Report

Referral

1.1 On 9 August 2017, the following matter was referred to the Senate Finance and Public Administration References Committee (the committee) for inquiry and report by 16 October 2017:

> Circumstances in which Australians' personal Medicare information has been compromised and made available for sale illegally on the 'dark web', including:
>
> (a) any failures in security and data protection which allowed this breach to occur;
>
> (b) any systemic security concerns with the Department of Human Services Health Professional Online Services system;
>
> (c) the implications of this breach for the roll out of the opt-out My Health Record system;
>
> (d) Australian government data protection practices as compared to international best practice;
>
> (e) the response to this incident from government – both ministerial and departmental;
>
> (f) the practices, procedures, and systems involved in collection, use, disclosure, storage, destruction, and de-identification of personal Medicare information;
>
> (g) the practices, procedures, and systems used for protecting personal Medicare information from misuse, interference, and loss from unauthorised access, modification, or disclosure; and
>
> (h) any related matters.[1]

Conduct of the inquiry

1.2 Details of the inquiry were placed on the committee's website at: www.aph.gov.au_fpa. The committee directly contacted relevant organisations and individuals to notify them of the inquiry and invite submissions by 31 August 2017. Submissions received by the committee are listed at Appendix 1.

1.3 A public hearing was held in Canberra on 15 September 2017. A list of the witnesses who gave evidence at the public hearing is available at Appendix 2. The Hansard transcript may be accessed through the committee's website.

---

1 *Proof Journals of the Senate*, No 50 – Wednesday 9 August 2017, p. 1638.

Background

1.4 On Tuesday 4 July 2017, *The Guardian Australia* reported that a darknet trader is selling Medicare patient's card details 'on request', and had sold at least 75 records since October 2016.[2] *The Guardian Australia* verified the seller is legitimate, and considered by darkweb users to be a 'highly trusted vendor' on a popular darknet site.[3]

1.5 The matter of potential identity fraud arising from stolen Medicare card numbers was also raised by at the Community Affairs Legislation Committee's Senate Estimates hearing on 21 October 2015.[4] At the hearing the Department of Human Services (DHS) confirmed 369 instances of possible identity theft from individuals; a small number of instances arose in 2014, with the remainder occurring progressively over the first half of 2015.

1.6 The Medicare card has also come to have an important secondary function in that it is used as one form of proof of identity under the Document Verification Service (DVS) scheme.[5] The Medicare card represents 25 points of the 100 points required to verify a person's identity. The 100 point check policy was adopted by the Australian Government to combat financial transaction fraud.[6]

Overview of the report

1.7 There are two separate aspects to this report. The first part of the report provides a background to the Health Professionals Online Service (HPOS) and My Health Record systems. The second part of the report considers issues arising out of the misappropriation of the Medicare card numbers.

---

2 The darkweb refers to web content that is only accessible with the use of an https address or encrypted software, such as TOR or peer-to-peer. The darknet can use overlay networks which encrypt internet communications, making them anonymous and hiding the IP address. A darknet trader is someone anonymously operating a business on the darkweb.

3 Paul Farrell, *'The Medicare machine: patient details of "any Australian" sold on darknet'*, *The Guardian Australia*, available at https://www.theguardian.com/australia-news/2017/jul/04/the-medicare-machine-patient-details-of-any-australian-for-sale-on-darknet, (accessed on 15 August 2017).

4 *Committee Hansard*, 21 October 2015, pp. 154-156.

5 The Document Verification Service (DVS), managed by the Attorney-General's Department, is an online system that allows organisations, including businesses with a reasonable need to use a government identifier, to take information from a person's identity document with the person's consent, and compare that record against the corresponding record of the document's issuing agency. The checks are conducted in real-time to inform decisions that rely on the confirmation of a person's identity. The DVS is a key tool for organisations that are seeking to prevent dealings with any person who may be using fraudulent identities. See Attorney-General's Department pamphlet, *Document Verification Service*, available at: https://www.ag.gov.au/RightsandProtections/Identity/Security/Pages/DocumentVerificationService.aspx (accessed on 21 August 2017).

6 For example, *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)*, s.4 and Pt 2.

DHS and digital service delivery

1.8 DHS stated that it is moving towards digital service delivery so that individuals can manage their interaction with the department through easy-to-use, secure, integrated digital channels.[7]

1.9 DHS advised that access to Medicare card numbers is required by health professionals in order to verify the eligibility of a patient to receive Medicare services, and to lodge bulk bill or electronic payment claims from the medical practice:

> Health care professionals access Medicare card numbers in order to confirm eligibility so that patients who do not have their card with them at the time of service can still access Medicare services…
>
> Individuals must be eligible for Medicare in order to receive Medicare subsidised services. It is important to note that individuals can still access health services if they are not eligible for Medicare, or if a health professional cannot confirm their eligibility. However, the health professional will not be able to bulk bill the patient or lodge a Medicare claim on their behalf.

1.10 DHS further advised that the integrity of the payments processed by the department relies largely upon health professionals determining and claiming correctly in relation to the services they provide. Health care providers are subject to the regulatory regime of the *Health Insurance Act 1973 (Cth),* and the *National Health Act 1953 (Cth)*. The objective of provider compliance is to ensure the correct payment of benefits to an eligible patient for an eligible service by an eligible health practitioner.[8]

Health Professional Online Service (HPOS)

1.11 The Health Professional Online Service (HPOS), introduced in 2009, is managed by DHS. HPOS provides health professionals with a dedicated web portal giving real-time access to a number of online services provided by the DHS, including looking up or verifying a patient's Medicare number.

1.12 HPOS was introduced as a way of ensuring that, in an emergency, people could get treatment immediately even if they did not have their Medicare card with them. It allows a health provider to acquire a card number on the basis of a name and date of birth. HPOS is utilised approximately 45,000 times per day from locations across Australia. Access to a Medicare card number does not give access to an individual's medical or clinical records.[9]

---

7 Department of Human Services, *Submission 7*, p. 4.

8 Department of Human Services, *Submission 7.*

9 Media Release: *Independent review of health provider's accessibility to Medicare number,* The Hon Alan Tudge MP, Minister for Human Services, and The Hon Greg Hunt MP, Minister for Health, 10 July 2017 https://www.mhs.gov.au/media-releases/2017/07010-independent-review-health-service-providers-accessibility-medicare-card-numbers, accessed 18 August 2017; see also, Dr Bartone, Australian Medical Association, *Proof Committee Hansard,* 15 September 2017, p. 3.

1.13 To access HPOS, health professionals must authenticate their credentials by either applying for an individual Public Key Infrastructure (PKI) certificate or creating a Provider Digital Access (PRODA) account. Where the PKI system is used to access HPOS, the user logs onto a computer which has uploaded the DHS specialist software and PKI certificate, and enters a correct Personal Identification Code. The system allows for site certificates to be installed on practice management software or on an organisation's internet browser, and once logged on, can be used by anyone using the software or practice network, without any requirement for individual sign-in.

1.14 In the case of PRODA, each health provider must create an individual PRODA account by providing a personal and unique email address, with personal identity verified in accordance with the DVS process. To access PRODA, the user must enter their username and password, and a separate unique verification code. The verification code is sent by either an SMS, email, or generated on the PRODA mobile application.[10]

My Health Record

1.15 The Australian Digital Health Agency (ADHA) is responsible for the systems operations of My Health Record, and for the implementation of the Government's National Digital Health Strategy.[11] The ADHA emphasised there is no direct or technical connection between the HPOS system and My Health Record.[12]

1.16 My Health Record is a secure national online summary of an individual's health information which can be made available electronically by consent to doctors, hospitals and other health care providers. Currently My Health Record is a voluntary 'opt-in' system. In May 2017, the federal government announced the transition of the 'opt-in' model of My Health Record, to an 'opt-out' model by the end of 2018, a move unanimously supported by the Council of Australian Governments:

> The transition to opt out will bring forward benefits many years sooner than the current opt-in arrangements. It is the fastest way to realise the significant health and economic benefits of My Health Record through, for example, reduced hospital admissions, reductions in adverse drug events, reduced duplication of diagnostic tests, better coordination of care for

10 Professor Peter Shergold AC, Dr Bastian Seidel, President, Royal Australian College of General Practitioners, Dr Michael Gannon, President, Australian Medical Association, and Dr Kean-Seng Lim, Australian Medical Association, *Discussion Paper, Independent Review of Health Providers' Access to Medicare Card Numbers*, Department of Human Services, available at: https://www.humanservices.gov.au/organisations/health-professionals/subjects/independent-review-health-providers-access-medicare-card-numbers (accessed on 30 August 2017).

11 National Digital Health Strategy – *Safe, seamless and secure: evolving health care to meet the needs of modern Australia*, approved by the Council of Australian Governments in August 2017: https://digitalhealth.gov.au/australias-national-digital-health-strategy; accessed 21 September 2017.

12 *Proof Committee Hansard*, 15 September 2017, p. 15.

> people seeing multiple heath care providers and, of course, more control in the hands of the patient and the citizen of their health and wellbeing.[13]

1.17 ADHA advised that the My Health Record system has been supported by a range of health care provider leaders, including the Australian Medical Association (AMA), and the Royal Australian College of General Practitioners (RACGP), and the Pharmacy Guild of Australia:

> These peak bodies have entered into compacts with the Government on behalf of the health care providers they represent recognising that electronic health records can play a crucial role in supporting healthcare outcomes. These organisations are committed to the system and are encouraging health care providers to adopt the use of My Health Record system into daily practice.[14]

Conjecture as to the potential cause to the misappropriation of Medicare card numbers

1.18 The facts of the misappropriation of the Medicare card numbers are not known as the matter is currently under investigation by the Australian Federal Police.[15] However, a number of submissions surmised as to possible causes. Future Wise and the Centre for Internet Safety contended that the data breach most likely arose out of an authorised user accessing the HPOS for an unauthorised purpose for gain.[16] A variation on this theme was that the breach was likely to have arisen out of stolen HPOS authentication credentials, and was not as a result of the hacking of HPOS.[17]

1.19 Mr Paul Power of eHealth Privacy noted that the design of the HPOS system was such that it would not be possible to determine if the breach of Medicare card numbers was as the result of deliberate computer hacking, and that it cannot be said with authority that the breach was by an authorised user based only on the identification of a personal computer as being the source of the breach.[18]

1.20 At the public inquiry DHS advised the committee that the Medicare card number breach was not a cyber-attack, and nor was it an internal DHS employee accessing the system inappropriately:

---

13 Australian Digital Health Agency, *Proof Committee Hansard*, pp. 16 – 17.

14 Australian Digital Health Agency, *Submission 4*, p. 2. See also, Royals Australian College of General Practitioners, *Submission 3;* Australian Medical Association, *Submission 11*.

15 Department of Human Services, *Submission 7*, p. 7; see also *Proof Committee Hansard*, 15 September 2017.

16 Future Wise, *Submission 9;* Centre for Internet Safety, *Submission 1*.

17 Centre for Software Practice, University of Western Australia, *Submission 12.*

18 Paul Power, eHealth Privacy Australia, *Submission 8.*

> [The breach] appears to have been an external person or persons making an illegitimate use of a legitimate channel by which healthcare providers access Medicare numbers when they need them.[19]

1.21 The AMA noted that the breach of the Medicare card numbers, must be kept in proportion particularly as there is no evidence that patients' health information was compromised:

> While not seeking to downplay the significance of the alleged sale of Medicare numbers, the allegations must be put into perspective. The AMA understands that 75 Medicare card numbers were sold on the dark web and this needs to be put into context. Every day there are 45,000 provider interactions with the HPOS, an estimated 27,000 HPOS confirmations of Medicare details and in the last year 14.8 million GP services claimed against Medicare. There is no evidence of a systemic problem and no evidence that patients' health information has been compromised.[20]

The possible motive for the misappropriation of Medicare card numbers

1.22 A number of submitters highlighted the value of the Medicare card numbers was in the card's secondary use as an aspect of proof of identity under the Attorney-General's DVS.[21] Dr David Glance of the University of Western Australian Centre for Software practices observed:

> The small number of sales of Medicare information indicated on the vendor's profile on the Dark Web Market AlphaBay suggests that access to this information would have been for targeted use in identity fraud and/or doctor shopping for scripts. A significant issue with the Medicare card is that is it used as identification in situations that are unrelated to health care.[22]

1.23 Both the AMA and the RACGP observed that the Australian people have a role in reducing the risk identity theft.[23] The RACGP observed:

> While the design and functionality of systems, procedures, and practices for protecting Medicare information are important, the Australian public have a role in reducing the risk of identity theft by safeguarding their information. Investment in public awareness and education campaigns on personal

19 Department of Human Services, *Proof Committee Hansard,* p. 16.

20 Australian Medical Association, *Submission 11*, p. 2.

21 Royal Australian College of General Practitioners, *Submission 3;* Department of Human Services, *Submission 7;* Centre for Software Practice, University of Western Australia, *Submission 12.*

22 Centre for Software Practice, University of Western Australia, *Submission 12.*

23 Dr Kidd, Australian Medical Association, *Proof Committee Hansard,* 15 September 2017, p. 2; Dr R Hosking, Royal Australian College of General Practitioners, *Proof Committee Hansard,* September 2017, p. 2.

> information protection strategies will assist in strengthening the security of Medicare information.[24]

1.24 DHS emphasised that access to a Medicare card number does not give access to personal health information or Medicare online accounts:

> The Medicare card can be used to help verify an identity and, like other evidence of identity credential, is therefore susceptible to theft for identity fraud and other illicit activities. However, it is important to note that the Medicare card alone does not provide access to personal health information or Medicare online accounts.[25]

Data protection issues

1.25 A range of data protection issues were identified. Submissions identified design vulnerabilities in the HPOS's authentication processes.[26] Mr Paul Power and Dr Robert Merkel noted the exacerbating factor that a significant number of health care practices have poor office security practices at the everyday level.[27] Mr Power and Dr Merkel also noted the very large number of access points to HPOS increased its vulnerability, and that it is not possible to achieve the requisite level of data security at each and every access point for the HPOS system to be secure.[28] Future Wise noted the 'insider threat' – that is, an authorised user accessing the system for an unauthorised purpose – is very difficult to prevent.[29]

1.26 The AMA noted that any changes in security protection must err in favour of access to care, expressing concern that a disproportionate response may impose new layers of red tape on medical practices. The AMA considered the current arrangements for HPOS to be working relatively well. The AMA suggested it would be useful to address the complicated and confusing nature of the multiple policies and terms and conditions documents that PKI holders are expected to comply with, while noting that the PRODA system is more secure.[30]

1.27 RACGP similarly supports any measure that strengthens the security of HPOS, but argued that this needs to be balanced against reasonable administrator access:

> RACGP supports the continuation of a system where health-care providers, and in particular, administrators can safely access Medicare details of a patient via a system such as HPOS. Restricting access to Medicare

---

24 Royal Australian College of General Practitioners, *Submission 3,* p. 3, paragraph g.

25 Department of Human Services, *Submission 7*, p. 4.

26 For example, Future Wise, *Submission 9;* see also *Proof Committee Hansard*, 15 September 2017.

27 For example, Paul Power, eHealth Privacy, *Submission 8;* see also *Proof Committee Hansard*, 15 September 2017.

28 *Proof Committee Hansard*, 15 September 2017.

29 Future Wise, *Submission 9.*

30 Australian Medical Association, *Submission 11*.

> information could compromise the provision of essential health care if patients are unable to confirm evidence of eligibility. This poses a significant risk to Australia's most vulnerable people.[31]

Implications for My Health Record roll-out

1.28 Some people were concerned that the compromise of some Medicare data numbers potentially undermined the public's confidence in Australian government digital services, which may slow the roll-out.[32] Future Wise expressed concern that the issue of the re-identification of de-identified personal information may pose difficulties.[33]

1.29 The AMA and RACGP both state that they do not see any implications for the My Health Record roll-out arising from compromised Medicare card numbers, on the basis that the Medicare card number itself does allow access to My Health Record. Both the AMA and RACGP noted the multiple layers of security for My Health Record, and the strict access controls.[34] The AMA strongly emphasised that the Medicare card as an identifier is a completely separate system from My Health Record authentication processes.[35] The AMA contends:

> It is important as we move towards an opt-out My Health Record system, that we can be reassured that patient information is protected. There are multiple layers of security around this information, and a person's Medicare card number is just one part of that. It's unfortunate that media reports incorrectly link the sale of Medicare card details to the security of My Health Record because of the potential this has to undermine public confidence it.[36]

1.30 Ms Caroline Edwards, Deputy Secretary, Health and Aged Care, DHS, emphasised that the issue of the compromised Medicare card numbers has no implications for My Health Record:

> I might just add one thing: access to a Medicare number is not in any way access to any clinical information. It does not allow access to My Health Record or any clinical information whatsoever. It fact, it doesn't even allow

---

31 Royal Australian College of General Practitioners, *Submission 3.*

32 Centre for Internet Safety, *Submission 1;* Office of the Australian Information Commissioner, *Submission 2;* Professor Danuta Mendelson and Dr G Wolf, Deakin University, *Submission 6;* Shaun McCarthy, Associate Professor Bronwyn Hemsley, University of Newcastle, and Professor Susan Balandin, Deakin University, *Submission 10.*

33 Future Wise, *Submission 9.*

34 Australian Medical Association, *Submission 11*; Royal Australian College of General Practitioners, *Submission 3.*

35 Dr Kidd, Australian Medical Association, *Proof Committee Hansard*, 15 September 2017, pp. 2, 3.

36 Dr Kidd, Australian Medical Association, *Proof Committee Hansard*, 15 September 2017, pp. 1–2.

> you to claim a rebate into your own account, if you have got one fraudulently.[37]

1.31 Mr Tim Kelsey, Chief Executive Officer, ADHA, agreed that the issue of the compromised Medicare card numbers was quite separate from My Health Record.[38]

Compliance

1.32 DHS notes that the integrity of the payments processed by the Department relies largely upon health professionals to determine and claim correctly in relation to the Medicare services they provide, with compliance being a shared responsibility between DHS and the Department of Health. DHS advised that the object of provider compliance is to ensure the correct payment of Medicare benefits to an eligible patient for an eligible service by an eligible practitioner, a process governed by the *Health Insurance Act 1973 (Cth)* and the *National Health Act 1953 (Cth).*[39]

1.33 The ADHA advises that healthcare provider organisations are only authorised to access the databases if they are providing health care to that individual, noting that criminal and civil penalties apply to health care providers that deliberately access an individual's health records without authorisation. The ADHA also notes that the Cyber Security Centre continually monitors the system for evidence of unauthorised access.[40]

1.34 However, submitters contended that it is apparent that from the fact of the Medicare card number breach that departmental oversight and preventative cyber security and business accountability processes have failed:[41] the fact of the breach is evidence in itself of a systems failure.[42] Mr Paul Power of eHealth Privacy noted an Australian Cyber Security Centre Report concerning the threat in relation to botnets:

> [S]uch threats that happen over a protracted period of time, where they (botnets) operate for months undetected and, once they fulfil their role, they go away.[43]

1.35 A number of submitters contend that reliance on civil and criminal penalties is to little or no avail, penalties being: after the event;[44] of no assistance to individual's whose privacy has been breached;[45] assumes the breach will be found[46], or the breach

---

37 The Department of Human Services, *Proof Committee Hansard,* 15 September 2017, p, 22; see also p. 26.

38 Australian Digital Health Agency, *Proof Committee Hansard,* 15 September 2017, p. 16.

39 Department of Human Services, *Submission 7*, p. 15.

40 Australian Digital Health Agency, *Submission 4.*

41 Centre for Internet Security, *Submission 1.*

42 Paul Power, eHealth Privacy, *Submission 8*; see also *Proof Committee Hansard*, 15 September 2017.

43 Paul Power, eHealth Privacy, *Proof Committee Hansard*, 15 September 2017, p. 13.

44 Professor Danuta Mendelson, and Dr Gabrielle Wolf, Deakin University, *Submission 6;* Future Wise, *Submission 9.*

45 Future Wise, *Submission 9.*

is identified in sufficient time (not years later) to warrant investigation;[47] is unlikely to deter those intending to breach the system;[48] assumes the perpetrators are located and prosecuted;[49] and, assumes the perpetrators are within the purview of Australian domestic law.[50] One submitter noted:

> [D]etecting bad behaviour doesn't mean you have prevented it.[51]

Privacy

1.36 Submitters noted the application of the *Privacy Act 1988 (Cth)* (the Privacy Act) to the collection and storage and disclosure of individual's health information.[52] DHS advised that, in addition to the Privacy Act and the Australian Privacy Principles, it is also bound by the secrecy provisions of e.g. the *Health Insurance Act 1973 (Cth),* and the *National Health Act 1953 (Cth).*[53]

1.37 DHS noted that Australian National Audit Office Audit No. 27 *Integrity of Medicare Customer Data*, found that DHS has a comprehensive framework for managing Medicare customer privacy.[54]

Committee view

1.38 The committee notes the Government has commissioned a Review of health professionals' access to Medicare card numbers via the HPOS system and the telephone channel. The committee notes that the Review is due to report to the Government by 30 September 2017.

1.39 The committee acknowledges that the secondary role of Medicare card numbers as an aspect of proof of identity under the DVS makes the card valuable for identity theft. While the committee considers this to be a serious issue, it also notes that there appears to be considerable support to the continued use of the Medicare card as an identity document. DHS has advised the committee that the preliminary view of the Review is the Medicare card should be retained as a proof of identity document.[55]

---

46 Paul Power, eHealth Privacy, *Submission 8*; see also *Proof Committee Hansard*, 15 September 2017.

47 Professor Danuta Mendelson, and Dr Gabrielle Wolf, Deakin University, *Submission 6.*

48 Professor Danuta Mendelson, and Dr Gabrielle Wolf, Deakin University, *Submission 6.*

49 Professor Danuta Mendelson, and Dr Gabrielle Wolf, Deakin University, *Submission 6.*

50 Professor Danuta Mendelson, and Dr Gabrielle Wolf, Deakin University, *Submission 6;* see also *Proof Committee Hansard*, 15 September 2017.

51 Paul Power, eHealth Privacy, *Proof Committee Hansard,* 15 September 2017, p. 12.

52 Office of the Australian Information Commissioner, *Submission 2*; Professor Danuta Mendelson, and Dr Gabrielle Wolf, Deakin University, *Submission 6*; Department of Human Services, *Submission 7.*

53 Department of Human Services, *Submission 7*, pp 11 – 15.

54 Department of Human Services, *Submission 7*, pp. 11 – 15.

55 *Committee Hansard,* 15 September 2017, p. 26.

1.40 The committee is aware of the wider impact on the community were the Medicare card to be withdrawn as a proof of identity document. The committee also notes that the secondary use of the Medicare card as a proof of identity document under the DVS falls within the Attorney-General's portfolio. The committee is, however, satisfied that the potential for identity theft by means of a stolen Medicare card number does not result in an individual's health information being accessed, as the Medicare card system is a discrete system completely separate from My Health Record, with My Health Record requiring a different authentication process.

1.41 The committee considers the issue to be one of striking a balance between the security of HPOS and My Health Record, against the utility of these systems for health care professionals. The committee notes the comments of the AMA:

> While it is important that the security of Medicare information is better protected, the AMA wants to ensure that any response from the government to safeguard it is proportional to the risk and does not increase the administrative burden on practitioners or practices or introduce any unnecessary administrative barriers to care, particularly for the disadvantaged patients and their access to timely Medicare funded or bulk-billed consultations.[56]

1.42 The committee notes with great concern that the issue of potential identity fraud has arisen before, and that DHS was questioned about it at the Community Affairs Legislation Committee's Senate Estimates hearing on 21 October, 2015. The submissions from the department do not indicate that this risk is fully understood, or has been addressed.

1.43 The committee notes that it was a media organisation investigation rather than internal government monitoring that identified the security breach. The committee is also concerned by the department's failure to promptly notify affected individuals once the breach was identified. The committee considers that responsible data management requires prompt and timely disclosure when security breaches occur, and proactive engagement with investigative agencies to facilitate such an outcome wherever possible.

1.44 The committee is cognisant of the fact that the issue of the alleged sale of Medicare card numbers on the darknet is currently under investigation by the Australian Federal Police. Accordingly, the committee considers it not appropriate to comment further on this issue.

Senator Jenny McAllister

Chair

56 *Proof Committee Hansard,* 15 September 2017, p. 1.