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 Pinskier, 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 Rensberg, *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 Kerryn Phelps, *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 Pinskier, *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.