Queensland Health Response

Attachment 1

Discussion Paper - Independent Review of Health Providers' Access to Medicare Card Numbers

Consultation questions -

1. Do patients have sufficient control and awareness of access to their Medicare card details?

- Patients are likely to have sufficient control but probably lack the awareness and understanding of the implications of improper/unauthorised use of their Medicare number. Unless a patient experiences "a total loss of their identity (i.e. from identify theft)" then it is likely to be difficult to convince them that there is a personal incentive to guard against misuse as any cost is likely to be incurred by the system and not the individual.
- Currently there is no audit log of access to Medicare card numbers through the telephone channel. It is recommended that there is an auditable record of any enquiry made for each respective Medicare card number, which would restrict enquiries to computer-based access.
- Suggest that individuals are able to seek access to the audit logs for their Medicare card number if required.
- If individuals identify discrepancies (for example, a claim for a service that they have not received), these can be reported to the Department of Human Services for further investigation. It is recommended that information about the process for reporting of discrepancies regarding an individual's claiming history be made readily available to all Medicare Card holders.

2. What identifying information should patients have to produce to access health services?

- Medicare Card or if possible approved photographic identification.
- The option to require individuals to present identification in order to obtain Medicare benefits for non-urgent or long term treatment, but allow them to claim for urgent or emergency treatment even if they are unable to verify that they are using their own Medicare details should be considered.

3. Are the current access controls for Health Professional Online Services (HPOS) sufficient to protect Medicare information and prevent fraudulent access?

- The process of mailing a USB or CD-ROM via Australia Post to obtain a PKI certificate may pose issues:
    - A package may be damaged through the Australia Post sorting process resulting in the USB (or similar device) being lost.

- It is understood that USBs, as well as many other items, are detected each month, having come loose from their envelope or packaging.
- Sending in secure packaging or via registered post is also not a guarantee that this will not occur.
- Recommend alternative and secure methods be considered, such as via courier.

- It is recommended that all devices must be encrypted.
- The process for providing hard copies of identity documents for manual processing to access PRODA is not clear.
  - Clarity is required on whether it is the provision of original copies of identity documents, or photocopies of those identity documents.
  - It is recommended that there be a clear procedure about how the verification process will be handled, including compliance with the Commonwealth Privacy Act 1988.
  - It is necessary to consider what information will be provided to the individual about this process, and if identity documents are to be returned or appropriately and securely destroyed once the purpose is fulfilled.
- Patient identity verification requirements include first name, surname and date of birth. It is recommended that patient identity verification requirements be strengthened.

4. What would the impact on health professionals be if they were required to move from an individual or site level PKI certificate to a PRODA account? Would any enhancements to PRODA be required for health professionals to accept it as a replacement?

- Moving away from a reliance on PKI would alleviate some of complexity for health users but would also reduce the level of assurance around identity validation.

5. If PRODA accounts and PKI certificates were to be suspended following a period of inactivity, what processes or alerts would the Department need to put in place? What would be a reasonable period of inactivity before accounts were suspended?

- The time period is dependent on the “level of risk tolerance for potential opportunity for fraud”.
- It is recommended that the following suggestions be considered:
  - Active, deactivated and expired accounts/certificates should be audited, reviewed and monitored.
  - They should be deactivated if not used within a specified period of time. A 6 month period of inactivity would seem appropriate.
  - If the user requires PRODA access in the future, they should be required to go through the identity verification process again.

6. **If delegate arrangements in HPOS were to be time limited, what processes or alerts would the Department need to put in place? What would be a reasonable period for delegate arrangements to last before they require review?**

   - Alerts should be configured to notify if the delegate has been changed within the system.
   - The time period is dependent on the "level of risk tolerance for potential opportunity for fraud". A twelve month period of inactivity would seem appropriate.

7. **In what circumstances do health professionals need to make batch requests for Medicare card details through HPOS Find a Patient? Can such requests be limited to certain types of providers or health organisations? Should they be subjected to a higher level of scrutiny?**

   - The ability to make 500 requests at a time appears excessive, particularly where the request comes from a GP or a small practice, compared with a hospital.
   - Agree that batch requests should be subjected to a higher level of scrutiny.

8. **In what circumstances do health professionals require access to Medicare card numbers through the provider enquiries line? Could the provider enquiries line be made available in more limited circumstances?**

   - There appears to be inadequate security measures in place for telephone enquiries. All phone enquiries, including the identity of the caller, should be recorded against the relevant Medicare card number for auditability.
   - It is not clear why seven Medicare card numbers can be requested per telephone call. Suggest this is reviewed.
   - Given the inadequate security and auditing measures in place for the telephone enquiries line, it is recommended either reducing the number of requests allowed per call, and/or strengthening the security measures for this process and ensuring the enquiry can be traced and audited. Alternatively, phase out the telephone enquiries line and require secure computerised access.

9. **Is the information available to health professionals regarding their obligations to protect Medicare card information (including the terms and conditions for accessing this information online) sufficiently clear and understood?**

   - It is not clear if there are similar terms and conditions for the telephone service.
   - Agree that terms and conditions may need to be more explicit in their references to the sharing of credentials and information with third parties.

10. **Should Medicare cards continue to be used as a form of evidence of identity?**

    - Yes as a secondary form in conjunction with some other accepted photographic identification.

11. How can Government build public awareness of why it is important for individuals to protect their Medicare card information?

- Run an awareness campaign to educate the public on securing personal information and why it matters.
- Promote awareness on how Medicare card information will be protected, including how it will be stored and how it will be destroyed when it is no longer required.
- Publish an annual audit into how the government is securing Medicare card information.
- Provide a yearly statement to individuals as part of their tax return.

12. Do you have any other comments about the Review Panel's possible responses or any other matters relating to the Terms of Reference?

- Measures to reduce Medicare fraud and identity theft are welcomed. There is a need to ensure that the measures do not become a barrier to eligible patients obtaining care, or impose additional burdens on health providers who already carry a high administrative load.