11 Royle Review, p. 55.

12 Royle Review, p. 55.

13 Royle Review, p. 55.

14 Royle Review, pp. 28, 55.

15 The Royle Review noted evidence from New Zealand and the United Kingdom and noted that the summary care record rollout by the National Health Service in England contacted 45,997,228 people with an opt-out rate of 1.4 percent. Royle Review, p. 28.

16 Royle Review, p. 16.

17 Royle Review, p. 16.

1. Understand public reaction to an opt-out participation arrangement for the My Health Record
2. Understand the extent to which healthcare provider contribution and use of the My Health Record system improves when the majority of their patients have a My Health Record
3. Understand any implementation issues that would need to be addressed before any decision is made about future participation arrangements.¹⁸

4.12 The Evaluation found that there was consistent growth in the number of healthcare provider organisations registering for the MHR across the trial period, with consistently higher proportional growth in opt-out trial sites compared to opt-in sites.¹⁹ The Evaluation concluded that there was evidence and support to transition the MHR system to an opt-out model.²⁰

4.13 The concerns about an opt-in model were echoed in submissions to this inquiry. A number of submitters stated that an opt-out model remains the only way to achieve a sustainable number of users.²¹ For example, the Australian Medical Association (AMA) told the committee that it considered that the move to an opt-out system was necessary to promote a high level of participation in the system and highlighted the low rate of participation in the system since its introduction in 2012:

The My Health Record has had a long and difficult history and there is now considerable Australian evidence to show opt in arrangements are very unlikely to achieve high levels of participation – amongst citizens and clinicians. When the Personally Controlled Electronic Health Record was launched as an opt in model in 2012, uptake remained low. As at 19 August 2018, only 24 per cent of Australian citizens had opted in.²²

4.14 Allied Health Professions Australia (AHPA) told the committee that its experiences during the participation trials indicated that the system becomes more effective as the number of users increase:

Our own involvement with practitioners involved in the 2016 opt-out participation trials and understanding about other similar international systems shows that the system becomes vastly more effective and the benefits far more significant as the volume of users grows. Conversely, our longer-term engagement with the system and its precursor show that without that volume of consumers, the benefit to engaging with the system isn't there and practitioners may seek in vain to make use of the system,

18 Siggins Miller, *Evaluation of the Participation Trials for the My Health Record*, Final Report, November 2016 (Evaluation), p. iii.

19 Evaluation, pp. 32–33.

20 Evaluation, p. vi.

21 Dr Linc Thurecht, Senior Research Director, Australian Healthcare and Hospitals Association, *Committee Hansard*, 11 September 2018, p. 9; Royal Australian College of Physicians, *Submission 106*, p. 6; Allied Health Professions Australia (AHPA), *Submission 33*, [p. 5]; Australian Medical Association (AMA), *Submission 79*, p. 9.

22 AMA, *Submission 79*, p. 9 (emphasis omitted).

finding that their patients don't have records or these don't contain relevant health information.²³

Benefits without active engagement

4.15 The Royle Review noted that transitioning to an opt-out system would allow 'healthy' individuals, who might not otherwise have signed up to the system, to obtain the benefit of having an electronic health record when they need clinical care without having to take active steps to participate. The Royle Review noted concerns that there had been a lack of focus on those consumers in most need of an electronic health record, such as those with chronic medical conditions or those living in remote areas.²⁴ It concluded that an opt-out system may have benefits to vulnerable and disadvantaged groups who may otherwise face obstacles to signing up.²⁵

4.16 Federation of Ethnic Communities' Councils of Australia (FECCA) submitted that while it believes that schemes such as the MHR should be opt-in as a matter of principle, 'many harder-to-reach [culturally and linguistically diverse] communities may not have opted in to the MHR.'²⁶

4.17 The Australian Digital Health Agency (ADHA) told the committee that the ability to obtain the benefits of the system without having to actively engage remains one of the key reasons for having an opt-out system.²⁷ Mr Tim Kelsey, Chief Executive Officer of the ADHA pointed to evidence of the success of the Northern Territory's ehealth record, to support this approach.²⁸

4.18 The Evaluation of the MHR trials found that once people received information regarding the benefits of the MHR system, their responses to the system were positive.

For most individuals, after automatic creation was explained and the benefits of the My Health Record system were understood, the sentiment was positive. They said the fact that they did not have to do anything to create their My Health Record was a major plus. They expressed the view that they would not have registered for a My Health Record themselves and would have expected that their healthcare providers already would be sharing information with other healthcare providers in this way.²⁹

4.19 The Evaluation also noted that while the opt-out approach achieved greater relative registrations, it did so at an increased cost over the rest of Australia. However, the Evaluation considered that this increased cost is likely to be offset by bringing

23 AHPA, *Submission 33*, [p. 5].

24 Royle Review, p. 14.

25 Royle Review, p. 28; DOH and DHS, *Submission 22*, p. 6.

26 Federation of Ethnic Communities' Councils of Australia (FECCA), *Submission 45*, p. 2.

27 Ms Bettina McMahon, Chief Operating Officer, ADHA, *Committee Hansard*, 17 September 2018, p. 39.

28 Mr Kelsey, *Committee Hansard*, 17 September 2018, p. 41.

29 Evaluation, p. vi.

forward the benefits of the MHR system and achieving registrations with potentially vulnerable and hard to reach groups that may not otherwise have been engaged.³⁰

4.20 At the same time, the Evaluation noted that the proportion of Aboriginal and Torres Strait Islander people registered with MHR was low and did not change during the trial period. The Evaluation found that this confirmed evidence from focus groups and trial teams that there are particular barriers to the participation of Aboriginal and Torres Strait Islander peoples in rural and remote areas, such as computer literacy, internet access, health literacy and lack of linkages with other specific healthcare programs.³¹ The Evaluation noted that neither the opt-out or opt-in trials have provided lessons on how to address the impact of no or unreliable internet access.

Committee view

4.21 The committee notes the findings of the Royle Review that without a critical mass of patients registered, there is little or no incentive for medical practitioners to participate in an electronic health record system. Evidence received during this inquiry also indicates that an opt-out model remains the only way to achieve a sustainable number of users. The committee has noted the Royle Review's observation that an opt-out system would be well received. While the Royle Review cites consultation undertaken by the Consumer Health Forum and international experience,³² as supporting a move to an opt-out system, the committee considers it is important to note that the Royle Review did not undertake community consultation to determine the acceptability of an opt-out system to the Australian public. The committee also notes that the Royle Review's finding was predicated on safety and security issues being addressed and clear standards for clinical users being established.

4.22 The evidence to the Royle Review suggested that there had not been sufficient focus on the needs of vulnerable or hard to reach individuals, who may stand to benefit from an electronic health record. The committee considers that the Evaluation identified a need for particular focus on the needs of hard to reach individuals, such as those living in rural and remote locations, Aboriginal and Torres Strait Islander people and people and on barriers to participation in the MHR system, such as computer literacy, internet access

4.23 The committee recognises that an opt-out participation model has potential to facilitate the engagement of hard to reach individuals through the automatic creation of MHRs. However, the committee notes that while an opt-out model has the capacity to significantly increase participation, the findings of the Royle Review and the Evaluation identify that increased participation in the trials was underpinned by participants receiving an explanation of the system that addressed any concerns they had about privacy and security. The Evaluation also noted other measures necessary to address the needs of vulnerable and hard to reach individuals.

30 Evaluation, p. xiii.

31 Evaluation, p. vi.

32 Royle Review, p. 28.

Supporting individuals to actively engage with the MHR system

4.24 Both the Royle Review and the Evaluation noted the importance of developing and implementing a comprehensive education campaign to inform consumers and clinicians about the impact of the change to an opt-out process, the benefits of the MHR system and the provision made to ensure the security and privacy of records in the system.³³

4.25 The Evaluation noted the importance of explaining the benefits of the MHR system in allaying individuals concerns about security and privacy.

They most often said that, while they thought that no computer-based systems were totally safe, on balance they thought that the benefits to them, their families and the health system far outweighed those risks. This attitude held firm across general population, people from culturally and linguistically diverse (CALD) backgrounds, Aboriginal and Torres Strait Islander participants, gender, age groups, varying levels of computer literacy and access to computers or reliable internet. This reinforces the need for national awareness activities which make clear the benefits of the My Health Record system as well as the privacy and security protections.³⁴

4.26 Stakeholders also advised the Evaluation of the need to develop strategies to reach specific populations, 'such as patients who lack capacity due to dementia or more transient states of cognitive impairment, and others with carers acting as legal guardians (e.g. people with a disability, the elderly, CALD populations)'.³⁵ The Evaluation noted the 'motivators to use the My Health Record were most often described as: access to information and the influence of patients' use of the system or their own beliefs that the My Health Record system will improve access and save them time.'³⁶

The communication strategy

4.27 Submissions from ADHA and DOH and DHS advised the committee that the current communications campaign has been informed by the trials and focuses on a national campaign with information developed centrally, but media strategies and advertising run at a local level.³⁷

4.28 ADHA explained that the national communications plan considered the following key findings from the trials:

- General consumer awareness should be raised by a nationally coordinated, but locally run communications campaign;

33 Royle Review, p. 16; Evaluation, p. xiii.

34 Evaluation, p. vi.

35 Evaluation, p. 195.

36 Evaluation, p. xv.

37 *Submission 22*, p. 20; *Submission 31*, p. 11.

- Consumers were most receptive to messages about the My Health Record when they were in a healthcare setting, compared with mass communication such as letters sent to every household;
- Once aware of the My Health Record, consumers often sought more information or an opinion about the system from their healthcare provider – typically their GP or pharmacist; and
- It was a mistake to commence the public communications campaign before the opt-out period had started, as some consumers wanted to opt out immediately but were unable to, and other dismissed the message because they were unable to act on it for another 4-6 weeks.³⁸

4.29 Responsibility for communicating the benefits of the MHR system and the rights people have to opt out of it rests with the ADHA. The ADHA advised the committee that it has put in place a comprehensive campaign to ensure as wide awareness as possible,³⁹ and that \$27.5 million has been allocated to raise consumer awareness about opting out.⁴⁰

4.30 Noting the findings of the Evaluation, the communications plan for national opt-out included:

- initial focus on healthcare provider awareness of MHR and the opt-out system via multiple channels to enable providers to respond to enquiries from consumers;
- placement of consumer messages in healthcare settings;
- central design of campaign messages to support media strategies run at a local level;
- provision of messaging on what the MHR was and assisting consumers to make an informed decision about whether to opt out, including on-line information and videos on how to set privacy controls; and
- commencement of the campaign to coincide with when consumers could opt out.⁴¹

4.31 In its submission, ADHA advised that the campaign has involved expenditure of \$5.454 million dollars⁴² and had wide circulation resulting in:

- over 925 million opportunities to see social media content;
- more than 1.5 million visits to the MHR website following interest and publicity in the media;
- 5067 pieces of traditional media (press, radio and television); and

38 *Submission 31*, p. 11.

39 Mr Kelsey, *Committee Hansard*, 17 September 2018, p. 37.

40 *Submission 31*, p. 12.

41 *Submission 31*, p. 12.

42 Mr Kelsey, *Committee Hansard*, 17 September 2018, p. 50.

- availability of information in over 15 000 health care locations including general practices, pharmacies, hospitals and Aboriginal medical services.⁴³

4.32 The ADHA advised that, as of 3 September 2018 and based on tracking research surveying 1000 people weekly, awareness of the MHR system has increased to 87 percent and awareness that every Australian will get a MHR, unless they choose to opt out, has increased from 16 percent to 59 percent since the commencement of the opt-out period. The ADHA further advised that more than 1.5 million people have visited the MHR website since the commencement of the consumer awareness campaign with the percentage of new visitors (>81 percent) and the bounce/exit rate (>29 percent) indicating that people have found the information they needed.⁴⁴

4.33 However, a number of submitters and witnesses to the inquiry raised concerns that people are not sufficiently informed about the MHR system, its functions and settings, to make an informed decision about whether they should participate in the system.⁴⁵ The Royal Australian and New Zealand College of Psychiatrists (RANZCP) called for an expanded public information campaign and noted:

While there has been more information since the start of the opt-out period, RANZCP members have noted that awareness levels still appear to be low. Furthermore, there has been confusion around the intent and scope of the My Health Record, particularly since the start of the opt-out period. It is appreciated that assurances have been given to address some of the issues raised during the start of the "opt out" period, however, this has added to the confusion as some of the information provided to carers and consumers is now out of date.⁴⁶

4.34 The ADHA acknowledged that there had been criticism of the communications strategy for the MHR system. Mr Kelsey told the committee:

I fully accept the fact that there's been criticism of the communications. Certainly there's more that can be done, and we will absolutely be doing as much as we can.⁴⁷

4.35 Many submitters felt that a more comprehensive media communications strategy should be implemented.⁴⁸ For example, the Australian Healthcare and Hospitals Association said that the ADHA must ensure that the benefits and relative risks of the MHR system are understood by all segments of the Australian population to the greatest extent possible.⁴⁹ The Royal Australian College of General

43 ADHA, *Submission 31*, pp. 12–13.

44 ADHA, *Submission 31*, p. 12.

45 See for example: Royal Australian and New Zealand College of Psychiatrists (RANZCP), *Submission 30*, p. 8; Royal Australian and New Zealand College of Radiologists (RANZCR), *Submission 47*, [p. 6].

46 *Submission 30*, p. 5.

47 *Committee Hansard*, 17 September 2018, p. 39.

48 See for example: Health Consumer's Alliance SA, *Submission 23*, p. 6.

49 Dr Thurecht, *Committee Hansard*, 11 September 2018, p. 8.

Practitioners (RACGP) recommended that the consumer awareness campaign should better articulate what the MHR system is, and is not, and should focus on consumer controls, including security settings, access restrictions and default settings and the standing consent principle underlying healthcare provider access and upload.⁵⁰

Raising awareness among medical practitioners

4.36 As noted above, the initial focus of the communications strategy was on raising healthcare provider's awareness of the MHR system and the opt-out mechanism.

4.37 A number of submitters recognised the important role health practitioners could play in providing information and guidance to consumers regarding the information held in their MHR to help them make decisions about whether information should be uploaded, removed or protected through access controls.⁵¹ The AHPA submitted that the role of health practitioners, particularly mental health professionals and professionals providing genetic and other types of counselling, has not been well considered and resourced. The AHPA stated that such practitioners would benefit from targeted training and specific digital resource packs that they could provide to their patients.⁵²

4.38 The RACGP advised that it is delivering an education and awareness program for general practice 'to ensure they understand the impacts on their teams and patients with the change to an opt-out model.'⁵³ The committee heard that the RACGP currently has a national roadshow visiting capital cities in all the major states and territories. Dr Pinskiert told the committee that, while it is a slow process, general practitioners who have participated in the sessions have found them helpful.

What we're tending to find is that most of our sessions-and I did one today by webinar-start off with an awareness level of about 20 percent. So about 20 percent of our members will have a My Health Record, which is relatively consistent with the population. About 20 percent have used My Health Record to try and obtain information. But they have not really understood the historical and environmental settings. By the end of the session, the awareness rises substantially. Most walk out saying, 'I am so much better informed. I should have known this two, three years ago'.⁵⁴

4.39 The Law Council of Australia (LCA) noted the importance of health care professionals being involved in assisting patients to understand their MHR, but proposed that consideration be given to providing reasonable remuneration for their expertise and time in doing so.⁵⁵

50 *Submission 74*, p. 5.

51 AHPA, *Submission 33*, [p. 9].

52 *Submission 33*, [p. 9].

53 *Submission 74*, p. 3.

54 *Committee Hansard*, 11 September 2018, p. 45.

55 Law Council of Australia (LCA), *Submission 108*, p. 24.

Informed consent in an opt-out model

4.40 A key concern for many submitters to the inquiry was that, as the MHR system was originally designed and implemented as an opt-in system, there was a reasonable expectation that the decision to register was underpinned by a level of engagement and informed consent. Submitters told the committee that this cannot be assumed in an opt-out model of participation⁵⁶ and emphasised the need to ensure that individuals fully understand what an MHR contains, who can access it and how and the access controls available to them.⁵⁷

4.41 The RACGP told the committee that, when a MHR is established, the healthcare consumer provides 'standing consent' for all healthcare organisations involved in their care to access that record and upload information. This standing consent applies until a patient explicitly communicates withdrawal of consent. The RACGP noted that there is no legal requirement for a healthcare provider to obtain consent from a patient on each occasion prior to uploading clinical information nor to provide an opportunity for a patient to review clinical information prior to upload.⁵⁸

4.42 In their submission the DOH and DHS explained:

The MHR system does not operate with any assumed or implied consent. The system recognises the importance of voluntary consent so where consent is required, express and informed consent is sought.⁵⁹

4.43 The President of the Australian Medical Association, New South Wales, Dr Kean-Seng Lim, told the committee that, as one of the first users of the opt-in system, his practice had typically spent 15 to 20 minutes with each patient, explaining what the MHR system could do and how the consumer could control access to it. Dr Lim expressed the view that the move from an opt-in system to an opt-out system changes the whole framework of informed consent and increases the responsibility to inform consumers adequately of the change.

We would argue that anyone who opted in under those circumstances had a level of understanding. In an opt-out system that same onus of education still exists, but the question is whether it is actually undertaken. Our view is that there hasn't been evidence that there is good understanding of those levels of control.⁶⁰

4.44 The Chair of the RACGP's Expert Committee on eHealth and Practice Systems, Dr Nathan Pinski, agreed that there is an increased requirement to provide education under an opt-out MHR model. He said that increased communication with consumer groups is needed to:

56 See for example: Mr Thomas Ballantyne, Head of the Victorian Medical Law Practice, Maurice Blackburn Lawyers, *Committee Hansard*, 17 September 2018, pp. 26–27.

57 Royal Australian College of General Practitioners (RACGP), *Submission 74*, p. 2.

58 *Submission 74*, p. 5.

59 DOH and DHS, *Submission 22*, p. 11.

60 *Committee Hansard*, 11 September, 2018, p. 36.

improve digital health literacy and to ensure that consumers are better informed about what My Health Record is, what the My Health Record expansion process is, and how they can use My Health Record to participate in their healthcare delivery; targeted consumer education on My Health Record consumer controls, how the record is activated, what the trigger event is and the impacts of the current standing consent process regarding information uploaded and viewed by healthcare providers.⁶¹

4.45 DOH and DHS and the ADHA maintain that by providing Australians with education and the opportunity to opt-out, the system ensures that Australians who remain within the system are providing their explicit consent to do so.⁶²

4.46 The ADHA said:

While originally established as an opt-in registration model, under an opt-out participation model, the original principles still apply: people have the right to participate but can choose not to, and the record is truly personally controlled.⁶³

4.47 However, other submitters were less confident that the system would support informed consent for access to data.⁶⁴

4.48 Mr Paul Shetler expressed concern about the extent to which individuals could provide clear, informed consent if they do not understand what it is they are consenting to:

...the default needs to be that it needs my affirmative consent to release anything. If I do give it, it's to my practitioners, my doctors, my pharmacists—the people who are actually serving me directly. Anything beyond that, I'm relatively suspicious of for many reasons. One is that a lot of the time, it's very difficult to give clear, informed consent to things you don't really understand in the first place.⁶⁵

4.49 Mr Grahame Grieve, Principal of Health Intersections Pty Ltd, told the committee that the system needs to be redesigned to support a distributed system that would enable patients to communicate directly with the healthcare service providers.

61 *Committee Hansard*, 11 September 2018, p. 41.

62 DOH and DHS, *Submission 22*, p. 11; ADHA, *Submission 31*, p. 5.

63 ADHA, *Submission 31*, p. 5.

64 Mr Ballantyne, *Committee Hansard*, 17 September 2018, p. 26; Future Wise, *Submission 15*, p. 8; Doctors Reform Society, *Submission 29*, [p. 3]; Positive Life NSW and National Association of People with HIV Australia, *Submission 44*, pp. 7–8; Consumers of Mental Health WA, *Submission 64*, p. 10; Children and Young People with Disability Australia, *Submission 102*, p. 5; Australia Manufacturing Workers' Union, *Submission 105*, [p. 4]; Joshua Badge, *Submission 113*, p. 6.

65 *Committee Hansard*, 17 September 2018, p. 4.

He said that people would remain suspicious of the system for as long as it remained a single national database.⁶⁶

In my experience the agreements people make when they use the system is that they want to share information with their care providers. Different clinical contexts mean different care providers, different requirements, but My Health Record only has one national agreement that everything has to fit into. Something simple, 'I agree to share this with my hospital and GP, but nobody else,' is too complex for the system because it's a one size fits all, and people can't decide that without a personal care context.⁶⁷

4.50 The LCA argued that the need for healthcare recipients to opt out of the secondary use of their data is at odds with the underlying principles in both Commonwealth and state privacy laws. The LCA told the committee that these principles provide that a health entity that holds information about a patient can only use or disclose the information for the particular purpose for which it was collected. The LCA recommends that healthcare recipients must provide explicit consent if their healthcare information is to be accessed for a secondary purpose and considered that this could be sought and obtained via the user settings and communication channels facilitated by the MHR system.⁶⁸

4.51 The ADHA noted that this issue was considered as part of the transition to the opt-out system but noted that placing barriers to participation in the system would effectively defeat the purpose of changing the system to opt-out.⁶⁹

4.52 The Consumers Health Forum of Australia (CHF) told the committee that it believed that, while it may not be possible to obtain fully informed consent for the entire population, the option to delete records or request cancellation of MHR registration should largely mitigate the consent issues that may be created by having an opt-out model.⁷⁰ However, the CHF agreed that an understanding of how data will be used, and the benefits of this, were key to consumers providing consent.

Our research shows that Australians want ownership and control of their own health data and want to give consent when it is used by governments, private companies and researchers. The same research also found that consumers are more likely to give permission if they understand how their data will be used and the benefits that will come from its use. There is a level of comfort among the majority of consumers in data being used to support health providers to improve care or make better policy. But

66 Mr Grahame Grieve, Principal, Health Intersections Pty Ltd, *Committee Hansard*, 17 September 2018, p. 11.

67 Mr Grieve, *Committee Hansard*, 17 September 2018, p. 11.

68 Mr Morry Bailes, President, LCA, *Committee Hansard*, 17 September 2018, p. 27.

69 Ms McMahon, *Committee Hansard*, 17 September 2018, p. 39.

70 CHF, *Submission 16*, pp. 20–21.

consumers are significantly less willing to share their data if it's to be used for commercial gain.⁷¹

4.53 AHPA submitted that greater clarity is required about how consent operates within the MHR framework and how this might compare to the way consent operates outside the MHR system. AHPA stated that greater clarity around the range of patient health information that can be accessed through the courts and other means would benefit both consumers and providers.⁷²

Awareness of privacy settings in the MHR system

4.54 As noted in Chapter 3 and above, in addition to having the ability to opt-out, individuals have the ability to choose to apply a number of access controls to manage the privacy of their MHR. These access controls are set out in the My Health Records Rule 2016 along with the default settings that apply to every MHR.⁷³

4.55 DOH and DHS explained that these advanced settings:

...enable a consumer to set a code to limit access to their whole MHR and to particular documents in it, and to prevent clinical information systems from automatically checking where a consumer has a MHR.⁷⁴

4.56 Submitters were generally supportive of the range of access controls available to consumers to manage access to their MHR.⁷⁵ However, concerns were expressed regarding healthcare recipients' awareness of the available access controls and default settings was considered particularly important by submitters, as they viewed access controls as being a key mechanism for managing inappropriate access to the MHR information of vulnerable groups of people.⁷⁶ The CHF told the committee that while it is quietly confident that there are enough features in the privacy and protections, further improvements to privacy and security settings need to be made available in easy to understand formats. CHF also recommended the development of dedicated user education about how to deploy existing privacy and security settings.⁷⁷

4.57 Some submitters and witnesses to the inquiry expressed concern that the default settings for these access controls were quite low and expressed concern that

71 Ms Leanne Wells, Chief Executive Officer, CHF, *Committee Hansard*, 17 September 2018, p. 7.

72 *Submission 33*, [p. 8].

73 ADHA, *Submission 31*, p. 9.

74 DOH and DHS, *Submission 22*, p. 10.

75 See for example: AMA, *Submission 79*, p. 3; Australian Healthcare and Hospitals Association, *Submission 86*, p. 10.

76 NSW Privacy Commissioner, *Submission 43*, p. 3.

77 CHF, *Submission 16*, p. 15.

this posed a risk for individuals who were not aware of the potential need to adjust them.⁷⁸

4.58 Ms Caroline Edwards of DOH confirmed that this was intentional:

The decision is to have an opt-out system, where everyone has a record unless they don't want one, and to provide a very comprehensive system where people can choose to go in and set those access controls, but making sure the default situation is one where health practitioners and patients have the most open access to the record in order to get the health outcomes we want.⁷⁹

4.59 Submitters and witnesses indicated better public information or training is needed for healthcare recipients to increase their understanding of the MHR system's access controls.⁸⁰ Dr Lim told the committee that it is vital to build trust in the system and ensure that patients are aware they are able to change their access controls 'before they be downgraded to a level that may not be in alignment with their wishes.'⁸¹

4.60 These concerns echo submissions to the Royle Review that argued an electronic health record 'cannot be described as personally controlled if a population group (e.g. Aboriginal and Torres Strait Islander peoples) do not have the skills or tools to personally control it.'⁸²

4.61 As noted earlier, based on responses to its weekly omnibus survey, the ADHA advised that levels of awareness have increased significantly since the commencement of the communications campaign and are tracking upwards.⁸³ Mr Kelsey said

In specific terms, the target of our real effort has been on ensuring people are fully aware of their rights to opt out and of those privacy controls you've described. So the more mature levels of awareness have gone from 16 per cent, before 16 July, to 59 per cent and that is tracking upwards⁸⁴

4.62 Mr Kelsey confirmed that this more mature level of awareness referred to an understanding of the option to opt-out of the MHR system:

There's a level of awareness of the privacy settings. The task that the agency was set was to ensure that people were aware of the benefits of My

78 See for example: Aboriginal Health Council of Western Australia (AHCWA), *Submission 91*, p. 3; Health Workers Union, *Submission 96*, p. 9.

79 Ms Caroline Edwards, Deputy Secretary, DOH, *Committee Hansard*, 17 September 2018, p. 40.

80 Primary Health Networks, *Submission 75*, [p. 4]; Pharmaceutical Society of Australia, *Submission 46*, p. 7; Dr Nathan Pinski, Chair, RACGP Expert Committee eHealth Practice Systems, RACGP, *Committee Hansard*, 11 September 2018, p. 44.

81 Dr Kean-Seng Lim, President, AMA, New South Wales, *Committee Hansard*, 11 September 2018, p. 31.

82 Royle Review, p. 54.

83 *Committee Hansard*, 17 September 2018, pp. 37–38.

84 *Committee Hansard*, 17 September 2018, p. 38.

Health Record, of their rights to opt out, and, as far as possible, of the additional communications around the privacy controls.⁸⁵

4.63 However, Mr Kelsey advised that the ADHA does not explicitly monitor the proportion of Australians who understand their ability or need to set access controls.⁸⁶

4.64 As discussed in Chapter 3, the ADHA told the committee that at 2 September 2018, 20 957 record access codes or limited document access codes had been set. Of this total number of access codes, 16 848 healthcare recipients had set a record access code; 4 109 documents had been protected by a limited document access code and 136 644 healthcare recipients had set notifications to alert them by email or text message when someone accesses their MHR for the first time.⁸⁷

4.65 At that time, the system had 6 105 536 registered users and contained 7 362 529 clinical documents.⁸⁸ Mr Kelsey noted that this meant that approximately 0.25 percent of healthcare recipients had elected to activate one of the privacy controls.⁸⁹

4.66 CHF expressed some caution in regard to these figures:

The low numbers of records with any controls set so far and the high level of consumer engagement with privacy and security controls when able and motivated to do so indicates that improvements to the MHR privacy and security settings could and should occur. These low numbers could indicate that few want to set privacy and security controls, but it is likely that, for many people who currently have a record, they simply don't yet know that they can exercise this level of control over their record or, if they do, don't have the digital literacy skills to make it happen.⁹⁰

Barriers to participation and 'hard to reach' individuals

4.67 A number of witnesses noted that the MHR appears to be based on the assumption that individuals have a high level of digital literacy.⁹¹ Submitters expressed concern about the ability of the average consumer to opt out of MHR or set appropriate privacy settings and noted low levels of digital literacy among some groups of consumers.⁹²

85 *Committee Hansard*, 17 September 2018, p. 38.

86 Mr Kelsey, *Committee Hansard*, 17 September 2018, pp. 38–39.

87 Ms McMahon, *Committee Hansard*, 17 September 2018, p. 36.

88 DOH and DHS, *Submission 22*, p. 5.

89 Mr Kelsey, *Committee Hansard*, 17 September 2018, p. 36.

90 CHF, *Submission 16*, p. 15 (footnotes omitted).

91 FECCA, *Submission 45*, p. 2.

92 See for example: CHF, *Submission 16*, p. 15; Carers Australia WA, *Submission 36*, p.2; Women's Legal Service Qld, *Submission 19*, p. 5.

4.68 Similar barriers to engaging with the system were raised in relation to people with lower levels of English language proficiency or digital literacy.⁹³ FECCA identified a lack of targeted communication, lower levels of English language proficiency or digital literacy as some of the key factors inhibiting CALD communities' involvement in an opt-in participation model. FECCA recommended that resources and funding should be allocated to ongoing education of new migrants who arrive after the cessation of the 2018 opt-out period, to enable them to make informed choices in the management of their MHR.⁹⁴

4.69 Future Wise also expressed particular concern that individuals from disadvantaged, or non-English speaking backgrounds are less likely to have the privacy awareness and digital literacy to exercise an informed choice about opting-out.⁹⁵ Future Wise saw benefit in improving general community education on digital literacy, not just in relation to the MHR system.⁹⁶

4.70 The Royal Flying Doctor Service (RFDS) also noted that both health literacy and digital literacy levels are often low in rural and remote communities. The RFDS submitted that the impact of this on participation in the MHR system has not been well considered in the rollout of the system and related public information campaigns to date. The RFDS strongly recommended a more targeted information campaign for rural and remote populations be developed.⁹⁷

4.71 The Aboriginal Health Council of Western Australia (ACHWA) expressed concern that no formal process currently exists to assist people with limited or no access to electronic connectivity and no or limited digital literacy to access and manage their record. The RFDS also noted the lack of technological infrastructure in a significant number of rural and remote locations would impact on individual's ability to access the MHR system.⁹⁸

4.72 Submitters also noted that it is difficult for young people and some Aboriginal and Torres Strait Islander peoples to opt-out, because this requires identity documents that they may not have or that may be held by others.⁹⁹

4.73 ACHWA recommended that consideration be given to funding the Aboriginal Community Controlled Health Services to provide assistance to Aboriginal people to

93 See for example: Carers WA, *Submission 36*, p. 2. Institute for Healthcare Transformation, Deakin University, *Submission 37*, p. 3.

94 FECCA, *Submission 45*, p. 2.

95 *Submission 15*, pp. 14–15.

96 *Submission 15*, p. 15.

97 *Submission 101*, p. 1.

98 *Submission 101*, p. 1.

99 See for example: Dr Robert Walker, *Submission 55*, [p. 2]; Orygen, the National Centre of Excellence in Youth Mental Health (Orygen), *Submission 63*, p. 3; Consumers of Mental Health WA, *Submission 64*, p. 4; RACGP, *Submission 74*, p. 7; AHCWA, *Submission 91*, pp. 2, 3.

access and manage their record.¹⁰⁰ ACHWA noted that a number of practical limitations would impact on the ability of Aboriginal and Torres Strait Islander peoples to manage the privacy settings on their MHR:

While the client can change the privacy functions, there are issues with Aboriginal people especially those in remote locations having reliable digital/electronic/phone connectivity e.g. with the Helpline, waiting times can be long, the client may not have a phone, and there may be not mobile phone connectivity.¹⁰¹

4.74 Submitters who represent people living with disability noted factors that would limit the accessibility of the MHR system via MyGov and My Health Record portals. For example, people with low vision cannot use the My Health Record website because it is not compatible with screen readers. Similarly, concerns were raised in on behalf of people with limited hand movement or other disabilities.¹⁰²

4.75 The Departments advised that the 2016 opt-out trials had identified certain individuals as 'hard to service' due to limited access to mainstream communication channels. Adult prisoners, juvenile detainees between the ages of 14 and 17 years and Defence personnel deployed overseas were confirmed as 'hard to service' in the 2017-18 Budget. DOH advised that it had consulted with correctional services staff in all jurisdictions, under the auspice of the Corrective Services Administrative Council, and with the Department of Defence to develop a strategy to ensure that these 'hard to service' individuals are given the opportunity to opt-out. The DOH also took advice from each state and territory regarding internal mechanisms available to communicate with prisoners in each jurisdiction.¹⁰³

4.76 In addition to this consultation, the ADHA advised that it has engaged with over 40 national and state-based peak advocacy and other organisations representing or supporting a wide range of 'hard to reach' and vulnerable groups. ADHA said that a number of these groups have been funded to assist with the dissemination of communication information directly to their members. The ADHA is also working with organisations to tailor information for their members, including mental health organisations.¹⁰⁴

4.77 However, the committee received evidence from some organisations expressing concern that some hard to reach communities or individuals had not received the same opportunity to access information or the required access to enable them to opt-out of having a MHR.¹⁰⁵ For example, Orygen, The National Centre of

100 *Submission 91*, p. 2.

101 Aboriginal Health Council of Western Australia, *Submission 91*, p. 3.

102 See for example: People with Disabilities ACT Inc, *Submission 18*, p. 3.

103 *Submission 22*, p. 20.

104 ADHA, *Brief: Reaching People with Mental Health Conditions*, additional information received 25 September 2018, pp. 1–3.

105 See for example: National Rural Health Alliance, *Submission 66*, [p. 8]; People with Disabilities ACT Inc, *Submission 18*, p. 3.

Excellence in Youth Mental Health (Orygen) expressed concern on behalf of vulnerable young people, such as those experiencing mental ill-health, living in out-of-home care, in secure welfare or in detention, remand or prison.¹⁰⁶ Orygen expressed concern about a lack of timely and age appropriate information developed for young people.

An offer by Orygen to ADHA to provide assistance and advice resulted in Orygen facilitating the provision of feedback from young people on the information sheet after the opt-out period had opened.¹⁰⁷

Committee view

4.78 The committee understands the need for the MHR system to attract a critical mass of participants in order to maximise its utility to health consumers and medical practitioners. However, the committee is concerned that, without careful administration and a comprehensive program of education and support for all participants, there appears to be a high degree of risk of unintended consequences.

4.79 Of particular concern is the apparent assumption that by not opting out of the MHR system, an individual has given their consent for access to information in their MHR. The committee considers that, while this may be the case, it is equally likely that individuals who have not opted out of the system may have only a limited understanding of the system.

4.80 The committee considers that the focus of the communications campaign to date has not supported people to understand the benefits of the MHR system or the significance of reviewing the access controls on their MHR. The committee is concerned that the default settings are lower than many people would expect. The committee considers that the default settings should be set higher and the system should require an individual to actively choose to remove the default setting. Without a thorough understanding of the MHR system, individuals may not be aware what records are available in their MHR and who can access them.

4.81 The committee is particularly concerned for the wide range of groups in the Australian community who may experience difficulty accessing and using the MHR system. The committee notes advice from the ADHA regarding the preparation of information materials tailored to the needs of particular groups, but is concerned by evidence that suggests the level of support provided to vulnerable groups or 'hard to reach' individuals may not have been sufficiently timely or appropriate. The committee proposes to consider the range of information and support available to assist people who may experience difficulties accessing the system in greater detail.

4.82 The committee notes that the ADHA is implementing a staged communications campaign, and welcomes its recognition that there is more that needs to be done to effectively communicate an adequate understanding of the MHR system to all participants. The committee considers that there is a need for greater

106 Orygen, *Submission 63*, p. 2.

107 *Submission 63*, p. 3.

transparency in how awareness and understanding of the system is being tracked and measured and with regard to steps taken to address issues as they are identified. The committee considers that there is a need for an expanded and more comprehensive communications strategy, particularly with regard to providing explicit guidance to enable people to review and set access controls for their MHR. The committee considers that the opt-out period should be extended to accommodate this.

Chapter 5

Conclusion and recommendations

5.1 The My Health Record (MHR) system is a significant healthcare reform with the potential to improve the quality of healthcare and health outcomes for many Australians. To achieve this, the system needs a high degree of support from both the public and medical practitioners. For this to happen, both the public and medical practitioners need to have a high degree of confidence in the integrity of the system.

5.2 However, the MHR system presents considerable operational complexity given its application in a wide variety of healthcare settings, and the diverse healthcare and privacy needs of the healthcare recipients using it. The committee considers that the transition to an opt-out participation model has highlighted some significant tensions within the system.

System utility at the expense of patient privacy and security

5.3 The committee notes evidence received from inquiry participants regarding a need for balance between access for clinicians and privacy controls for healthcare recipients. The committee received evidence that highlighted the significant clinical benefits that could be achieved through the MHR system. The ability to ensure that clinically important medical information is available at the point of care, where ever that might be, should result in improved patient care and patient safety, improved medical communication and improved continuity of care between providers.

5.4 To achieve an appropriate level of utility within the MHR system, it is important to have broad participation in the system, that the information held within the system is as accurate and complete as possible, and that those medical practitioners who need to access a healthcare recipient's MHR are able to do so in a timely, efficient and secure manner. However, this level of utility should not to be achieved at the expense of a healthcare recipient's privacy or security.

5.5 Healthcare information is a particularly sensitive category of information, and requires significant protection within the health system. Some evidence received during this inquiry suggests that an unreasonable compromise has been struck between ensuring the utility of the system, through an opt-out mechanism and low default access settings, and safeguarding the privacy and safety of healthcare recipients.

5.6 The committee notes that amendments currently before the Senate¹ have the potential to strengthen some of the privacy and security protections within the MHR system. However, the committee considers that further amendments are necessary if the Australian public is to have confidence in the MHR system.

1 My Health Records Amendment (Strengthening Privacy) Bill 2018.

Informed consent

5.7 Evidence to the committee suggests that a level of implied consent is implicit in an opt-out participation model. However, the committee is not persuaded that this can be assumed. The fact that an individual does not opt-out of the MHR system, or does not take steps to restrict access to part or all of their MHR, does not necessarily mean that they have understood the risks and benefits of the MHR system and made a considered decision based on this. As a number of submitters indicated, it could simply mean that they do not fully appreciate what a MHR is, or who has access to it and in what circumstances.

5.8 While the committee appreciates that the opt-in participation model was not successful in delivering the critical mass necessary for the success of the MHR system, it considers that the current opt-out model has swung too far in favour of ease of access and has not focussed enough on the importance of ensuring that the public is able to make an informed choice about whether to participate in the system and the level of security they might require if they do.

Default access settings

5.9 It is the committee's view that the responsibility of the System Operator to apply considered and robust default settings that protect the privacy of all registered healthcare recipients is considerably increased under an opt-out model.

5.10 The committee appreciates that a strong rationale exists for designing the MHR system in favour of reasonable access for clinicians. However, the committee notes that when healthcare recipients' MHRs are created, the default access settings applied to their records will be, as many submitters described, 'open'. Evidence to the committee does not support a high degree of confidence that individuals are aware of this and recognise that they should review the access settings applying to their MHR to ensure that they reflect their personal circumstances. However, the committee notes evidence that where healthcare recipients have received an explanation of the risks and benefits of the system and the mechanisms available to them to control access to their MHR, they have reacted positively to the MHR system.

5.11 In this context, the committee considers that the default access settings should be considerably higher and should only be relaxed when the healthcare recipient explicitly consents to this.

Recommendation 1

5.12 The committee recommends that record access codes should be applied to each My Health Record as a default and that individuals should be required to choose to remove the code. The committee further recommends that the ability to override access codes in the case of an emergency should only be available to registered healthcare providers for use in extraordinary and urgent situations.

Protecting the privacy and security of vulnerable people

5.13 The committee is mindful that MHRs will be used by a diverse range of Australians, some of whom may have unique circumstances or vulnerabilities that make the information in their MHRs particularly sensitive. The committee considers

that having a MHR should not compromise the safety of vulnerable people and/or jeopardise their ability to confidentially seek medical advice. The committee is deeply concerned by evidence that perpetrators of domestic violence may be able to legitimately gain access to MHR records and exploit this to the detriment of their former partner or children.

5.14 The committee considers that careful consideration must be given to the use of MHRs by vulnerable people, particularly young people aged between 14–17 years or people escaping from domestic violence, and the protections offered to address their particular circumstances. The committee urges the Australian Digital Health Agency (ADHA) to work closely with service providers who support young people and people experiencing domestic violence. However, the committee considers the seriousness of these concerns warrants a legislative response.

Recommendation 2

5.15 The committee recommends that the Australian Government amend the *My Health Records Act 2012* to protect the privacy of children aged 14 to 17 years unless they expressly request that a parent be a nominated representative.

Recommendation 3

5.16 The committee recommends that the Minister for Health amend the *My Health Record Rule 2016* to extend the period for which a My Health Record can be suspended in the case of serious risk to the healthcare recipient, such as in a domestic violence incident.

Secondary use of MHR data

5.17 The committee recognises that information held within the MHR system has the potential to create a valuable data set. The committee notes evidence that MHR data could make a significant contribution to public health research, providing insights into population health issues and patterns of use of the health system.

5.18 At the same time, the committee notes that the default setting for secondary use of MHR data is that an individual is assumed to have consented to the use of their data, unless they actively withdraw this consent. The committee considers that while such an assumption may have been reasonable under an opt-in participation model, where an individual chose to create a MHR, it is not reasonable under an opt-out model.

Recommendation 4

5.19 The committee recommends that data which is likely to be identifiable from an individual's My Health Record not be made available for secondary use without the individual's explicit consent.

5.20 The committee also notes concerns that MHR data could be made available for commercial purposes, by insurers and other commercial entities. The committee considers that in order for the Australian public to place their trust in the MHR system, there must be no doubt that MHR data, including de-identified data, will not be used for commercial purposes. The committee notes that the current Secondary Use

Framework prohibits the use of data for 'solely commercial purposes'. The committee recognises that there is a lack of clarity around this prohibition.

Recommendation 5

5.21 The committee recommends that the current prohibition on secondary access to My Health Record data for commercial purposes be strengthened to ensure that My Health Record data cannot be used for commercial purposes.

Access by third parties

5.22 The committee notes concerns regarding third party access to information within the MHR system. In particular, the committee is concerned by evidence suggesting that MHR data could be made available to employers by employer nominated health practitioners or that employers may ask employees to consent to the release of information in their MHR. The committee notes evidence from the Department of Health and the ADHA that it is not intended that information contained in an individual's MHR could be accessed for any purpose other than the provision of health care to that individual. The committee considers that this intention should be made explicit in the legislation.

Recommendation 6

5.23 The committee recommends that no third-party access to an individual's My Health Record be permissible, without the explicit permission of the patient, except to maintain accurate contact information.

5.24 The committee is concerned by evidence indicating the protection provided by the current prohibition in the *Healthcare Identifiers Act 2010* on healthcare providers disclosing a healthcare identifier in an employment context could be circumvented. The committee is also concerned by evidence suggesting that employees may be coerced by an employer into providing their consent for access to their MHR. The committee considers that the legislation must be strengthened to ensure that an employee's right to privacy is protected in the context of employer-directed health care.

Recommendation 7

5.25 The committee recommends that the Australian Government amend the *My Health Records Act 2012* and the *Healthcare Identifiers Act 2010* to ensure that it is clear that an individual's My Health Record cannot be accessed for employment or insurance purposes.

Recommendation 8

5.26 The committee recommends that access to My Health Records for the purposes of data matching between government departments be explicitly limited only to a person's name, address, date of birth and contact information, and that no other information contained in a person's My Health Record be made available.

Deletion of records

5.27 The committee notes concerns regarding the practicality of measures providing for the permanent deletion of records. The committee recognises that amendments contained in legislation currently before the Senate will require the permanent destruction of any record upon request from a healthcare recipient.² Evidence to the inquiry has expressed concern about the extent to which such a request can be satisfied, noting that it is standard practice to create backups of databases and create cache files. The committee considers that the MHR system must include measures to ensure that any saved version of a person's MHR record is permanently destroyed in such circumstances and that cached or back-up versions of MHR records cannot be accessed by third parties, even after they have been deleted.

Recommendation 9

5.28 The committee recommends that the legislation be amended to make explicit that a request for record deletion is to be interpreted as a right to be unlisted, and as such, that every record is protected from third-party access even after it is deleted, and that no cached or back-up version of a record can be accessed after a patient has requested its destruction.

Supporting individuals and practitioners to engage with the MHR system

5.29 The committee is concerned that the current communication campaign has been insufficient to communicate a clear understanding of the MHR system and the significance of the change to an opt-out participation model. The committee considers that the campaign to date has focussed on achieving a broad level of awareness of the MHR system and the ability for individuals to opt-out and that this is insufficient to enable people to understand and consider their options.

5.30 The committee considers that, in an opt-out system, it is more important than ever to ensure that individuals understand the benefits of the system, the privacy and security implications of participation in the system and the degree of control they can exercise over access to their MHR before they decide whether or not to opt-out. Without a commitment to a comprehensive communications campaign, many individuals will be denied the opportunity to make an informed choice regarding their involvement in the system and many of the system's important security features will be rendered redundant.

5.31 The committee is concerned that the ADHA's tracking of the campaign is not adequately identifying the extent of the public's awareness of the security and privacy measures within the system and what they need to do to activate them. As already discussed, the default settings for controlling access to a MHR have been deliberately set to provide an 'open' level of access to maximise the utility of the system. The committee has already noted its concerns regarding the implications of this for some vulnerable groups.

2 See My Health Records Amendment (Strengthening Privacy) Bill 2018, item 6.

Recommendation 10

5.32 The committee recommends that the Australian Digital Health Agency revise its media strategy to provide more targeted comprehensive education about My Health Record.

5.33 The committee is particularly concerned for those in the Australian community who may experience difficulty accessing and using the MHR system. Many Australians face a range of practical impediments to their engagement with the MHR system. For example, the committee heard that the system assumes a level of connectivity and digital literacy that many individuals living in rural and remote communities simply do not have. Many groups within the community will not be able to readily access the identity documents needed to opt-out. The committee also notes evidence that people living with disability may have limited access to the MHR portals.

5.34 The committee recognises that the ADHA has developed strategies to ensure certain groups of 'hard to service' individuals, such as adult prisoners and juvenile detainees and defence personnel deployed overseas. However, the committee is concerned by evidence that suggests some vulnerable or hard to reach individuals may not have received timely and appropriate information and support to enable them to exercise their rights in relation to the MHR system.

5.35 At the same time, the committee considers that the Australian Government and the ADHA must redouble efforts to ensure that the Australian public has a clear understanding of the benefits and risks of the MHR system and the steps they can take to manage their privacy and security within it.

Recommendation 11

5.36 The committee recommends that the Australian Digital Health Agency identify, engage with and provide additional support to vulnerable groups to ensure that they have the means to decide whether to opt out, whether to adjust the access controls within their My Health Record and how to do this.

Recommendation 12

5.37 The committee recommends that the Australian Government commit additional funding for a broad-based education campaign regarding My Health Record, with particular regard to communicating with vulnerable and hard to reach communities.

Recommendation 13

5.38 The committee recommends that the Australian Government extend the opt-out period for the My Health Record system for a further twelve months.

Ongoing parliamentary oversight of the MHR system

5.39 The MHR system has the potential to revolutionise the quality and continuity of healthcare in Australia.

5.40 Any system that draws together personal health information on this scale involves a level of risk. In assessing the measures in the system to manage these risks,

the committee has been mindful of what the MHR system seeks to replace. Under the current system, there is a lack of interoperability and a lack of sophistication in the transfer of medical records between practitioners that does not meet the expectations of either healthcare recipients or medical practitioners. For example, the committee notes that there is still a high reliance on fax machines to transmit medical records.

5.41 The ability for multiple doctors and allied health practitioners, treating the same patient, in different places over a period of time, to access relevant patient clinical data at the time of treatment should result in safer, faster and more efficient health care and better health outcomes. However, it is important that the patient safety considerations in this equation are not neglected in the interests of speed and efficiency, either within the system itself, or in its implementation.

5.42 This inquiry has identified a number of key areas where the committee considers patient security appears to have been compromised in favour of the needs of health practitioners. It has made recommendations to address these concerns. At the same time, it is acutely aware of the need to continue to strive for an appropriate balance between patient privacy and security and the utility of the system for health practitioners.

5.43 The committee considers that the importance of this task and the significance of the privacy and security concerns identified with the implementation and administration of the MHR to date, warrant a level of ongoing parliamentary oversight.

5.44 The committee considers that public confidence in the integrity of the system would be enhanced by greater transparency in its administration. This includes greater transparency in tracking and evaluating understanding of and engagement with the system by individuals and medical practitioners.

Recommendation 14

5.45 The committee recommends that the My Health Record system's operator, or operators, report regularly and comprehensively to Parliament on the management of the My Health Record system.

Senator Rachel Siewert

Chair

Coalition Senators' Dissenting Report

Recommendation 1

The committee recommends that record access codes should be applied to each My Health Record as a default and that individuals should be required to choose to remove the code. The committee further recommends that the ability to override access codes in the case of an emergency should only be available to registered healthcare providers for use in extraordinary and urgent situations.

1.1 This recommendation is not supported as there are concerns with this proposal. In order for all Australians to set access controls, they would need to be provided their access code securely. Those Australians who did not (or could not) want to receive their PIN online, would need their access code to be sent to their postal address.

1.2 This represents a serious implementation challenge for many Australians. The health system does not have an accurate and current address for all Australians, which would result in a large number of Australians not being able to receive their PIN in order to provide it to their clinician. Furthermore, it would not be possible to guarantee that an individual's PIN would be protected from a third party, creating a privacy and security risk for the individual.

1.3 The evidence heard by the committee during the public hearings indicated that to realise the full benefits of the My Health Record system, an individual's multiple healthcare providers need to have timely and comprehensive access to their patients' medical history in which to better make a diagnoses and provide treatments.

1.4 Asking for a PIN, and requiring consumers to remember their PIN, will interrupt the clinical workflow and impede use of the record. Clinicians treating people who are unable to recall their PINs will not be able to view their patient's record. Both the clinician's and the consumer's time will be wasted while the consumer attempts to remember or locate their PIN.

1.5 In addition much valuable clinical work is undertaken for patients when they are not directly in the presence of their treating clinicians. For example, a general practitioner may receive important updated information from a specialist by letter such as a medication change or new investigation being required. Unless the patient was present to provide their record access control, the GP would be unable to check their MHR at that moment for important medication interaction information, or whether or not various investigations had already been done by another clinician. This would represent a great barrier to the realisation of benefits from the MHR system associated with medication safety and reducing unnecessary test duplication.

1.6 The proposal would also in practical terms effectively return the My Health Record to an opt-in participation model. This was noted by the AMA's Dr Chris Moy during the Senate hearings:

Basically, what happens then is the personal access code means that the only way anybody can access it in a reasonable situation, generally, is if the PIN is actually given to the individual, and it basically becomes opt-in then. The person has to go in there to change those details or actually has to be there every single time to be able to provide that information, so it makes it much more difficult.¹

1.7 Information on the My Health Record website provides clear concise information on how an individual can set a record access code and provide it to the healthcare providers they choose.

1.8 We therefore believe the current process is appropriate.

Recommendation 4

The committee recommends that data which is likely to be identifiable from an individual's My Health Record not be made available for secondary use without the individual's explicit consent.

1.9 We do not support this recommendation as this would be inconsistent with the Government's general opt-out approach to My Health Record.

1.10 The Australian Government has developed a framework to guide the secondary use of My Health Record system data for research, policy and planning purposes. This framework was developed in consultation with consumers, clinicians, medical researchers and industry experts.

1.11 The aim of the Framework is to be clear and open about the potential use of data.

1.12 The committee heard from organisations that appeared before the committee such as the Australian Health and Hospitals Association there is also considerable latent value to researchers in the information that will accumulate within the My Health Record system.

This has the potential to provide unique insights into population health issues and service utilisation patterns to the benefit of public providers and governments. Longer term, it also has the potential to gain longitudinal insights into how individuals' health evolves over time and how their interactions with the health system change in response.²

1.13 Coalition senators are therefore concerned that making the system 'opt-in' for research purposes would greatly diminish the potential data pool and limit the potential benefits highlighted above. It could also lead to distortions in data sets and individuals who chose to opt-in under this approach may not be a representative sample of the wider Australian public.

1 Dr Chris Moy, Member, AMA Federal Council, Chair, Federal Ethics and Medico-Legal Committee, AMA, *Committee Hansard*, 11 September 2018, p. 39.

2 Dr Linc Thurecht, Senior Research Director, Australian Healthcare and Hospitals Association, *Committee Hansard*, 11 September 2018, p. 8.

Recommendation 13

The committee further recommends that the Australian Government extend the opt-out period for the My Health Record system for a further 12 months.

1.14 Coalition Senators do not support this recommendation.

1.15 The program to create a My Health Record for all Australians by the end of 2018, unless individuals choose not to have one, is the culmination of ten years of planning, design and development carried out under several Health Ministers, current and former federal governments.

1.16 The legislation and program have been scrutinised by several independent enquiries, and shaped by national and international experience on the most appropriate national system for Australia with regard to our federated health system, mix of public and private healthcare, and sentiment of the Australian community.

1.17 The legislation to enable My Health Record to become an opt-out system passed the Parliament **unanimously** in 2015 and has received bipartisan support over this period. As recently as May this year, the Shadow Minister for Health Catherine King indicated support for an opt-out approach.

1.18 The opt-out approach has the support of every major health peak body including the AMA, RACGP and CHF, several of whom reaffirmed their support for an opt-out approach in their appearance before the committee. In addition all State and Territory Health Ministers unanimously reaffirmed their support for an opt-out approach as recently as the August COAG Health Council Meeting.

1.19 More than 6.1 million Australians already have a My Health Record and over 13,000 healthcare professional organisations are connected, including general practices, hospitals, pharmacies, diagnostic imaging and pathology practices.

1.20 The system has been in operation for over 6 years (commencing under the previous Labor Government with support of Liberals and Nationals), with My Health Record already improving the safety and healthcare management for individuals and healthcare providers.

1.21 The Government has also extended the opt-out period by one month to 15 November 2018 to provide additional time to educate consumers and healthcare providers about the benefits of having a My Health Record.

1.22 The Committee heard evidence provided by the Australian Digital Health Agency that it has implemented comprehensive multi-channelled campaign to reach all Australians through trusted clinical and community networks, that recognise the complexity of the messages and allows the opportunity to answer detailed questions. The ADHA also has plans in place to engage with vulnerable groups and those living in remote areas.

1.23 We therefore consider that a 12 month extension recommended by the Committee to be excessive and unnecessary.

1.24 It should also be noted the proposed legislative amendments announced by Minister Hunt to Section 17 of the My Health Record Act would require the System

Operator (ADHA) to permanently delete health information it holds for any consumer who has cancelled their My Health Record. This makes it clear that the Government will not retain any health information if a person chooses to cancel at any time. The record will be deleted forever.

1.25 This 'hard deletion' effectively means an individual's right to opt-out remains constant, even after the after the conclusion of a formal opt-out period. This was noted by Dr Chris Moy of the AMA when he appeared before the committee.

The other thing is I think the importance of the ability to hard delete the file on patient request is underestimated. I think it basically negates the need to extend the opt-out period, because, in effect, individuals can hop on and off the My Health Record based on their comfort level with privacy. That will vary over time. So, basically, the AMA's position is the amendments appear robust.³

Additional Comments by Coalition Senators

Recommendation 2

The committee recommends that the Australian Government amend the My Health Records Act 2012 to protect the privacy of children aged 14 to 17 years unless they expressly request that a parent be a nominated representative.

1.26 This is a sensitive policy issue and we believe it is premature to suggest specific recommendations on this matter at the present time.

1.27 There is likely to be a divergence of views within the community balancing the rights of minors with the view and expectations of parents and carers. It is also important to ensure such a change would not cause any unintended consequences resulting from this change.

1.28 We also consider it is important that there is consistency in the way policy is handled between My Health Record, Medicare and the State and Territories where possible.

1.29 Therefore, further engagement with all stakeholders is suggested before any changes should be considered.

Senator Lucy Gichuhi

3 Dr Moy, *Committee Hansard*, 11 September 2018, p. 32.

Labor Senators' Additional Comments

1.1 Labor Senators share the privacy and security concerns expressed in the Chair's report. In particular, we agree that the Government's botched implementation of an opt-out model means 'an unreasonable compromise has been struck between ensuring the utility of the system ... and safeguarding the privacy and safety of healthcare recipients'.

1.2 Labor Senators therefore urge the Government to commission an independent review of the My Health Record system by the Privacy Commissioner and the Office of the Australian Information Commissioner, which has itself called for further consideration of several privacy and security concerns.

1.3 In particular, the Privacy Commissioner and OAIC should consider:

- the appropriate balance between utility for clinicians, patients and others (such as carers), and privacy and security for individuals;
- the difficulty of ensuring informed consent in an opt-out model, and measures to encourage consumer engagement and informed choice;
- changes to default access settings that are necessary because of the shift to an opt-out model (from an opt-in model, where informed consent was assured);
- particular protections for vulnerable people, including minors aged 14-17 and families fleeing domestic violence; and
- further legislative, policy and system changes that are needed to achieve these aims.

1.4 In the meantime, the Government must suspend the opt-out rollout until the Privacy Commissioner and OAIC report, the Government makes necessary changes, and public confidence in this important reform is restored.

Senator the Hon Kristina Keneally

Senator Louise Pratt

Senator the Hon Lisa Singh

Senator Murray Watt

APPENDIX 1

Submissions and additional information received by the Committee

Submissions

- 1** Australian Privacy Foundation
- 2** Centre for Digital Business Pty Limited
- 3** CREATE Foundation
- 4** Population Health Research Network
- 5** Australasian Sleep Association
- 6** Optometry Australia
- 7** Mr Ian Bowie
- 8** Dr FM Janse van Rensburg
- 9** Name Withheld
- 10** Name Withheld
- 11** Confidential
- 12** Dr Oliver Frank
- 13** National Council of Single Mothers and their Children Inc
- 14** Health Intersections Pty Ltd
- 15** Future Wise
- 16** Consumers Health Forum of Australia
- 17** Australian Council of Trade Unions
- 18** People With Disabilities ACT

- 19 Women's Legal Service Queensland
- 20 Victorian Trades Hall Council
- 21 Electrical Trades Union of Australia
- 22 Department of Health and Department of Human Services
- 23 Health Consumers Alliance SA
- 24 Mr Paul Templeton
- 25 Maurice Blackburn Lawyers
- 26 Office of the Australian Information Commissioner
- 27 Police Federation of Australia
- 28 Rural Doctors Association of Australia (plus an attachment)
- 29 Doctors Reform Society
- 30 Royal Australian and New Zealand College of Psychiatrists
- 31 Australian Digital Health Agency
- 32 Multiple Sclerosis Australia
- 33 Allied Health Professions Australia
- 34 Australian Podiatry Association
- 35 Western Queensland Primary Health Network
- 36 Carers WA
- 37 Institute for Healthcare Transformation, Deakin University
- 38 Name Withheld
- 39 Name Withheld
- 40 Name Withheld

-
- 41 Queensland Nurses and Midwives' Union
- 42 Australian Federation of AIDS Organisations
- 43 Information and Privacy Commission NSW
- 44 Positive Life NSW and National Association for People with HIV
Australia
- 45 Federation of Ethnic Communities' Councils of Australia
- 46 Pharmaceutical Society of Australia
- 47 Royal Australian and New Zealand College of Radiologists
- 48 Women's Legal Service NSW
- 49 Australian Association of Social Workers
- 50 nib health funds limited
- 51 Mr Paul Power (plus two attachments)
- 52 Mrs Bianca Phillips, Mr Shane Genziuk, and Mr Jerome Owagage
- 53 Dr Juanita Fernando
- 54 Dr David More
- 55 Dr Robert Walker
- 56 Dr Thomas Rechnitzer
- 57 Dr Andrew Magennis
- 58 Dr Donald Rose
- 59 Dr Chris Culnane, A/Prof Benjamin Rubinstein, and Dr Vanessa Teague
- 60 Dr Stuart Jones
- 61 Mr Stephen Ma

- 62 Name Withheld
- 63 Orygen, The National Centre of Excellence in Youth Mental Health
- 64 Consumers of Mental Health WA
- 65 MIGA
- 66 National Rural Health Alliance
- 67 Wentworth Healthcare
- 68 Australian Medical Association (NSW)
- 69 Australian Primary Health Care Nurses Association
- 70 Australian Genomics
- 71 University of Sydney
- 72 Pharmacy Guild of Australia
- 73 Australian Psychological Society
- 74 Royal Australian College of General Practitioners
- 75 PHN Cooperative
- 76 Cancer Council Australia
- 77 Queensland Advocacy Incorporated (plus two attachments)
- 78 Australian Genetic Non-Discrimination Working Group, Regulatory Sub-Group (plus an attachment)
- 79 Australian Medical Association
- 80 Unions NSW
- 81 Medicines Australia
- 82 University of Melbourne

- 83 Health Care Consumers' Association Inc
- 84 Australian Nursing and Midwifery Federation
- 85 Lockstep Technologies
- 86 Australian Healthcare and Hospitals Association
- 87 The George Institute for Global Health
- 88 MSD Australia
- 89 Bayer Australia
- 90 Consumers e-Health Alliance
- 91 Aboriginal Health Council of Western Australia
- 92 Australian Injecting and Illicit Drug Users League
- 93 Gold Coast Domestic Violence Integrated Response
- 94 Rape and Domestic Violence Services Australia
- 95 Biotronik Australia Pty Ltd
- 96 Health Workers Union
- 97 Public Health Association of Australia
- 98 Queensland Office of the Information Commissioner
- 99 Research Australia
- 100 Australian College of Rural and Remote Medicine
- 101 Royal Flying Doctor Service
- 102 Children and Young People with Disability Australia
- 103 Northern Territory Office of the Information Commissioner
- 104 Youth Advocacy Centre

- 105 Australian Manufacturing Workers' Union
- 106 Royal Australasian College of Physicians
- 107 Australian Dental Association
- 108 Law Council of Australia
- 109 National Mental Health Consumer and Carer Forum
- 110 Breast Cancer Network Australia
- 111 Rare Cancers Australia
- 112 RMIT University Blockchain Innovation Hub
- 113 Mr Joshua Badge
- 114 Harm Reduction Victoria
- 115 Confidential
- 116 Confidential
- 117 Dr Robert Merkel
- 118 Dr Louis Wang

Additional Information

- 1 Brief: Reaching People with Mental Health Conditions, from Australian Digital Health Agency, received 25 September 2018
- 2 Further details on the financial relationship between the Consumers Health Forum of Australia (CHF) and the Australian Digital Health Agency, from CHF, received 27 September 2018

Answers to Questions on Notice

- 1** Answers to Questions taken on Notice during 11 September public hearing, received from Australian Medical Association, 27 September 2018
- 2** Answers to Questions taken on Notice during 17 September public hearing, received from Department of Health, 21 September 2018
- 3** Answers to Questions taken on Notice during 17 September public hearing, received from Health Intersections Pty Ltd, 21 September 2018
- 4** Answers to Questions taken on Notice during 20 September public hearing, received from Department of Health, 11 October 2018
- 5** Answers to Questions taken on Notice during 20 September public hearing, received from Australian Digital Health Agency, 11 October 2018

Correspondence

- 1** Correspondence clarifying evidence given at Canberra public hearing on 11 September 2018, received from Australian Healthcare and Hospitals Association, 17 September 2018
- 2** Correspondence clarifying statements made at Canberra public hearing on 20 September 2018, received from Ms Sue Dunlevy, 4 October 2018

APPENDIX 2

Public hearings

Tuesday, 11 September 2018

Parliament House, Canberra

Witnesses

PHELPS, Professor Kerryn, Private capacity

Australian Healthcare and Hospitals Association

THURECHT, Dr Linc, Senior Research Director

HADDOCK, Dr Rebecca, Director, Deeble Institute for Health Policy Research

Australian Privacy Foundation

ROBERTSON-DUNN, Dr Bernard, Chair, Health Committee

MERKEL, Dr Robert, Private capacity

POWER, Mr Paul, Private capacity

BAIN, Professor Chris, Private capacity

BRAGGE, Associate Professor Peter, Director of Health Problems,
BehaviourWorks Australia, Monash Sustainable Development Institute, Monash
University

Australian Medical Association

MOY, Dr Chris, Member, AMA Federal Council; Chair, Federal Ethics and Medico-
Legal Committee

TOY, Mr Luke, Director, Medical Practice Section

Australian Medical Association, New South Wales

LIM, Dr Kean-Seng, President

Royal Australian College of General Practitioners

PINSKIER, Dr Nathan, Chair, RACGP Expert Committee eHealth and Practice
Systems

Carers Australia

CRESSWELL, Ms Ara, Chief Executive Officer
ELDERTON, Ms Susan, National Policy Manager

Monday, 17 September 2018

Parliament House, Canberra

Witnesses

SHETLER, Mr Paul, Private Capacity

Consumers Health Forum of Australia

WELLS, Ms Leanne, Chief Executive Officer
HEWSON, Mr Dean, Digital Health Adviser

Health Intersections Pty Ltd

GRIEVE, Mr Grahame, Principal

Australian Council of Trade Unions

McCALLUM, Mr Lance, National Campaign Coordinator
WATTS, Mr Christopher, Social Policy Advisor

Health Services Union

HAYES, Mr Gerard, National Secretary
SVENDSEN, Ms Leigh, Senior National Industrial Officer

Electrical Trades Union of Australia

GAULD, Mr Trevor, National Policy Officer

Law Council of Australia

BAILES, Mr Morry, President
GANOPOLSKY, Ms Olga, Chair, Privacy Law Committee, Business Law Section
MOLT, Dr Natasha, Director of Policy
KAYLER-THOMSON, Ms Wendy, Chair, Family Law Section

Maurice Blackburn Lawyers

BALLANTYNE, Mr Thomas, Head of the Victorian Medical Law Practice

Department of Health

EDWARDS, Ms Caroline, Deputy Secretary

RISHNIW, Ms Tania, First Assistant Secretary, Portfolio Strategies Division

KELLEHER, Mr Brian, Assistant Secretary, Digital Health Branch, Portfolio Strategies Division

Australian Digital Health Agency

KELSEY, Mr Tim, Chief Executive Officer

McMAHON, Ms Bettina, Chief Operating Officer

O'CONNOR, Mr Ronan, Executive General Manager, Core Services Systems Operations

MAKEHAM, Clinical Professor Meredith, Chief Medical Adviser

Office of the Australian Information Commissioner

FALK, Ms Angelene, Australian Information Commissioner and Privacy Commissioner

DRAYTON, Ms Melanie, Acting Deputy Commissioner

GHALI, Ms Sarah, Acting Assistant Commissioner, Regulation and Strategy

Thursday, 20 September 2018

Parliament House, Canberra

Witnesses**Department of Health**

EDWARDS, Ms Caroline, Deputy Secretary

RISHNIW, Ms Tania, First Assistant Secretary

KELLEHER, Mr Brian, Assistant Secretary, Digital Health Branch, Portfolio Strategies Division

Australian Digital Health Agency

KELSEY, Mr Tim, Chief Executive Officer

McMAHON, Ms Bettina, Chief Operating Officer

O'CONNOR, Mr Ronan, Executive General Manager, Core Services Systems Operations

MAKEHAM, Professor Meredith, Chief Medical Adviser