Submission in response to the Australian Government's independent review of health providers' access to Medicare card numbers

5 September 2017

Table of Contents

1 Overview

The Australian Healthcare and Hospitals Association (AHHA) is pleased to provide this submission to the Australian Government's independent review of health providers' access to Medicare card numbers.

The AHHA is Australia's national peak body for public hospitals and health care providers. Our membership includes state health departments, Local Hospital Networks and public hospitals, community health services, Primary Health Networks and primary healthcare providers, aged care providers, universities, individual health professionals and academics. As such, we are uniquely placed to be an independent, national voice for universal high quality healthcare to benefit the whole community.

2 Responses to the review's consultation questions

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

The Australian public does not have sufficient awareness of access and control of their Medicare card details.

The current arrangement that a health professional does not have to obtain an individual's consent before obtaining their Medicare card number through the Find a Patient function of the Health Professional Online Services (HPOS) or through the Australian Government Department of Human Service's Medicare provider enquiries telephone line should be changed.

Consent should be a requirement for a health service provider to access an individual's Medicare card details in non-urgent or long-term treatment care. The manner in which consent is obtained should be with as little administrative burden as possible while balancing the need for integrity of the health system and of Medicare cards. For example, upon being admitted to a public hospital consent could be obtained when the individual presents to the hospital and remains in force throughout the individual's treatment.

Consent is ideal but should not hinder urgent or emergency treatment.

Requiring individuals to confirm they are accessing HPOS Find a Patient for claiming purposes only should be retained, but consideration should be given on how to make this confirmation not simply a box ticking exercise that risks losing its meaning over time. A similar assurance should be made verbally when utilising the Department's Medicare provider enquiries telephone line.

As My Health Record is a secure online summary of an individual's health information, the existing audit logs of access to Medicare card numbers through HPOS should be made available to individuals via their My Health Record, and it should be made available to an individual upon request.

Audit logs of access to Medicare card numbers through the Department's Medicare provider enquiries telephone line should be kept and also made available to individuals via their My Health Record, and it should be made available to an individual upon request.

An individual's Medicare claiming history should continue to be made available to individuals via their My Health Record and upon request for individuals without a My Health Record.

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

Access to health services needs to be considered in two parts: Medicare funded and non-Medicare funded services.

An appropriate control to verify whether an individual is eligible to access Medicare funded services is for the individual to present their Medicare card and a proof of identity. However, this process should not hinder the provision of care—especially urgent or emergency treatment.

The AHHA supports the review panel's proposal whereby an individual presents identification in order to obtain Medicare benefits for non-urgent or long-term treatment, but allows for urgent or emergency treatment claims even if the individual is unable to verify that they are using their own Medicare details.

Consideration will need to be given to population groups who may not have ready access to identification or their Medicare card number. Examples include: disadvantaged population groups

such as individuals fleeing domestic violence, homeless people and refugees; transient population groups such as students; and Aboriginal and Torres Strait Islander peoples.

Generally, the acceptable identification should conform to the 'very high' (or 'Gold standard') level of assurance as outlined in the Attorney-General's Department's 2014 National Identity Proofing Guidelines. This level of assurance is appropriate for transactions that would have very serious consequences if associated with fraud.

Such a requirement should be a legal condition required to be met in order to lodge a Medicare claim.

The Australian Government should also consider moving toward the implementation of more secure Medicare cards similar to those used in Canadian provinces. For example, the most recent healthcare card used to access the public healthcare system in Ontario is plastic with the front of the card bearing the insured person's photo and signature (unless a photo and signature exemption has been granted or the person is under 16 years of age), name, 10-digit personal health number and version code, date of birth, the card's issue and expiry date and the depiction of a trillium (the provincial flower) in optical variable ink that changes colour when the card is tilted and various tactile features. The back of the card contains organ donor information, a stock control number and a magnetic strip and 2-D barcode encoding specific data.[1] A more secure Medicare card such as those used in Ontario would strengthen identity verification processes for individuals accessing Medicare.

The Australian Government should also consider how it could utilise emerging technology, such as fingerprint authentication, similar to recent moves by Australian and international banking institutions with their banking applications available on smartphone, as a means to verify identity.

2.3 Are the current access controls for HPOS sufficient to protect Medicare information and prevent fraudulent access?

It is not secure for a health service organisation to apply for an organisational level Public Key Infrastructure (PKI) certificate that allows any user of the organisation's software or network to access HPOS without any requirement for individual log-in by those working within the registered organisation.

Each individual within a registered organisation who accesses HPOS should have their own log-in details—as is the current practice with the Provider Digital Access (PRODA) system to access HPOS. This is also the practice of the banking industry whereby a bank provides each authorised officer in an organisation with their own bank token (for example, an RSA Secure ID token), username and password. General practices, like other businesses, would be accustomed to managing their banking processes and staff access to accounts in this manner, so it is not unreasonable to expect that they might be required to use similar processes to access Medicare information.

Legitimate concerns about administrative burdens must be appropriately balanced against the higher need of ensuring the integrity in the health system and with Medicare cards.

[1] http://www.health.gov.on.ca/english/providers/pub/ohip/ohipvalid_manual/ohipvalid_manual.pdf

2.4 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?

AHHA supports the transition from an individual or site level PKI certificate to a PRODA account, or a PRODA-like system with similar features, to access HPOS. PRODA is a more secure system with its two-step verification process, requiring a username, password and verification code to log in. AHHA supports all new HPOS users only being able to apply for a PRODA account.

An expedited transition period for all PKI certificate holders to transition to PRODA would be ideal. However, the Commonwealth Government must work with state and territory departments of health to ensure any transition does not unduly overburden public hospitals. The first phase of a transition would include pre-transition awareness raising tactics with targeted change management activities and communications. This would be followed by a period to transition all PKI certificate holders to the PRODA, or PRODA-like, system.

The three year time period under consideration by the review panel is too long a timeframe considering broader community expectations around cyber security concerns.

2.5 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?

PRODA accounts should expire, especially after a pre-determined period of inactivity. PKI certificates should be phased out over a period as noted in 2.4 above.

While the review panel notes it is important to avoid creating administrative burdens for health professionals who have a legitimate need to access HPOS, the review panel should note that health service providers currently comply with stringent security arrangements for their financial arrangements and transactions with banks. Security requirements to access Medicare card and patient information should be just as stringent.

2.6 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?

To reduce the risk that HPOS delegations are not reviewed and removed when they are no longer required, the AHHA supports that delegations should only be in place for a set time period, after which they will be automatically removed if not renewed by the provider or if they sit inactive. A period of 12 months should be considered. This would ensure registered organisations keep up-to-date on who within their organisation is able to appropriately access HPOS.

The review panel should consider arrangements in place in the banking sector with regards to reasonable time periods. Health service providers currently conform to banking rules and regulations regarding employee access to their finances through online and in-person banking systems. A similar system for HPOS access should not be onerous.

2.7 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 AHHA supports limiting the availability of batch Find a Patient requests, for example by reducing the number of patients whose details can be requested or by imposing a threshold number beyond which a second stage approval is required.

2.8 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?

Callers to the Department's Medicare provider enquiries telephone line should be required to identify themselves and verify their identity similar to a business' use of telephone banking services.

Health service providers should be required to obtain an individual's consent to access Medicare details in order to obtain Medicare benefits, but individual consent could be waived for urgent or emergency treatment.

As noted in 2.1 above, the manner in which consent is obtained should be with as little administrative burden as possible while balancing the need for integrity of the health system and of Medicare cards.

Additionally, audit logs of access to Medicare card numbers through the Department's Medicare provider enquiries telephone line should be kept and also made available to individuals via their My Health Record and upon request.

2.9 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?

The AHHA recommends that the current terms and conditions for HPOS, PKI and PRODA should be reviewed to ensure that user obligations are clear and prominent, that they take confidentiality requirements with third parties into account, that they be strengthened to reflect user obligations when providing third parties with system access, that they clearly outline penalties for breaches and contact details for where an individual can report a breach, and that they are not simply a box ticking exercise.

2.10 Should Medicare cards continue to be used as a form of evidence of identity?

As Medicare cards have become one of the credentials most commonly used as evidence of a person's identity, and as Medicare cards are recognised in guidelines as a secondary form of evidence in identity verification, the Australian Government should consider moving toward more secure Medicare cards similar to those used in Canadian provinces as outlined in section 2.2 above.

As Medicare cards continue to be used as a secondary form of evidence in identity, the current ability to access the card's details in essentially anonymous form via PKI certificate access to HPOS and the Department's Medicare provider enquiries telephone line is extremely inadequate. Security arrangements surrounding Medicare cards should be updated to reflect how they are being used now.

Legitimate concerns about administrative burdens, must be appropriately balanced against the higher need of ensuring the integrity of the health system and of Medicare cards.

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

The Government should undertake a long-term communications campaign utilising a number of tactics across various platforms. This could include mandatory posters and/or signage at point of use within a health service provider, a text box with key messages as part of all Medicare correspondence with card holders, and public service announcements in traditional and online form.

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

See previous and subsequent comments.

3 Conclusion

The AHHA commends the work of the Australian Government's independent review of health providers' access to Medicare card numbers and recommends the following for action:

- Consent should be a requirement for a health service provider to access an individual's Medicare card details in non-urgent or long-term treatment care; consent is ideal but should not hinder urgent or emergency treatment. The manner in which consent is obtained should be with as little administrative burden as possible while balancing the need for integrity of the health system and of Medicare cards.
- Audit logs of access to Medicare card numbers through HPOS and the Department's Medicare provider enquiries telephone line should be kept and also made available to individuals via their My Health Record and upon request.
- An individual should present identification in order to obtain Medicare benefits for non-urgent or long-term treatment. Urgent or emergency treatment claims should proceed even if the individual is unable to verify that they are using their own Medicare details. Consideration needs to be given for disadvantaged and transient population groups and Aboriginal and Torres Strait Islander peoples who may not readily have access to identification or their Medicare card number.
- Medicare cards continue to be used as a secondary form of identity verification, and the Australian Government should consider moving toward the implementation of more secure Medicare cards similar to those used in Canadian provinces.
- Consideration should be given to utilising emerging technologies, such as fingerprint authentication.
- Access to HPOS should be through PRODA to ensure each individual within a registered organisation has their own log-in details.
- Access to HPOS through PKI certificate should be phased out with a transition to PRODA over an agreed period. The Commonwealth Government must work with state and territory departments of health to ensure any transition does not unduly overburden public hospitals.
- PRODA accounts should be renewed after a pre-determined period in line with business banking security arrangement, and PRODA accounts should expire after a pre-determined period of inactivity. A period of 12 months should be considered.
- The number of batch Find a Patient requests should be limited down from 500 per day or by imposing a threshold number beyond which a second stage approval is required.
- Callers to the Department's Medicare provider enquiries telephone line should be required to identify themselves and verify their identity similar to a business' use of telephone banking services.
- The current terms and conditions for HPOS, PKI and PRODA should be reviewed to ensure clear and prominent user obligations, penalties for breaches, contact details for where an individual can report a breach. Agreeing to these terms and conditions should not simply be a box ticking exercise.
- The Australian Government should build public awareness of why it is important for individuals to protect their Medicare card information.

Australian Healthcare and Hospitals Association
Unit 8, 2 Phipps Close

Deakin ACT 2600
PO Box 78

Deakin West ACT 2600
P: 02 6162 0780
F: 02 6162 0779
E: admin@ahha.asn.au
W: ahha.asn.au
@AusHealthcare
facebook.com/AusHealthcare
linkedin.com/company/australian-healthcare-&-hospitals-association
ABN: 49 008 528 470