Australian Government
Office of the Australian Information Commissioner

www.oaic.gov.au
GPO Box 5218 Sydney NSW 2001
P +61 2 9284 9800 F +61 2 9284 9666
E enquiries@oaic.gov.au
Enquiries 1300 363 992 TTY 1800 620 241
ABN 85 249 230 937

Senator Jenny McAllister
Chair, Senate Standing Committees on Finance and Public Administration
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Senator

Submission to the Inquiry into circumstances in which Australians' personal Medicare information has been compromised and made available for sale illegally on the 'dark web'

I welcome the opportunity to make a submission to the Inquiry into circumstances in which Australians' personal Medicare information has been compromised and made available for sale illegally on the 'dark web'.

The Office of the Australian Information Commissioner (OAIC) is an independent Commonwealth statutory agency established by the Australian Parliament to bring together three functions:

- privacy functions (protecting the privacy of individuals under the *Privacy Act 1988* (Privacy Act), and other Acts)
- freedom of information functions (access to information held by the Commonwealth Government in accordance with the *Freedom of Information Act 1982* (FOI Act)), and
- information management functions (as set out in the *Information Commissioner Act 2010*).

The integration of these three interrelated functions into one agency has made the OAIC well placed to strike an appropriate balance between promoting the right to privacy and broader information policy goals. This includes ensuring that personal information, including government related identifiers, held by government agencies is kept secure.

At the outset, I am concerned about any report that personal information of Australians is being offered for sale on the dark web, particularly if it is suggested to be government held information.

OAIC engagement

My Office first became aware of this matter on 3 July 2017, when a journalist informed the OAIC that a site on the 'dark web' was offering to sell Medicare card numbers of Australians. Following this, my Office contacted the Department of Human Services (Department) about

the incident and officers of the Department briefed my staff about its initial response, including the referral of the matter to the Australian Federal Police (AFP) for criminal investigation.

Subsequently, on 5 July 2017, I wrote to the AFP and the Department to request that they keep me informed of the progress of the investigations. The Department has since provided periodic updates to my Office about the progress of the investigations.

As the Committee would be aware, the Government has also commissioned a review of the accessibility by health providers to Medicare card numbers, led by Professor Peter Shergold AC. My Office has also met with the Secretariat to the review and will further engage with the review process.

My Office will consider the findings of the AFP's investigations, the review conducted by Professor Shergold as well as the results of your Inquiry, when considering whether any regulatory action under the *Privacy Act 1988* (Privacy Act) is required.

Observations

I understand that healthcare providers are able to obtain their patient's Medicare card number from the Department using online or telephone channels and that these arrangements help ensure healthcare remains accessible, even for those that may not be able to present their Medicare card.

While I appreciate the policy considerations around making this information available to healthcare providers, consideration must also be given to the security of that information and whether the use of personal information in this manner strikes an appropriate balance between achieving policy goals and any impact on privacy.

Security of personal information

The Privacy Act contains thirteen Australian Privacy Principles (APPs) which outline how Australian Government agencies, private sector organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses must handle, use and manage personal information. Under APP 11, entities are required to take reasonable steps to protect personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.

My Office has published the *'Guide to securing personal information'* to provide guidance on the reasonable steps entities should take under the Privacy Act to protect the personal information they hold.

The security of personal information is not only about ensuring compliance with the requirements of the Privacy Act. It is also essential to ensuring public trust and confidence in the handling of personal information. This is important as the Australian community is increasingly aware of privacy issues, especially in light of new technological advances and information sharing initiatives. People expect government to act transparently when handling their personal information and to keep that information secure. This is particularly so in

circumstances where government agencies have the legal authority to collect, use and disclose personal information in particular ways.

Even where an agency may have this legal authority, the use of personal information should be necessary, proportionate and reasonable to achieve the policy goals.

A useful tool to assist agencies to consider these matters is a Privacy Impact Assessment (PIA). A PIA is an assessment tool that describes the personal information flows in a project and analyses the possible privacy impacts on the privacy of individuals.

In this situation, a PIA would highlight any privacy impacts associated with accessing Medicare card numbers through an online portal environment and identify any further proactive measures required to mitigate those impacts.

Further considerations

The OAIC's 2017 Australian Community Attitudes to Privacy Survey[1] found that a majority of Australians (69%) reported to be more concerned about the privacy of their personal information when using the internet than five years ago, a consistent finding compared to the last two surveys.

A significant majority of Australian (83%) think that online environments are inherently more risky than offline. Although trust in Government is relatively high, with both state and federal governments scoring 58% when the community was asked how trustworthy they considered 14 different types of organisations, this was still below banking and finance institutions (59%) and significantly below healthcare providers (79%).

On 18 May 2017, I announced the development of the *Australian Public Service (APS) Privacy Governance Code* that will apply to all Australian Government agencies that are subject to the Privacy Act. The Code is being developed by the OAIC, with the support of the Department of Prime Minister and Cabinet. It will play a key role in supporting strong privacy governance and capability in the Australian Public Service. Information on the Code can be found on the OAIC website.[2]

If you would like to discuss these comments or have any questions, please contact Paula Cheng, Director, Regulation and Strategy

Yours sincerely

Timothy Pilgrim PSM
Australian Information Commissioner
Australian Privacy Commissioner

30 August 2017

---

[1] https://www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017

[2] https://www.oaic.gov.au/engage-with-us/consultations/aps-privacy-governance-code/