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

Our reference: D2017/006061

The Review Secretariat
Independent Review of Health Providers' Access to Medicare Card Numbers
By email: mca.review@humanservices.gov.au

Dear Sir/Madam

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

I welcome the opportunity to comment on the discussion paper of the Independent Review of Health Providers' Access to Medicare Card Numbers (Review). The Review considers how best to balance the need for accessing health services with the security controls required to protect Medicare card numbers.

The discussion paper outlines the key issues for consideration and possible responses to these issues. I broadly support the recommendations the Review is considering in Part 5 of the discussion paper in so far as they relate to the security of personal information. In this regard, I have outlined below some additional considerations.

Role of the OAIC

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.

Security of personal information

The Privacy Act contains thirteen Australian Privacy Principles (APPs) which outline how Australian Government agencies, privacy 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'*[1] to provide guidance on the reasonable steps entities are required to 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 a legal authority, the collection, use and disclosure of personal information should be necessary, proportionate and reasonable to achieve the policy goals.

Observations

As I understand, healthcare providers are able to obtain their patient's Medicare card number from the Department using online or telephone channels and these arrangements help ensure healthcare remains accessible, even for those who 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.

It is pleasing that the recommendations under consideration by the Review generally align with the suggested strategies provided in the OAIC's *Guide to securing personal information*. My additional comments and suggestions cover four broad areas and are set out below.

[1] https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information

Use of a Privacy Impact Assessment

I would recommend that the Department conducts a Privacy Impact Assessment (PIA) to assist it in the implementation of Review recommendations. A PIA is an assessment tool that describes the personal information flows in a project and analyses the possible privacy impacts that those information flows, and the project as a whole, may have on the privacy of individuals.

In this situation, a PIA would highlight any privacy impacts associated with implementing the Review recommendations and identify proactive measures required to mitigate those impacts, including security considerations.

The Review may wish to consider including as one of its recommendations that the Department undertake a PIA to assist it in implementing any other recommendations made by the Review.

Access controls by healthcare providers

The Review notes, and I agree, that healthcare practitioners need to be able to access and confirm a patient's Medicare card number in the ordinary course of their work. I also agree that stronger access controls may be required.

With regard to the use of HPOS, I understand that a public key infrastructure (PKI) certificate is often installed on a healthcare provider's practice software, enabling multiple users at the healthcare provider's location to access Medicare card information. This raises a risk that persons may use the practice software to access Medicare card numbers when they are not authorised to do so.

The OAIC's *Guide to securing personal information* sets out a number of steps organisations could take to improve their access security.[2] This includes limiting the number of people who can access relevant personal information, keeping audit logs of their activity and ensuring their access is removed when it is no longer needed.

Healthcare providers who use the My Health Record system are already subject to the *My Health Record Rule 2016*, rule 42. Under this rule, healthcare provider organisations must have a written policy that reasonably addresses a number of security related matters, such as the requirement to be able to identify who, in the healthcare provider's practice, has accessed an individual's My Health Record. The Review may wish to consider similar provisions for inclusion in the HPOS, PKI and Provider Digital Access (PRODA) terms and conditions in relation to Medicare card numbers.

I support the Review's proposed response to suspend inactive PRODA accounts and PKI certificates. Any authority to access Medicare card numbers should be periodically reviewed by the healthcare provider and removed if no longer needed. Providing for the suspension of

[2] www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information#access-security

inactive HPOS accounts or time limiting access through a PRODA account may be an alternative way of mitigating this risk.

With regard to telephone enquiries, I am not aware of the current authentication tests applied to callers before Medicare card numbers are disclosed by the Department. However, in principle those tests should be as robust as those applied to access the HPOS. I would support the Review recommending that those tests be reviewed.

Use and protection of Medicare card numbers

I agree with the Review that the community should be made more aware of the importance and use of their Medicare card number, its value to criminals and the need to keep it secure.

I understand that there are audit logs of access to Medicare card numbers through HPOS (although there is currently no audit log of access to Medicare card numbers through the telephone channel). The Review may wish to consider whether individuals should be provided with access to those audit logs automatically through their Medicare Online account (if they have one) and for such logs to be created for telephone requests and for individuals to have similar access.

Making this information available to individuals will increase their control over the use of their Medicare card number and may increase the chance of fraudulent activity being identified by the individual. This arrangement may go beyond the identification of Medicare fraud to identity theft generally.

I note that similar information is made available to individuals in the My Health Record system, where audit logs will show when a person has accessed their My Health Record or retrieved their individual healthcare identifier.

Identification information to be provided by individuals

The Review is considering a recommendation that individuals should be required to present a secondary form of identification when they first attend a health service, to verify that they are eligible for Medicare. The Review recognises that requiring a secondary form of identification could create further barriers to accessing healthcare for individuals who are unable to present identification.[3] The Review appears on balance to conclude that any barriers for individuals are outweighed by the need to restrict fraudulent claims and inaccurate data being uploaded to an individual's Medicare Online account or My Health Record.

As noted above, the collection, use and disclosure of personal information should be necessary, proportionate and reasonable to achieve the intended policy goals. To increase transparency and manage community concerns, I encourage the Review to draw out why the individuals concerns are outweighed. I would also like the Review to consider whether a health service would be required to collect any personal information from a secondary form of identification presented by an individual. If the health service collects personal information from a secondary form of identification, the health service must take reasonable steps to

[3] Paragraph 4.2 'Access to health services' of the discussion paper.

protect the information from misuse, interference and loss and from unauthorised access, modification or disclosure.

Further considerations

The OAIC's 2017 Australian Community Attitudes to Privacy Survey[4] 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 building public trust in the Australian Public Service, supporting the Australian Government's public data agenda and enhancing privacy governance and capability. Information on the Code can be found on the OAIC website.[5]

If you would like to discuss these comments or have any questions, please contact Paula Cheng, Director, Regulation and Strategy on (02) 9284 9652 or paula.cheng@oaic.gov.au.

Yours sincerely

Timothy Pilgrim PSM
Australian Information Commissioner
Australian Privacy Commissioner

8 September 2017

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

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