Consumers Health Forum of Australia

SUBMISSION TO THE INDEPENDENT REVIEW OF HEALTH PROVIDERS' ACCESS TO MEDICARE CARD NUMBERS

RESPONSE TO THE DISCUSSION PAPER RELEASED 18 AUGUST 2017

September 2017

Consumers Health Forum of Australia (2017)
Response to Discussion Paper – Independent Review of Health Providers' Access to Medicare Card Numbers
Canberra, Australia

P: 02 6273 5444
E: info@chf.org.au

twitter.com/CHFofAustralia
facebook.com/CHFofAustralia

Office Address
7B/17 Napier Close,
Deakin ACT 2600

Postal Address
PO Box 73
Deakin West ACT 2600

Consumers Health Forum of Australia is funded by the Australian Government as the peak healthcare consumer organisation under the Health Peak and Advisory Bodies Programme

CONTENTS

Contents

Overview

The Consumers Health Forum of Australia (CHF) is the national peak body representing the interests of Australian healthcare consumers and those with an interest in health consumer issues. CHF works to achieve safe, quality, timely healthcare for all Australians, supported by accessible health information and systems.

CHF welcomes the opportunity to provide this submission in response to the Discussion Paper released by the Independent Review of Health Providers' Access to Medicare Card Numbers.

CHF agrees with the Discussion Paper that there is a balance to be struck between security protections surrounding health professionals' access to patients' Medicare card numbers to avoid unauthorised, inappropriate or fraudulent use, and timely access to Medicare benefits for patients who are unable to present their Medicare card at the time of service.

Particular considerations for CHF are as follow:

- The July 2017 media reports of illegal selling of Medicare card numbers on the Dark Web suggest that current controls for access to others' Medicare card numbers need to be tightened, and possible weaknesses rectified, within the Health Professional Online Services (HPOS) system and the arrangements for the Medicare provider enquiries line.
- Individuals who are unable to present their Medicare card at the time of service typically have understandable reasons for being in this situation, while possibly also being financially unable to meet the whole cost of the service provided out of their own pocket at the time of the service. For example, these individuals may be acutely or chronically unwell, homeless, escaping family violence, or under other significant stress for whatever reason. As the Discussion Paper notes, Medicare is Australia's universal healthcare system, providing all Australians with access to timely and affordable healthcare. It is important that individuals who are unable to present their Medicare card at the time of service are not disadvantaged by changes to the HPOS system.
- CHF supports the move to a national opt-out approach to the implementation of My Health Record, as well as measures which genuinely address consumers' legitimate security concerns in relation to the My Health Record system. It would be unfortunate if inappropriate access to Medicare card numbers, as highlighted by the July 2017 media reports, reduced public confidence in the My Health Record system.

Comments in response to consultation questions

CHF provides the following responses to the consultation questions in the Discussion Paper, and the possible recommendations flagged by the Review Panel.

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

The Discussion Paper explains that under current arrangements, a health professional does not have to obtain a patient's consent before obtaining their Medicare card number through HPOS or the Medicare provider enquiries telephone line.

Informed patient consent is a fundamental principle in health service delivery. CHF believes that obtaining patient consent should be an explicit requirement for a health professional to obtain the patient's Medicare card number particularly for instances where the patient is otherwise unknown to the practice. The form of this consent should be meaningful, but kept simple and uncomplicated. It is preferable if this is done using a standard consent form which the patient signs to ensure consistency. In instances where the patient is known but does not have their Medicare card on a particular occasion, it would be our expectation and assumption that it is common place for practices to take a record of a patient's Medicare number and could refer to that in order to access it.

2 – What identifying information should patients have to provide to access health services?

CHF notes the possible recommendation that individuals who wish to claim a Medicare benefit should have to present proof of identity, in addition to a Medicare card, when they first attend a health service. However, CHF requires further information about the need for, and implications of, this recommendation.

CHF agrees with the Discussion Paper that:

- "limiting access to Medicare services to those who are able to produce a Medicare card may restrict access to health services by vulnerable people who are eligible for Medicare services but are unable to present a card for a range of reasons" (page 7);
- "requiring patients to present a Medicare card could also increase the risk that people will attempt to obtain Medicare cards fraudulently", and "if this occurs and Medicare items are applied to the wrong person's Medicare card, this will be reflected in an individual's Medicare claiming history and potentially in their My Health Record" (page 8).

The Discussion Paper then concludes that "these risks could be reduced if people are required to present another form of identification when they first attend a health service". While the Discussion Paper proposes that individuals would still be able to access Medicare benefits for urgent or emergency treatment even when they are unable to present identification, identification "would be required in most circumstances for non-urgent or longer-term treatment" (page 8).

There needs to be clarity on what forms of proof of identity would be acceptable, i.e. a predetermined list for practices/consumers to choose from. It should not require the often quoted "100 points" used in banking and some other areas. We do not want to set the bar too high as this would risk this new requirement becoming an additional barrier to access to care.

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

CHF notes that a range of HPOS access controls are currently in place to protect Medicare information and prevent fraudulent access. However, the July 2017 media reports of illegal selling of Medicare card numbers on the Dark Web suggest that current HPOS access controls are not sufficient and need to be tightened.

The Discussion Paper indicates the media reports "alleged that the Dark Web vendor was 'exploiting a vulnerability' in a government system that allowed access to Medicare card details, enabling the vendor to supply the card number of any Australian following provision of their name and date of birth" (page 3). While CHF is not aware that it has been definitively confirmed that HPOS was the source of the July 2017 breach, this possibility needs to be addressed and changes implemented to remove this risk.

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 professions to accept it as a replacement?

CHF would support a recommendation that the Department should accelerate its current plans to move healthcare providers from Public Key Infrastructure (PKI) individual certificates to Provider Digital Access (PRODA) accounts, and should develop a PRODA-based alternative to PKI site certificates. As PRODA accounts are already being used by some health professionals to access the HPOS system, and given the descriptions in the Discussion Paper of the PKI and PRODA processes suggest both involve minimal steps for users, such a recommendation would appear reasonable.

CHF notes that based on advice received, the Review Panel considers that three years is a reasonable timeframe for all PKI certificate holders to transition to PRODA.

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?

It is concerning that currently HPOS users may continue to have access to HPOS when they no longer need it. CHF would support a recommendation that PRODA accounts and PKI certificates should be suspended if they have not been used for a certain period.

In relation to the appropriate length of the period of inactivity which would trigger suspension, and the processes or alerts that would need to be put in place, CHF expects that there may be relevant industry benchmarks or experiences from other systems. In addition, the period of inactivity would need to be longer than the typical periods of annual leave taken in a block by HPOS users. It may also be possible to examine the general frequency and pattern of HPOS

use to determine the appropriate length of the period of inactivity which would trigger suspension (for example, if most users access HPOS at least once every three months, the critical period of inactivity would need to be longer than that). A simpler process for previous HPOS users to reactivate their PRODA accounts and PKI certificates if required (for example, if a user returns to the same or a different medical practice after an extended period of leave or break in employment) may also be possible and appropriate.

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?

It is also concerning that currently HPOS delegations may not be reviewed and removed when staff members cease employment or change roles. CHF would support a recommendation that HPOS delegations should only be in place for a set period, after which they would be automatically removed if not renewed by the provider.

In relation to the appropriate length of the period after which removal would occur, CHF notes the suggestion of 12 months in the Discussion Paper. The introduction of a set period for delegate arrangements should be supplemented by additional prompts to health professionals within the system encouraging them to review their delegations and remove any which are no longer required.

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 higher level of scrutiny?

CHF would support a recommendation that would limit the availability of batch Find a Patient requests, for example by reducing the number of patients whose details can be requested or by limiting who can make these requests. The current limit of 500 requests seems very high and too generous.

The Discussion Paper does not indicate how often the batch request feature is used currently, for example, as a proportion of all requests. It would be reasonable for batch requests to be subjected to a higher level of scrutiny than single requests.

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

CHF notes that the current security check on the Department's provider enquiries line is based on information that could potentially be obtained by a third party. CHF would support a recommendation that this security check should be strengthened, and in addition that all callers to the provider enquiries line, including practice staff, must be individually identified.

Given the increased security and auditability of the HPOS system, CHF also agrees that health professionals should be encouraged to make greater use of HPOS, with a view to minimising the number of telephone Medicare card enquiries.

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?

CHF would support a recommendation that the current HPOS, PKI and PRODA Terms and Conditions should be reviewed to ensure that user obligations are clear and prominent, and that they take confidentiality requirements with third parties into account. CHF also agrees that the Terms and Conditions could be strengthened to reflect user obligations when providing third parties, such as IT or other service providers, with system access.

We all know that in general, online terms and conditions are often accepted quickly with no real review of them by the user. This is accentuated by the frequent use in online terms and conditions of overly legalistic terminology, and generally reader-unfriendly language. The obligations of users of HPOS, PKI and PRODA to protect Medicare card information need to be clear, unambiguous and expressed in plain English that can be understood by all users, including those not of an English-speaking background.

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

CHF notes that given the widespread use of Medicare cards as a secondary form of evidence of identity, and the fact that they are not sufficient on their own to verify an individual's identity, the Review Panel is likely to recommend that there should be no change to the use of Medicare cards as a form of evidence of identity.

It is not explained in the Discussion Paper whether there are security risks associated with Medicare cards' current widespread use as a form of evidence of identity. It is unclear whether the use of Medicare cards in this way might be responsible for the alleged breach related to a number of Medicare card numbers in July 2017. Is this a concern or is it not? In addition, the Discussion Paper does not outline what other secondary forms of evidence of identity are available, which makes it difficult to know how easy it might be for individuals to not use their Medicare card for this purpose.

Given these gaps in the Discussion Paper, it is difficult for CHF to respond to this consultation question.

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

CHF would support in-principle a recommendation that the Government should work to increase public awareness of why it is important for individuals to protect their Medicare card

information, and the steps they can take to safeguard this information. However, CHF also considers that changing the HPOS system so that the patient's consent is required before obtaining their Medicare card number through the HPOS system or the Medicare provider enquiries telephone line (see consultation question 1) would be essential before any attempts to increase public awareness about protecting Medicare card information. It would be inconsistent to encourage individuals to be confident about questioning whether their Medicare card information is really required and how it will be protected, including how it will be stored and how it will be destroyed when it is no longer required, but while also not requiring patient consent before a health professional can obtain a patient's Medicare card information through HPOS or the telephone line.

CHF would also support a recommendation aimed at encouraging organisations (such as schools and childcare centres) to consider whether they really need to collect Medicare information, and if they do, to ensure that they store this information securely and destroy it when it is no longer required. CHF notes that this encouragement would be consistent with organisations' obligations under the *Privacy Act 1988*. Such encouragement would also complement any attempts to increase the general public's awareness of the need to protect Medicare card information.

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

As mentioned already (see consultation question 3), the Discussion Paper indicates that the July 2017 media reports of illegal selling of Medicare card numbers "alleged that the Dark Web vendor was 'exploiting a vulnerability' in a government system that allowed access to Medicare card details, enabling the vendor to supply the card number of any Australian following provision of their name and date of birth" (page 3).

CHF is unclear whether the Government is certain that HPOS or the telephone line was the source of the July 2017 breach, and is concerned that the possibility of other sources is not being explored to ensure that all possible vulnerabilities are being identified and addressed.