31 August 2017

Senate Finance and Public
Administration Committees
PO Box 6100
Parliament House
Canberra ACT 2600

By email: fpa.sen@aph.gov.au

Dear Committee Secretary,

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'

We thank the Senate Finance and Public Administration References Committee for the opportunity to make a submission to its inquiry into the circumstances in which Australians' personal Medicare information has been compromised and made available for sale illegally on the 'dark web'.

We address the following key points

- There are fundamental weaknesses in both the HPOS (Medicare card data) and My Health Records systems, which make them vulnerable to illegal access.
- Those weaknesses mean that fraudulent users of the systems can assume the identity of legitimate users to gain illegal access.
- It is not sufficient to mitigate these weaknesses in the My Health Records system.
- It is necessary and possible to virtually eliminate the weaknesses by employing a different implementation method.
- An alternative implementation method addressing those weaknesses is currently being rolled out elswhere

Yours sincerely,

Paul Power
Principal eHealth Privacy Australia
BSc (Hons)
IT Consultant to the Medical Profession

Terms of reference addressed:

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' (DHS) Health Professional Online Services (HPOS) system
c. the implications of this breach for the rollout of the opt-out My Health Record system

Summary:

Fundamental weaknesses in both HPOS and My Health Records systems are identified and discussed.

We maintain that it is impossible to reliably identify the author(s) of the Medicare information compromise due to such fundamental weaknesses.

A system that addresses the fundamental weaknesses is proposed.

Detail:

a. "any failures in security and data protection which allowed this breach to occur"

The evident availability of Medicare data, available on request by Guardian journalist, Paul Farrell [1] and SBS journalist, James Elton-Pym [2] is a failure in security and data protection.

b. "any systemic security concerns with the Department of Human Services' (DHS) Health Professional Online Services (HPOS) system"

Access points to HPOS are typically medical practices.

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.

1. https://www.theguardian.com/australia-news/2017/jul/04/the-medicare-machine-patient-details-of-any-australian-for-sale-on-darknet
2. http://www.sbs.com.au/news/article/2017/07/04/medicare-data-breach-tip-iceberg-world-australian-dark-web-fraud

There are approximately 660,000 access points registered for legitimate access to Medicare data via HPOS [3], 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% [4]. This means there is a probability of 99.9% that it would be hacked, exposing any and all records.

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 hacked by a hacker scanning for open ports exposed to the internet.
iv. The PKI PIC (Personal Identification Code) password is weak (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.

Ameliorating the security weaknesses around poor cyber security practices and certificate handling does not reduce the risk to an acceptable level.

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.

3. http://www.ahpra.gov.au/About-AHPRA/What-We-Do/AHPRA-in-numbers.aspx
4. 0.99999^660,000 = 0.001

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

The hacker(s) 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 the same 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.

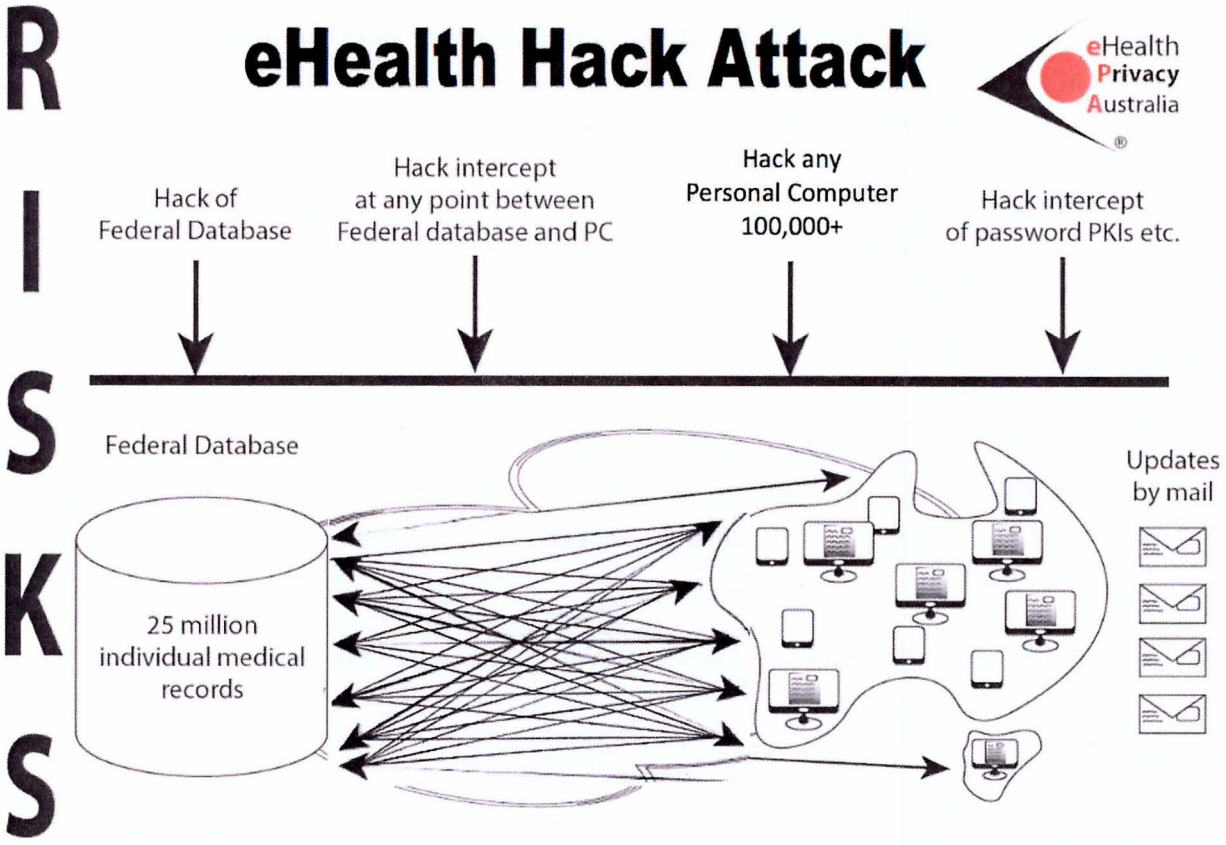
c. ***"the implications of this breach for the rollout of the opt-out My Health Record system"***

The same observations for HPOS, in relation to the inadequate level of individual security and the large number of access points, apply to the My Health Records system. In a manner similar to the Medicare data, the My Health Records data on a central data repository is secured by

1. NASH (National Authentication Service for Health) and site PKI certificates
2. Healthcare provider identifier
3. Medicare number, name and DOB (which by evident security failure of Medicare data, is already breached.)

Assuming only 100,000 legitimate access points [5], each of which has access to any record in the database, even with a security of 99.99% for every one of the access points, the security of the whole system is 0.005% [6]. That is, there is a 99.995% chance any and all records can be hacked. Even if the security of every point were 99.999%, the security of the whole system would be only 37% [7]. i.e. there would be a 63% chance it would be breached – since each access point has access to any record in the database, the entire database is breached.

5. http://www.aihw.gov.au/workforce/medical/how-many-medical-practitioners/
6. 0.9999^100,000 = 0.000045
7. 0.99999^100,000 = 0.37



It must be stressed that ameliorating the security weaknesses around poor cyber security practices and certificate handling <u>does not reduce the risk to an acceptable level.</u>
A system of on-line access to a central data repository to such a large number of legitimate access points, each of which has access to any record in the database, is fundamentally indefensible.
There is no risk mitigation that can protect the My Health Records system implemented as a central repository accessed over the internet by a large number of legitimate users.

Proposed Alternative:

- The My Health Records database is unlike other large government databases where restrictions are such that no users have access to all records.
- The only effective defence is to change the method of deployment away from a central repository.
- The method employed by Germany, in which the master data is held on an encrypted eHealth card by each citizen addresses this fundamental vulnerability. [8]

Example:

What we are being told by the guardians of the My Health Records system is like being advised "We take nuclear safety very seriously and look at the wonderful 10 meter high wall we've built to protect the Fukushima nuclear power station from tsunamis."

An expert could have advised the risk mitigation was inadequate [9].

Conclusion:

eHealth Privacy Australia advise that the risk mitigation is not adequate.
It is not possible to adequately mitigate the risk of a centralised data repository accessible over the Internet to such a large number of access points.

8. https://www.bundesgesundheitsministerium.de/health/the-electronic-health-card.html
9. The Fukushima Disaster and Japan's Nuclear Plant Vulnerability in Comparative Perspective, Phillip Y. Lipscy, Kenji E. Kushida and Trevor Incerti, Environ. Sci. Technol. 2013, 47, 6082−6088

eHealth Privacy Australia:

eHealth Privacy Australia (EHPA) is a not-for-profit business that comprises a coalition of digital health professionals working to establish a useful and effective Australian eHealth system.

Company principals are Dr Juanita Fernando, FACHI PhD MA BA PG Dip HPE GradCert BusSys, Biomedical & Health Informatics researcher and

Mr Paul Power, BSc (Hons), IT consultant to the medical profession.

EHPA has a keen interest in ensuring that eHealth data is private and secure, ensuring the My Health Record is fit for purpose and adequately protects patient confidentiality.

This page is intentionally

BLANK

to assist with duplex printing and collation.