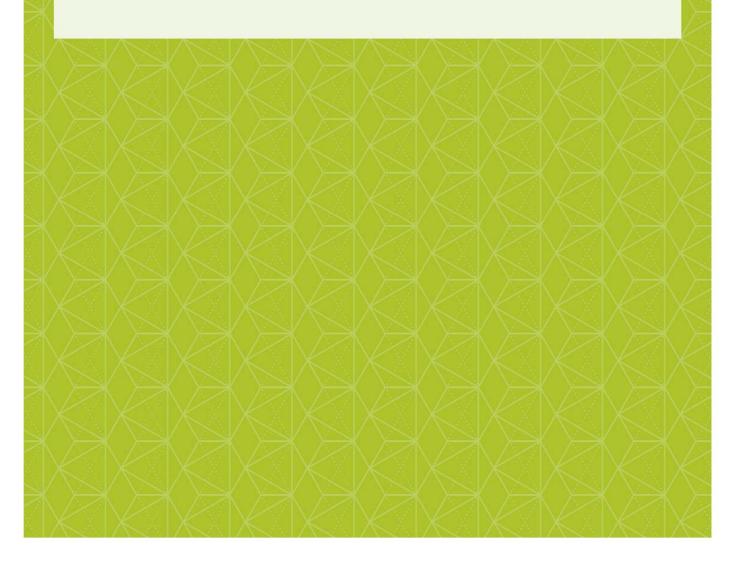# Australian College of Nursing

ACN submission response to the discussion paper released by the Independent Review of Health Providers' Access to Medicare Card Numbers.

ACN submission in response to the discussion paper released by the Independent Review of Health Providers' Access to Medicare Card Numbers.

1 Overview

The Government's response to the alleged sale of a small number of Medicare numbers on the dark web needs to be proportionate and considered and in developing any policy changes, it must ensure that health consumers, in particular vulnerable health consumers, do not have their access to medical care compromised. Indigenous health consumers, homeless people, people with mental health conditions and those living on low incomes already face significant barriers to accessing care.

While not seeking to downplay the significance of the alleged sale of Medicare numbers, the allegations must be put into perspective. Every day there are numerous health service provider interactions with more than 46,000 HPOS and greater than 28,000 Health Professional Online Services (HPOS) confirmations of Medicare details. There has been no evidence of a systemic problem and no evidence that patients' health information has been compromised to date.

It is important that systems are in place to protect Medicare data and Medicare has safeguards in place and hospitals, medical practices, and health professionals take the privacy of patient information very seriously.

2 Responses to the review's consultation questions

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

ACN believes that the general public do not have sufficient awareness of access and control of their Medicare card details. For example, a health professional does not have to obtain a health consumer'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 Services Medicare provider enquiries telephone line.

Recommendations:
- ACN recommends that consent should be a requirement for a health service provider to access a health consumer's Medicare card details in non-urgent or long-term treatment care.
- The process for 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.
- Consent should not hamper urgent or emergency treatment.
- My Health Record is a secure online summary of an individual's health information. The existing audit records 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 a health consumer upon request.
- Audit records 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.

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

An appropriate control to verify whether a health consumer is eligible to access Medicare funded services is for the individual to present their Medicare card and a proof of identity. *This process should not hinder the provision of care especially urgent or emergency treatment.*

ACN supports the review panel's proposal indicating a health consumer must present 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.

ACN recommends 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 and homeless people.

The acceptable identification should conform to the 'very high' level of assurance as outlined in the Attorney-General's Department's 2016 *National Identity Proofing Guidelines*.[1]

Such a requirement should be a legal condition required to be met in order to lodge a Medicare claim. ACN recommends that the Australian Government consider moving toward the implementation of more secure Medicare cards similar to those used in Canadian provinces.

The Australian Government should also consider how it could utilise emerging technology, such as fingerprint authentication.

Recommendations:

- ACN supports the review panel's proposal indicating a health consumer must present 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.
- ACN recommends 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 and homeless people.
- ACN recommends the Australian Government should also consider moving toward the implementation of more secure Medicare cards similar to those used in Canadian provinces.
- The Australian Government should also consider how it could utilise emerging technology, such as fingerprint authentication.

---

[1] Attorney-General's Department 2016, *National Identity Proofing Guidelines*, Commonwealth of Australia, <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/NationalIdentityProofingGuidelines.PDF>.

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

ACN members believe there are issues with the current access controls. A health service organisation can 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 staff working within the registered organisation.

ACN believes that each individual within a registered organisation who accesses HPOS should have their own individual log in details (This is the current practice with the Provider Digital Access (PRODA) system to access HPOS).

Recommendation:

- ACN believes that each individual within a registered organisation who accesses HPOS should have their own individual log in details.

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

ACN supports the move to PRODA as soon as possible. To encourage this, the Government needs to ensure that PRODA meets the needs of system users by enhancing the functionality of PRODA to also enable secure messaging, business transactions and data exchange between providers and Medicare Australia and other authorised parties approved by Medicare Australia. PRODA is a more secure system with its two-step verification process, requiring a username, password and verification code to log in. In a mobile, digital, online and cloud based world physical certificates tied to a physical address are restrictive and limiting. Our members suggest and support that all new HPOS users only being able to apply for a PRODA account. Transition to PRODA would need to be managed carefully with well managed change management program supported by a thorough communication plan. ACN believes the three-year time period being considered by the review panel is too long a timeframe considering health consumer's expectations around current cyber security concerns and acknowledging the change management processes that are required.

Recommendations:

- That PRODA meets the needs of system users by enhancing the functionality of PRODA to also enable secure messaging, business transactions and data exchange between providers and Medicare Australia and other authorised parties approved by Medicare Australia.
- All new HPOS users only being able to apply for a PRODA account.
- Transition to PRODA would need to be managed carefully with a well-managed change management program supported by detailed communication.

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?

In relation to suspending inactive PRODA accounts and PKI site certificates our members are uncertain what problem this proposed action would be addressing. Inactive PRODA or PKI site certificates are not a threat to the system as no one would be using them. There are several reasons why PRODA or PKI certificates may be inactive but still be required.

For example, a holder may be on extended sick leave, or temporarily not providing services or out of the country.

PKI certificates in particular are onerous to obtain and install. Once a provider has set up their details and delegates they may have no need for further interaction unless any of their personal or practice details change or a change to their delegations is required. Most interactions with HPOS are undertaken by the provider's delegates. Particularly, in the case of general practitioners, whose time is far better spent seeing health consumers than completing administrative tasks.

Suspending PRODA or PKIs of practice principals could cause their delegates to lose access, adding an administrative burden to practices.

If suspension or expiratory dates for PRODA are implemented ACN recommends the Department notifies holders so they are given the opportunity to confirm their PRODA account or PKIs are still required. Any suspension should be easily reversed. 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.

Recommendations:

- If suspension or expiratory dates for PRODA are implemented ACN recommends the Department notifies holders so they are given the opportunity to confirm their PRODA account or PKIs still required.
- Any suspension should be easily reversed.
- PRODA accounts should expire, especially after a pre-determined period of inactivity and the Provider should be warned of expiratory date.
- PKI certificates should be phased out over a period as noted in 2.4.

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, ACN supports that delegations should be in place for a set time period, after which they will be automatically removed if not renewed by the provider or if they are inactive. Consider a 12 months' duration.

Recommendation:

- ACN supports that delegations should be in place for a set time period, after which they will be automatically removed if not renewed by the provider or if they are inactive. (Consider 12-month duration).

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?

ACN members report that batch requests are usually made generally for the purpose of claiming bulk billed items or processing claims on behalf of the health consumer. The information in the discussion paper is insufficient to inform an opinion about the need for further conditions on batch requests. If the discussion paper could have provided some information as to how often batch requests are run, by whom and what the average volume of requests are, this information could then be used as the basis for any discussion about reducing the number of requests allowed.

Recommendation:

- ACN recommends that any unusual behaviour from a health service with regards to batch requests should be identified by the Department of Human Services and investigated.

2.8 Could the provider enquiries line be made available in more limited circumstances?

ACN believes that the Providers Enquiry Line currently represents a significant risk for duplicitously obtaining Medicare numbers. The information required for a phone enquiry is readily available to anyone who has been provided a service by a medical practice. An alternative for strengthening the security around phone confirmations of Medicare numbers would be to provide each practice with an Identification Number and perhaps an access PIN, similar to that used in telephone banking arrangements. This information could be then used to verify that the enquiry is authentic.

Health service providers should be required to obtain the health consumer consent to access Medicare details in order to obtain Medicare benefits. In the case of emergency treatment individual consent could be waived.

Recommendations:

- Obtaining consent should be with as little administrative burden as possible while balancing the need for integrity of the health system and access to Medicare cards.
- ACN recommends that audit records 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 individual request.
- An alternative for strengthening the security around phone confirmations of Medicare numbers would be to provide each practice with an Identification Number and perhaps an access PIN, similar to that used in telephone banking arrangements. This information could be then used to verify that the enquiry is authentic.
- Health service providers should be required to obtain the health consumer consent to access Medicare details in order to obtain Medicare benefits. In the case of emergency treatment individual consent could be waived.

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?

ACN supports reminding organisations of their obligations to protect Medicare information, recognising that it should be an ongoing focus of the Department of Human Services. Reviewing the HPOS and any changes to HPOS Terms and Conditions must not increase the administrative burden on service providers.

HPOS provides health professionals and their delegates with streamlined and secure access to Medicare Australia and Department of Human Services programs, services, tools and resources. Our members report that this not only facilitates service provider engagement with the Department and its programs, it also supports secure transfer of data and timely access to information. If HPOS becomes more burdensome service providers may cease to use it. This would add significantly to the costs of business for Government and providers alike through the use of less efficient process and systems. For example, if general practices are not able to readily access a health consumer's eligibility for Medicare, or to verify a Medicare rebate is payable for a particular health service (e.g. Health Assessment or GP Management Plan) they are more likely to bill the patient directly to ensure they are not out of pocket for providing the service.

Recommendation:

- ACN 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, and 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?

ACN supports the continued use of a Medicare card as a secondary evidence of identity, noting it is issued by the Australian Government and in such circumstances is used in conjunction with other forms of identification.

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.[2]

Recommendation:

- The Australian Government should consider moving toward more secure Medicare cards similar to those used in Canadian provinces.

---

[2] Researchomatic 2010, *Integration of Smart Cards into Canada Health Care System*, <http://www.researchomatic.com/Integration-Of-Smart-Cards-Into-Canada-Health-Care-System-16341.html>.

ACN submission: in response to the discussion paper released by the Independent Review of Health Providers' Access to Medicare Card Numbers.

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

ACN supports the concept of an awareness raising campaign so that patients understand the importance of the Medicare card in accessing their Medicare entitlements and that they should not share the information on their card inappropriately. The Australian Government should undertake an ongoing communications campaign utilising a number of strategies across numerous platforms. For example, posters and signage at point of use within a health service could increase awareness.

> **Recommendation:**
>
> - The Government should undertake an ongoing communications campaign utilising a number of strategies across numerous platforms. For example, posters and signage at point of use within a health service to increase awareness.

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?

The information in the discussion paper is insufficient to inform a discussion about the need for further conditions on batch requests. If the discussion paper could have provided some information as to how often batch requests are run, by whom and what the average volume of requests are, this information could then be used as the basis for any discussion about reducing the number of requests allowed.

3 Conclusion

ACN applauds the work of the Australian Government's independent review of health providers' access to Medicare card numbers and recommends the following for actions:

- ACN recommends that consent should be a requirement for a health service provider to access a health consumer's Medicare card details in non-urgent or long-term treatment care.
- The process for 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.
- Consent should not hamper urgent or emergency treatment.
- My Health Record is a secure online summary of an individual's health information, the existing audit records 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 a health consumer upon request.
- Audit records 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.
- ACN supports the review panel's proposal indicating a health consumer must present 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.
- ACN recommends 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. ACN recommends the Australian Government should also consider moving toward the implementation of more secure Medicare cards similar to those used in Canadian provinces.
- The Australian Government should also consider how it could utilise emerging technology, such as fingerprint authentication.

- ACN believes that each individual within a registered organisation who accesses HPOS should have their own individual log in details.
- That PRODA meets the needs of system users by enhancing the functionality of PRODA to also enable secure messaging, business transactions and data exchange between providers and Medicare Australia and other authorised parties approved by Medicare Australia.
- All new HPOS users only being able to apply for a PRODA account.
- Transition to PRODA would need to be managed carefully with well managed change management programs supported by detailed communication.
- If suspension or expiratory dates for PRODA are implemented ACN recommends the Department notifies holders so they are given the opportunity to confirm their PRODA account or PKIs are still required.
- Any suspension should be easily reversed.
- PRODA accounts should expire, especially after a pre-determined period of inactivity and the Provider should be warned of expiratory date.
- PKI certificates should be phased out over a period as noted in 2.4.
- ACN supports that delegations should be in place for a set time period, after which they will be automatically removed if not renewed by the provider or if they are inactive. (Consider 12-month duration).
- ACN recommends that any unusual behaviour from a health service with regards to batch requests should be identified by the Department of Human Services and investigated.
- Obtaining consent should be with as little administrative burden as possible while balancing the need for integrity of the health system and access to Medicare cards.
- ACN recommends that audit records 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 individual request.
- An alternative for strengthening the security around phone confirmations of Medicare numbers would be to provide each practice with an Identification Number and perhaps an access PIN, similar to that used in telephone banking arrangements. This information could be then used to verify that the enquiry is authentic.
- Health service providers should be required to obtain the health consumer consent to access Medicare details in order to obtain Medicare benefits. In the case of emergency treatment individual consent could be waived.
- ACN 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, and 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.
- The Government should undertake an ongoing communications campaign utilising a number of strategies across numerous platforms. For example, posters and signage at point of use within a health service.

Acronyms and Basic Terms

Department – Department of Human Services

Health professional – The term 'health professional' is used to refer to health service providers (such as nurses, doctors, and allied health professionals) as well as administrative and support staff in this document.

Government – Australian Government

HPOS – Health Professional Online Services

My Health Record - My Health Record is a secure online summary of individual health consumer's health information. The health consumer can control what goes into it, and who is allowed to access it. They can choose to share their health information with their health care providers.

PKI – Public Key Infrastructure

PRODA – Provider Digital Access