Medical Software Industry of Australia Submission

Independent Review of Health Providers' Access to Medicare Card Numbers

September 7th 2017

Medical Software Industry Association

Submission to the Independent Review of Health Providers'

Access to Medicare Card Numbers

Executive Summary - MSIA Profile

The Medical Software Industry Association (MSIA) represents interests of the medical software providers across the spectrum of Australian health care services. The vision of this Association is to enable vibrant and innovative software organisations to achieve better health outcomes for all Australians.

The MSIA is a valuable stakeholder in Australian healthcare, with members ranging from Small and Medium Enterprises (SMEs) to large Australian and Public companies. We are frequently invited to submit its responses and offer suggestions for initiatives such MyHealth Record, PBS Online, DHS Online PBS Authorities and the AMT.

MSIA members are responsible for approximately 90% of the transactions that occur through DHS infrastructure.

The MSIA has negotiated a range of important changes with government and other stakeholders having built a considerable profile with Commonwealth and jurisdictional Health Departments as the clearing house of communication between these organisations and the healthcare software providers.

The MSIA welcomes the opportunity to provide the feedback on Health Providers' access to Medicare Card Numbers from the point of view of the Australian Medical Software Industry.

Overview of the MSIA Position on Health Providers' Access to Medicare Card Numbers

Summary of consultation questions with MSIA responses

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

The Department of Human Services website publishes an overview of the Medicare System and information on how to enroll for and use Medicare[1]. Individuals requiring more information are directed to the myGov website and are provided details of how to engage further with Medicare staff via telephone or at Medicare branches.

Over recent years there has been a concerted push by government departments to reduce access to face-to-face interaction with the community. This is evidenced by the closure of multiple Medicare Branches across Australia and in some communities, the co-location of a small number of Medicare staff within other government services, such as the Australian Taxation and Centrelink offices[2].

There has been an ongoing trend to push individuals to the myGov website to link various government department online services. Unfortunately, anecdotal reports suggest that government developed portals and apps designed to replace the face-to-face interaction traditionally provided by local services such as Medicare Branches, are poorly designed and difficult to use - particularly in the case of the elderly or those with limited computer skills or unreliable internet access[3] .

For example, The Express Plus Medicare App was rated an average of 2.5 stars out of 5 by over 3,000 users on the Android Apps on Google Play store[4]

Conclusion:

If patients are not given comprehensive and convenient access to information about Medicare and their own personal Medicare information through traditional means, any alternative online service offerings should be secure, well designed, convenient and useable.

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

While some agencies and individuals may consider the Medicare Card Number as an essential method of identification when seeking health services, the RACGP in their current Standards, do not consider the Medicare number as an "approved identifier" in general practice.[5]

The Australian Commission for Safety and Quality do not recommend that the Medicare number be used as a patient identifier.[6] As such, provision of a Medicare Card as a mandatory identifier is not generally part of the typical workflow of most general practices.

---

[1] Department of Human Services website view online https://www.humanservices.gov.au/individuals/services/medicare/medicare-card

[2] Herald Sun website viewed online http://www.heraldsun.com.au/leader/east/medicare-branches-close-around-melbourne-and-more-on-federal-governments-hit-list/news-story/e9bc0d26d8d0d8c2a530c6fd363adf8b

[3] Sydney Morning Herald viewed online http://www.smh.com.au/nsw/medicare-branch-closures-and-digital-push-makes-it-hard-for-seniors-20150320-1m3qzk.html

[4] Android Apps on Google Play https://play.google.com/store/apps/details?id=au.gov.dhs.expressplus.medicare&hl=en

[5] RACGP – Patient Identification – Standards for general practices – 3.1.4 viewed online http://www.racgp.org.au/your-practice/standards/standards4thedition/safety,-quality-improvement-and-education/3-1/patient-identification/

[6] Australian Commission on Safety and Quality in Health Care – Standard 5 – Patient Identification and Procedure Matching guide, viewed online https://www.safetyandquality.gov.au/wp-content/uploads/2012/10/Standard5_Oct_2012_WEB.pdf

As multiple individuals within one family may use the same Medicare Card Number (albeit with each family member listed individually with a single digit IRN number), it is not practical to use the Medicare Card Number itself as a primary identifier as it is not unique.

Potential problems also occur in families as children become adults and are issued their own new number and IRN, but remain listed on the family card until that card expires.

Practice management software applications are designed to securely store the patient's personal information, including Medicare Card Numbers, which are used when prescribing medications and claiming rebates from Medicare. The Patient Medicare Card Number is routinely printed on various documents as part of the Patient's health care journey. For example, the Medicare Card Number is printed on Prescriptions, Referral Letters and a variety of forms as required by various government agencies and third parties involved in the patients' care.

Since the introduction of the Improved Monitoring of Entitlements (IME) legislation in 2001[7], the patients' Medicare number or DVA number is required to be disclosed for all claims for reimbursement by Pharmacy for PBS listed medications. The only time in which this number would not be available would be if the patient did not declare it to the prescribing doctor, or if the patient was not eligible (such as a foreign national with nonreciprocal healthcare rights).

If the patient is unable to produce their Medicare credentials at pharmacy (and this is for a PBS listed medicine) but they are enrolled with Medicare, there are two processes in place which allows the Pharmacist to provide the medicine to the patient:

1. The Pharmacist would ring the IME telephone line to request either the Medicare number or the concession, pension health care card number. Appropriate vetting of callers is undertaken before any details are provided. Anecdotal reports indicate that most calls to the IME telephone line are in relation to the patients' concessional entitlement status – not to provide the Medicare number details.

or

2. The prescription is dispensed as a private prescription and the patient is given a special receipt called S87A[8]. The patient may then make a claim to Medicare to receive the standard reimbursement appropriate to their concessional status.

The use of the Medicare Number in Pharmacy dispensing is well established and the Australian population is well educated into the fact that they are required to give evidence of their Medicare details prior to receiving medicine at a reduced price.

Conclusion:

In General Practice, the Medicare Card Number is not a recommended or practical method to use as a primary identifier for patients to access health services. The Medicare Card Number remains an important element of a patient profile in both Practice Management and Pharmacy software, and is used in prescribing and dispensing workflows as part government legislated initiatives, such as the Pharmaceutical Benefits Scheme. Software designers will continue to be guided by, legislation, Standards and the official recommendations of authoritative agencies such as RACGP and ACSQ as to what patient identifying information is appropriate and required at point of care. As an example of the legislation and guidelines we refer to Privacy Guidelines for

[7] https://www.humanservices.gov.au/organisations/health-professionals/enablers/medicare-cards-improved-monitoring-entitlements

8 Pharmaceutical Benefits Scheme Receipt – S.87A, National Health Act 1953

the Medicare Benefits and Pharmaceutical Benefits Programs (March 2008) Issued by the Privacy Commissioner under section 135AA of the National Health Act 1953[9].

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

The MSIA is of the understanding that PRODA, in its current form, was never intended to service large scale Vendor operations. If all systems were required to change from a site level PKI certificate to a PRODA account, the MSIA believes that it would have a significant impact on existing software applications and workflows and would be a major impost for all vendor software interfacing with Medicare at the site level, for example practice management and pharmacy dispense systems to name just two

HPOS is not widely used in pharmacy or practice management software and most applications do not interface directly to HPOS. Medicare number validation is done through the Medicare Client Adaptor which uses PKI. The interface with My Health Record is done through PKI. If PKI is replaced by PRODA, it will negatively affect users and require significant rewrites within software applications risking providers' ability to upload to MYHR.

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?

Very few GPs or Pharmacists have a personal PKI certificate. Most work in group settings or practices and share a site based PKI. Many work in team settings with multiple individual practitioners contributing the care of one patient. Many practitioners employ staff to perform tasks on their behalf using the PKI infrastructure. A change to individual PRODA accounts would impact on their role and workflows.

For example, how would a Practice Nurse upload to the National Immunisation Register a list of immunizations given by multiple practitioners working at the same group practice? How would a Practice Manager complete the Medicare Online batching for a group of doctors at the end of the working day?

From a software providers view, multiple issues have been identified in relation to the development of initiatives such as the PBS Online Authority service – many of which remain unresolved. The MSIA Report to the Department of Health, October 2016, provided comprehensive feedback about MSIA workshops conducted with the DHS on implementation of Online Prescription Authorities and PRODA included issues such as:

- poor design and documentation,
- complicated workflows,
- PRODA Log in process is time consuming and limited
- issues relating to shared care environments, to name a few.

These issues remain largely unresolved and make it near impossible for software developers to develop capabilities that would allow health professionals to use online government services effectively.

Any plan to require a full-scale change from site based PKI to individual PRODA accounts will need a well-documented development pathway to ensure that other integrations within existing software systems are not compromised and that end users are provided support and training to

[9] https://www.legislation.gov.au/Details/F2008L00706

learn new workflows. The proposal of 3 years may not be sufficient time, but a detailed industry consultation would be required to ascertain what was practicable.

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 current PRODA log-in process, while secure, is time-consuming, limited and impractical in most settings. The mandatory 4-hour time out and re-authentication requirement has the most potential impact on health professionals if they are required to move to a PRODA account.

For example, GPs need to login to PRODA to seek approval for an online authority prescription. If they see their first patient (requiring an authority script) at 9am, they would automatically time-out at 1pm. If the doctor sees another patient (also requiring an authority script) after 1pm, they will need to log-in again and go through the same complex re-authentication process. This has the potential to add significant time to each consultation, increase user frustration and impact on the efficiencies of general practices and patient care.

If "suspended" refers to a situation where an individual PKI has not "talked" to the Medicare Services for Online Claiming for a long period (say several months) and appears inactive, how would the Department contact that user to advise that their PRODA account appeared inactive and therefore would be suspended? It would be reasonable to advise the end user that their account will be suspended prior to any suspension.

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?**

Having surveyed our members, we find that there is very limited access to HPOS, in terms of direct integration from vendors' software so this is a fairly hypothetical response.

In general, where an existing facility which has been incorporated in vendor software is forecast to change, a period of three years with full consultation is considered the industry norm.

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?

N/A for MSIA to respond.

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?

Please refer to consultation questions 2 for MSIA feedback.

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?

Please refer to consultation questions 2 for MSIA feedback.

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

Please refer to consultation questions 2 for MSIA feedback.

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

Education

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

The MSIA is keen to ensure that any proposed changes to the security settings are done following close consultation and collaboration with industry to ensure no disruption to interactions with the DHS and MYHR. It is critical that if following such consultation changes are made in this area, that they are also consistent with changes in respect of the draft cloud computing policy and any new identification framework.

The MSIA recognises the importance of security. It is at the core of our members' business. The MSIA is however concerned about the ramifications of any possible "knee jerk" reactions to the media reports on the alleged Medicare security breach. The functionality of MBS, PBS and MYHR depend upon robust processes with industry and detailed consultation will be essential before any changes are made to this part of the public key infrastructure

Yours Sincerely,

Emma Hossack
BA (Hons), LLB, LLM

PRESIDENT