

5 September 2017

Professor Peter Shergold AC



By email:
mca.review@humanservices.gov.au

Dear Professor Shergold,

Submission to Independent Review of Health Providers' Access to Medicare Card Numbers

We welcome this opportunity to provide a written submission to the Independent Review. The ePA has a keen interest in ensuring that eHealth data is private and secure, ensuring fitness for purpose and the protection of confidential information. We support initiatives to review access to Australians' Medicare Card numbers.

Yours sincerely,

Dr Juanita Fernando and Mr Paul Power
Principals
eHealth Privacy Australia

Section 1: Our response

The eHealth Privacy Australia (ePA) note that the scope of this Review considers the balance between access to a patient's Medicare number for health professionals to confirm Medicare eligibility with the security of patients' Medicare card numbers. So a reworked version of the ePA response to the *Senate Finance and Public Administration References Committee's inquiry into the circumstances in which Australians' personal Medicare information has been compromised and made available for sale illegally on the 'dark web'* that addresses the specific Terms of Reference is outlined in Section 2 for your consideration. The ePA principals would be delighted meet with you, at your convenience, to discuss our submission in more detail.

Medicare card data underpins Australia's My Health Record, which is an online summary of health information intended to help clinicians know about peoples' allergies, current conditions and treatments online, for example, anywhere and at any time. This means the information it holds must be up-to-date, reliable, accurate, concise, easy to find and trusted by patients. All of these system benefits come about **after** an eHealth system is private and secure. The current Medicare card system, compromised as it is, can never achieve this goal in its current implementation.⁽¹⁻²⁾

The Medicare numbers, along with other identification, can currently be used to open bank accounts, obtain a passport or a driving license. They might also be used to compromise credit or debit records, steal or establish online accounts. Medicare numbers can be used to obtain unauthorised information by the mass media or others for publication purposes. And the list goes on. Most people, governments and organisations are unaware that private health data has been compromised by unauthorised people, for many years, if ever, such as occurred with the 2016 Yahoo hacks.

Individual users are not advised of unauthorized access to their private information on the Medicare card system either. Incorrect information, can be added to a Medicare card during a fraud or other criminal activity, which can foster unintended consequences.⁽³⁾ Trust concerns, not privacy or security worries, are at the heart of unsuccessful Australian digital health implementations. The risks outlined here undermine Australians' trust in the system.

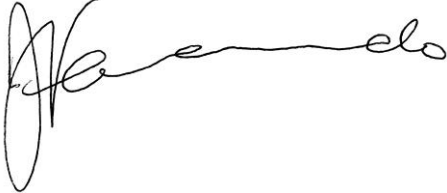
Section 2 illustrates that secondary uses of the Medicare card, such as providing a means of personal identification, should be avoided. The risk associated with providing the this card data online, using PKI (Public Key Encryption) and/or PRODA (Provider Digital Access) for access to centralised databases with 600,000 access points is significant. The risk is so extensive that HPOS use should be limited to its primary purpose - healthcare.

The ePA also ask the Review to recommend the introduction of an eHealth card based on international best practice, such as encrypted eHealth cards for each person, carrying master data or similar, as currently occurs in Germany. The Australian Government Department of Human Services should consider implementing the

system in the medium to longer term to ensure the security and protection of the information of Australians.

The ePA request that the Australian Government Department of Human Services and the Department of Health work to build trust in all parts of eHealth system by being more transparent and timely in the reporting of issues.

Yours sincerely



Dr Juanita Fernando

References

1. Scholefield, A. (2017) Worst health policy No. 5 - My Health Record. Australian Doctor, 4 September. <https://www.australiandoctor.com.au/news/latest-news/worst-health-policy-no-5-my-health-record>
2. Culnane, C, Rubinstein, B & TeagueV (2017) Submission to the Senate Finance and Public Administration References Committee's inquiry into the circumstances in which Australians' personal Medicare information has been compromised and made available for sale illegally on the 'dark web'. http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Finance_and_Public_Administration/medicareinformation/Submissions Aust Gov Department of Human Services (2017) Discussion Paper: Independent Review of Health Providers' Access to Medicare Card Numbers, <https://www.humanservices.gov.au/organisations/health-professionals/subjects/independent-review-health-providers-access-medicare-card-numbers> , August; p12
3. Parliament of Australia (2017) Question on Notice, Number 920, Health Portfolio, Senate Estimates Committee, Tabled documents 29 May. http://www.aph.gov.au/Parliamentary_Business/Senate_Estimates/clacctte/estimates/bud1718/Health/index

Section 2: Response to the Review's Terms of Reference

1. Identified area of potential weakness associated with policy, process, procedures and **systems** in relation to accessibility of Medicare numbers-
2. Scope of breach, and
3. Retaining the Medicare card as evidence of identity in the community

1. DETAIL

1.1 *“Identified area of potential weakness associated with systems”*

There are approximately 660,000 access points registered for legitimate access to Medicare data via HPOS⁽¹⁾, any one of which can access any record in the database: the system is fundamentally indefensible.

Even if every one of the 660,000 access points were 99.999% secure, the security of the whole system would be 0.1%⁽²⁾. This means there is a probability of 99.9% that it would be compromised, exposing any and all records.

1.2 *Scope of breach*

The evident availability of Medicare data, available on request by Guardian journalist, Paul Farrell⁽³⁾ and SBS journalist, James Elton-Pym⁽⁴⁾ is a failure in security and data protection.

If, for example, only 75 records were compromised, the probability that the Guardian journalist's and SBS journalist's just happen to be among those 75 is one billionth of one per cent⁽⁵⁾.

Or, putting it another way, in order for the probability of both Guardian journalist's and SBS journalists just happening to be among the records compromised to be 50%, the number of records compromised must be 17 million⁽⁶⁾.

2. ACCESS POINTS TO HPOS ARE TYPICALLY MEDICAL PRACTICES.

2.1 There are two methods of accessing HPOS, via

- (i) Public Key Infrastructure (PKI) certificate, or
- (ii) Provider Digital Access (PRODA)

Both methods (i) and (ii) are vulnerable to attack, due to the large number of access points, requiring unachievably high levels of security for each and every access point for the whole system to be secure.

2.2 But the reality is much worse, due to routine security weaknesses:

- i. A commonly used medical software product bulletin refers, in a recent edition, to the practice of storing certificates in shared folders on networks for convenience.
- ii. Prior to January 2017, a commonly used medical software stored certificates in a database table on the server, rather than in the prescribed encrypted certificates store.
- iii. Remote access is often effected by "port forwarding" the remote desktop port on the network router to the designated PC on the network. Port forwarding provides virtually no security and can be detected and collected by a hacker scanning for open ports exposed to the internet.
- iv. The PKI PIC (Personal Identification Code) password is weak (only 8 characters) and easily crackable.
- v. PKI certificates and passwords are sent by normal postal services (albeit separately, but easily intercepted).
- vi. PKI certificates can be reissued: there is no evidence of an effective process for revoking the supposedly replaced certificates. Practices are known to be able to use both original and replacement certificates at the same time.

2.3 What does this mean for the possibility of detecting the person or persons responsible for the Medicare data breach?

It means it is virtually impossible to determine who is responsible.

For, although we may be able to identify one or many legitimate access points as a source of breach, there is no reasonable way to rule out the possibility that such sources have been hacked.

A consequence is that tracing the source of the illegitimate request to a single PC does not mean that other PCs, possibly harvested by the same hacker, are not also sources of illegitimate requests.

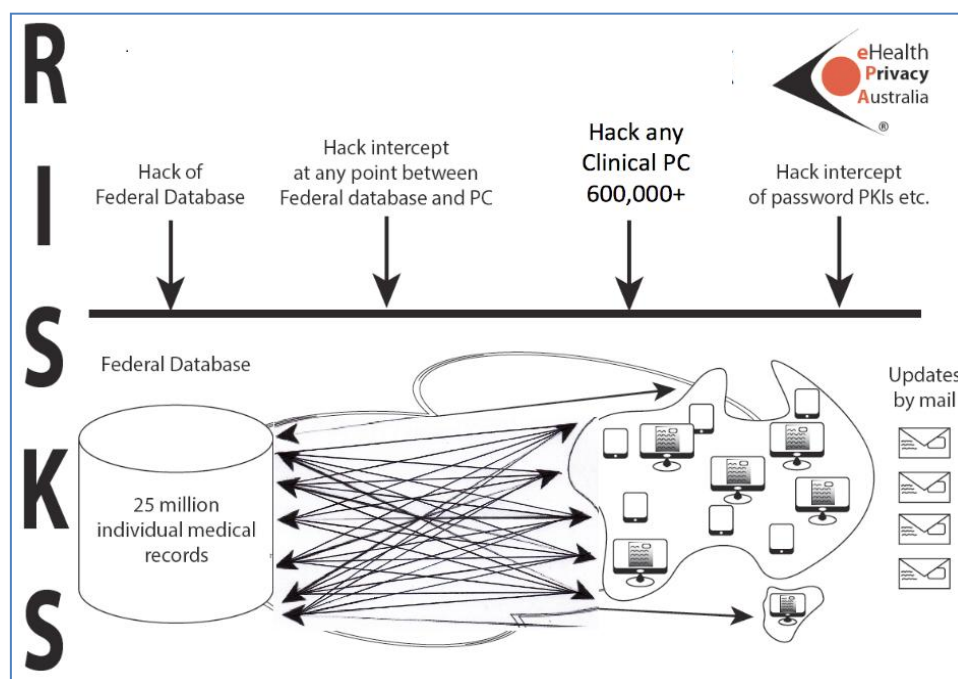


Figure 1: Many avenues for hacker attack

Ameliorating the security weaknesses around poor cyber security practices and certificate handling does not reduce the risk to a satisfactory level. This cannot be ignored.

The hacker(s) is (are) able to use one or more hacked PCs as conduits to the HPOS system.

The owners and regular users of these PCs would have no knowledge that their PCs have been used in this way. No forensic process can prove whether or not a suspect computer has been used as a conduit to the HPOS system.

All that can be said is that the whole system is basically vulnerable to being hacked and these PCs were somehow used as conduits, by persons unknown.

It is false to assert that the author(s) of the Medicare data breach are the actual normal users or owners of the PCs identified in the breach.

3. *“RETAINING THE MEDICARE CARD AS EVIDENCE OF IDENTITY IN THE COMMUNITY”*

The ePA notes the Discussion paper’s comment:

“Given their widespread use as a secondary form of evidence of identity, and the fact that they are not sufficient on their own to verify an individual’s identity, the Review Panel is likely to recommend that there should be no change to their use as a form of evidence of identity.”

The ePA submit that neither

(i) *“widespread use”*, or

(ii) the fact that they are *“insufficient on their own” (sic)*

justifies the Medicare card’s continued use as a form of identity, since their **weakness** as such has been demonstrated by the evident data breach.

4. CONCLUSION

The nature of the Healthcare Providers' Online Services dictates that the service be online. This means that risk mitigation or minimisation appears to be the only viable approach. However, the level of risk associated with providing the Medicare card data online is such that its use **should be limited to its primary purpose**, in relation to healthcare only. Secondary uses, such as providing a means of personal identification, should be avoided.

References

1. <http://www.ahpra.gov.au/About-AHPRA/What-We-Do/AHPRA-in-numbers.aspx>
2. $0.99999^{660,000} = 0.001$
3. <https://www.theguardian.com/australia-news/2017/jul/04/the-medicare-machine-patient-details-of-any-australian-for-sale-on-darknet>
4. <http://www.sbs.com.au/news/article/2017/07/04/medicare-data-breach-tip-iceberg-world-australian-dark-web-fraud>
5. $75 / 24 \text{ million} \times 75 / 24 \text{ million} = 0.000000001\%$
6. For the probability of one to be among the compromised to be 50%, the number to be compromised must be half of Australia's the population of 24 million; for both: $17 / 24 \times 17 / 24 = 0.5$