Discussion Paper

Independent Review of Health Providers' Access to Medicare Card Numbers

Professor Peter Shergold AC

Dr Bastian Seidel, President, Royal Australian College of General Practitioners

Dr Michael Gannon, President, Australian Medical Association

Dr Kean-Seng Lim, Australian Medical Association

Contents

1 Terms of Reference

(As announced on 10 July 2017 by the Minister for Health, the Hon Greg Hunt MP, and the Minister for Human Services, the Hon Alan Tudge MP)

Background

The Government is commissioning a review of health professional access to Medicare card numbers via the Health Professional Online Services (HPOS) system and the telephone channel.

HPOS offers health providers a single secure web portal giving real-time access to a number of online services provided by the Department of Human Services, including looking up or verifying a patient's Medicare number.

HPOS was introduced in 2009, and supports the accessibility of medical care in cases where a patient may not have their Medicare card with them. HPOS provides an alternative avenue to the existing telephone channel for a health professional to identify a patient's eligibility for Medicare benefits.

The Medicare number is a central component of Australia's Health system. It provides all Australians with timely access to healthcare regardless of their location. The Medicare number has also, in recent times, become an important component of Australia's proof of identity processes.

This Review follows recent public discussion about an alleged privacy breach related to Medicare numbers.

Scope of Review

The Review will consider the balance between appropriate access to a patient's Medicare number for health professionals to confirm Medicare eligibility, with the security of patients' Medicare card numbers.

The Review will examine and advise on:

- The type of identifying information that a person should be required to produce to access Medicare treatment in both urgent and non-urgent medical situations
- The effectiveness of controls over registration and authentication processes at the health provider's premises to access Medicare card numbers
- Security risks and controls surrounding the provision of Medicare numbers across the telephone channel, and the online connection between external medical software providers and HPOS
- The sufficiency of control by patients and the appropriateness of patient notification regarding access to their Medicare number
- The adequacy of compliance systems to identify any potential inappropriate access to a patient's Medicare number
- Any other identified area of potential weakness associated with policy, process, procedures and systems in relation to accessibility of Medicare numbers.

Based on the examination of the issues above, the Review will make recommendations for immediate practical improvements to the security of Medicare numbers while continuing to ensure people have access to the health care they need in a timely manner.

The Review may also provide recommendations for medium to longer term changes (or at least the identification of areas that require further examination) to ensure the security of the system and protection of information of Australians.

The Review will work closely with relevant stakeholders including the Australian and State and Territory Governments and peak industry bodies (including the Australian Medical Association, the Royal Australian College of General Practitioners, the Australian Association of Practice Managers, and the Consumers Health Forum).

Timing and Resources

The Review will be supported by a secretariat comprised of officials from the Australian Government Departments of Human Services, Health, and Attorney-General's.

The Review will commence immediately, provide an interim report by 18 August, and a final report by no later than 30 September 2017.

2 Introduction

2.1 Rationale for Review

On 10 July 2017, the Commonwealth Government commissioned a Review of Health Providers' Access to Medicare Card Numbers (the Review). The Review was commissioned to consider the balance between appropriate access to Medicare card numbers for health professionals[1] to confirm patients' Medicare eligibility, with the security of patients' Medicare card numbers. The Review will identify options to improve the security of Medicare card numbers while continuing to support access to health services and without unnecessarily increasing the administrative workload faced by health professionals.

Medicare is Australia's universal healthcare system, and is the cornerstone of public healthcare in Australia, providing all Australians with access to timely and affordable healthcare regardless of their location. Every day, thousands of Australians use their Medicare cards to access essential medical, allied and other health services funded through Medicare. Under current arrangements, health providers are able to obtain their patients' Medicare card numbers from the Department of Human Services (the Department) using online or telephone channels. These arrangements ensure healthcare remains accessible even for vulnerable individuals who may not be able to present their Medicare card.

The Review was commissioned following media reports of an alleged breach related to a number of Medicare card numbers. On 4 July 2017, media outlets reported that a Dark Web[2] vendor was illegally selling Medicare card numbers.[3] The media report alleged that the 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.

The Government and Department are taking this media report, and the security of Medicare card information, seriously. The incident has been referred to the Australian Federal Police (AFP), which has commenced an investigation. This Review, which is separate to the AFP investigation, will provide the Government with an independent, external perspective on current vulnerabilities in the system, and how these can be addressed so that Medicare card information is better protected. The reported sale of Medicare card numbers highlights the fact that the Medicare card has become an important component of Australia's proof of identity processes. The Medicare card can be used to help verify an identity and, like any evidence of identity credential, is therefore susceptible to theft for identity fraud and other illicit activities. Illegally obtained Medicare card numbers could also potentially be used for fraudulent Medicare claiming or enable ineligible individuals to access Medicare related health services. While it is clear that patients' medical records have remained secure, there is a danger that inappropriate access to Medicare card numbers might reduce public confidence in the My Health Record system.

The Review will consider how best to balance the need for access to health services with the controls required to ensure the security of Medicare card numbers. Drawing on stakeholder consultation (based on the consultation questions in this paper), the Review will consider the effectiveness of existing controls surrounding the provision of Medicare card numbers and the

[1] In this paper, 'health professional' is used to refer to health service providers (such as doctors or allied health professionals) as well as administrative and support staff.
[2] The Dark Web is a small portion of the internet that is intentionally hidden and can only be accessed using specific software, not through standard web browsers. The Dark Web is often used for illicit activities including the creation of marketplaces for the sale and trade of drugs, human trafficking and malware. The Dark Web makes users more anonymous and secure, and so hosts more illicit activity than other parts of the web.
[3] Farrell, P. 2017 'The Medicare Machine: Patient Details of 'Any Australian' for Sale on Darknet', *The Guardian Australia*, accessed at https://www.theguardian.com/australia-news/2017/jul/04/the-medicare-machine-patient-details-of-any-australian-for-sale-on-darknet.

adequacy of compliance systems to identify inappropriate access. It will also take into account the type of information a patient should be required to produce to access Medicare services, and whether patients have sufficient knowledge about, and control over, access to their Medicare card number.

The Review will focus on the channels identified in the Terms of Reference: HPOS and the Department's Medicare provider enquiries line.

The Review will present a final report to Government by early October 2017. This report will present recommendations for immediate practical improvements, and may also identify medium to longer term changes to improve the balance between the security and accessibility of Medicare card numbers.

The Review is being led by Professor Peter Shergold, supported by Dr Bastian Seidel, President of the Royal Australian College of General Practitioners (RACGP), and Dr Michael Gannon, President of the Australian Medical Association (represented by Dr Kean-Seng Lim as proxy).

2.2 Stakeholder consultation

The Review Panel is keen to obtain the views of stakeholders about the issues identified in the Terms of Reference. This discussion paper is intended to guide stakeholders by posing questions about possible reforms, including where the Review Panel has already identified potential areas for improvement. Each consultation question is followed by background information to provide context for stakeholders. The Review Panel would also welcome more general input about matters within the scope of the Terms of Reference.

Responses to the discussion paper will assist the Review Panel to refine their views as they form their recommendations to Government in their final report.

Submissions may be published at www.humanservices.gov.au/health-professionals/subjects/independent-review-health-providers-access-medicare-card-numbers unless stakeholders request that they be kept confidential.

2.3 Summary of consultation questions

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

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

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

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?[4] Would any enhancements to PRODA be required for health professionals to accept it as a replacement?

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?

[4] To access HPOS, health professionals must authenticate their credentials by either applying for a Public Key Infrastructure (PKI) certificate or creating a Provider Digital Access (PRODA) account. To access HPOS using a PKI certificate, users must install software and the certificate (a USB, smart card or pre-cut card for individual certificates, or a CD-ROM for site certificates), and enter a Personal Identification Code. Accessing HPOS through PRODA involves a two-step verification process, requiring a username, password and unique verification code that is sent to the user on each log-in. Further information on PKI and PRODA is in section 4.3.

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?

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?

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?

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?

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

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

3 Background – health professional access to Medicare card numbers

There are a number of channels a health professional can use to find a patient's Medicare card number when they are unable to present their card, including HPOS, the Department's Medicare provider enquiries telephone line, and practice software. Health professionals can confirm that Medicare card details are correct through the Department's other online claiming channels, but are unable to search for Medicare card details through these channels.

A broad range of health providers can provide Medicare services and may need to access Medicare card numbers for their patients. Health providers who can register with the Department include medical practitioners (general practitioners and specialists), midwives, nurse practitioners and allied health professionals including dentists, optometrists and psychologists. Administrative staff are more likely than the actual providers to seek Medicare card numbers for their patients, as they do more of the administrative tasks within a practice such as claiming and maintaining patient details.

3.1 Health Professional Online Services

The 'Find a Patient' functionality within HPOS allows a health professional to search and confirm a patient's Medicare card number, concessional eligibility and patient details. The health professional is required to enter the patient's first name, surname and date of birth. If more than one person matches the information entered, postcode and/or suburb/locality must be entered to further refine the search. Information will only display if a unique match is found. Once found, the screen will return the correct Medicare card number, Individual Reference Number (IRN), first name and card expiry date.

3.2 Provider Enquiry Line

To obtain a Medicare card number over the telephone, the caller must pass a security check confirming the provider details, and then provide sufficient patient information to identify the patient with their first name, surname, date of birth and address. A health professional can request up to seven Medicare card number details per phone call.

3.3 Practice software

The Department also offers integration for third party software products to facilitate claiming and information exchange between health professionals and the Department.

Software developers can choose to embed a link to HPOS within their software or utilise the Department's Business to Business (B2B) Patient Verification Services. B2B accesses the same patient search service offered through HPOS directly from the third party software, without any requirement for HPOS login.

3.4 Individual access

Alternatively, individuals can access their own Medicare card details if they do not have their card with them. This includes through the Express Plus Medicare mobile app, where an image of the Medicare card can be viewed in the 'Digital Wallet' section. Individuals can attend a Department service centre and request a temporary paper copy of their card. Individuals can also call the Medicare general enquiries line and request their Medicare card number. They must pass a security check before the information is released.

4 Consultation questions

4.1 Patient control and awareness

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

Under current arrangements, a health professional does not have to obtain a patient's consent before obtaining their Medicare card number through the HPOS Find a Patient function or through the Medicare provider enquiries telephone line. When using Find a Patient, the health professional must declare that the search is for claiming purposes only (in other words, that it will be used only for the purpose of lodging a claim for a Medicare rebate) by selecting a check box on the Find a Patient screen before proceeding with a search.

Although there are audit logs of access to Medicare card numbers through HPOS, individuals do not have access to these. There is no audit log of access to Medicare card numbers through the telephone channel.

Although they cannot view who has accessed their Medicare card details, individuals can review their claiming history (available through Medicare online accounts[5]) to see which health professionals have lodged claims on their behalf. 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 suspected customer fraud) or the Department of Health (for suspected provider fraud) for further investigation online or by telephone.

4.2 Access to health services

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

Health professionals currently access Medicare card numbers in order to verify the eligibility of their patients to receive Medicare services, and to lodge bulk bill or electronic patient claims at the practice.[6] In order to receive Medicare services, individuals must be eligible for Medicare.[7] It is important that health professionals are able to access Medicare card numbers and confirm eligibility so that their patients can access subsidised treatment even if they do not have their card with them.

Arguably, the expectation in most cases would be that access to Medicare services should be limited to those who are able to demonstrate their eligibility by presenting their Medicare card. However, 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.

---

[5] Medicare online accounts allow individuals to access a range of Medicare services online, such as viewing their claims history, submitting claims for some services, and updating contact and bank account details. Registration for Medicare online services is through myGov. To link a Medicare online account to myGov, individuals must provide personal information and other details, such as when they last visited a doctor. Further information is at https://www.humanservices.gov.au/customer/services/medicare/medicare-online-accounts.

[6] When a health professional bulk bills a patient, they bill Medicare directly and accept the Medicare rebate as full payment for the service. The patient does not pay any out of pocket costs. Where patients have been charged a full fee for the service, they can claim their Medicare rebate at a health professional's practice, if they offer electronic claiming. Claims can be lodged online or through an EFTPOS device. Depending on the channel, patients may receive their benefit almost immediately, or on the next working day. Processing times are much slower for channels where the patient lodges the claim. In 2016-17, 97.1 per cent of claims were lodged electronically.

[7] To be eligible for Medicare, an individual must be living in Australia or Norfolk Island, and be an Australian citizen, a New Zealand citizen, an Australian permanent resident, an applicant for permanent residency (with some exclusions), covered by a Ministerial order, or a Resident Return visa holder. Most visitors from Reciprocal Health Care Agreement countries may also receive a Medicare card to cover the cost of essential medical treatment. Individuals who do not fall into one of these categories are not eligible for Medicare.

Health services are still available to those who are not eligible for Medicare or where the health professional is unable to confirm their Medicare eligibility, but in these situations the health professional would not be able to bulk bill or lodge a claim electronically on behalf of the patient. This could cause additional problems for individuals who are already experiencing financial hardship, as out of pocket costs could be significant.

Requiring patients to present a Medicare card could also increase the risk that people will attempt to obtain Medicare cards fraudulently in order to access services to which they are not entitled, such as family or friends sharing Medicare cards. 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 Heath Record. These risks could be reduced if people are required to present another form of identification when they first attend a health service.

Patient identification is widely recognised as essential in healthcare settings, and is reflected in safety and quality standards.[8] However, these standards do not require that patients present any proof of identification, either to validate their identity details or to confirm that the Medicare card details being presented are consistent with other identification.

Requiring that people present some other form of identification in addition to a Medicare card when they first attend a health service could provide assurance that they are using their own identity to access healthcare, and that they are eligible to receive a Medicare rebate. However, this could create further barriers to access for individuals who are unable to present identification. A possible solution would be 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.

4.3 HPOS access controls

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

There are existing controls in place surrounding the registration process before health professionals can gain access to HPOS.

To access HPOS, health professionals must authenticate their credentials by either applying for an individual Public Key Infrastructure (PKI) certificate or creating a Provider Digital Access (PRODA) account. The authentication process includes providing evidence of identity and the validation of a provider number. A health service organisation can apply for a PKI certificate, which allows any user of the organisation's software or network to access HPOS, by submitting a PKI site certificate application form. (PRODA does not currently provide organisation-level access to HPOS.) Alternatively, administrative staff can apply for an individual PKI certificate or create their own PRODA account. These staff must also provide evidence of identity.

After applying for a PKI certificate, applicants need to wait for the certificate (a USB, smart card or pre-cut card for individual certificates, or a CD-ROM for site certificates) to be created by the Department's service provider and mailed to them via Australia Post (this can take up to six weeks). The PKI certificate is mailed separately from the Personal Identification Code (PIC), which is the password for the certificate. The user is then required to install software and the certificate on their computer. Where a PKI site certificate is used to access HPOS, the user is required to logon to a computer with the correct software and site certificate and enter the correct PIC. Site certificates

[8] See, for example, the Australian Commission on Safety and Quality in Health Care's *National Safety and Quality Health Service Standards* (available at https://www.safetyandquality.gov.au/wp-content/uploads/2012/10/Standard5_Oct_2012_WEB.pdf) and the RACGP's *Standards for General Practice* (available at http://www.racgp.org.au/your-practice/standards/standards4thedition/safety,-quality-improvement-and-education/3-1/patient-identification/).

can be installed on practice management software or on the organisation's internet browser, and once logged in can be used by anyone using the software or practice network without any requirement for individual sign-in.

PRODA involves a two-step verification process, requiring a username, password and verification code to log in. To register, users are required to create an account (only one account is permitted per person). This involves providing personal identity details (such as name and date of birth), setting up a username and password, and providing a personal and unique email address. They must also verify their identity by providing key information from three Australian Government issued identity documents. Identity documents are verified online in real time using the Document Verification Service (DVS).[9] For successful identity verification, the personal details used to create the account must match the details on the identity documents. Where documents cannot be verified online, applicants must complete a form and provide hard copies of identity documents for manual processing.

To access PRODA, the user must enter their username, password and unique verification code. The verification code is sent via the user's preferred method (either SMS, email or generated on the PRODA mobile app).

4.4 Moving from PKI certificates to PRODA

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?

The Department is in the process of transitioning users of PKI individual certificates to PRODA, as PRODA is a newer technology that provides increased security as well as benefits to the user. PRODA is a portable and digital end to end solution, which is available to anyone who requires access including those in regional and remote communities. It requires no additional hardware or software, and users can self-manage their account details online.

From a security perspective, PRODA provides increased visibility of user access, with improved ability to track activity back to individual users. The security process for registrations is more rigorous than for PKI, with the use of the DVS to verify applicants' identity documents. PRODA's two factor authentication model also provides greater security.

New HPOS users are now advised that they will need to apply for a PRODA account. However, PKI individual certificate holders are still able to access HPOS using this certificate, even if they also have a PRODA account.

Current limitations with PRODA include that it does not provide an equivalent to PKI site certificate functionality.

4.5 Suspending inactive PRODA accounts and PKI certificates

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 do not expire, even when they are no longer active. PKI certificates issued by the Department expire after two or five years, but some practice management software automatically renews PKI certificates before they expire (PKI certificates can only be renewed once). This presents a risk that users will continue to have access to HPOS after it is no longer required. Suspending

[9] The DVS is a secure, online system that enables user organisations to match information on a range of evidence of identity documents against the corresponding record of the document issuing agency.

PRODA accounts and PKI certificates if they have not been used for a certain period would reduce the risk that these accounts could be used inappropriately.

However, should the Department implement such a measure, it will be important to have robust processes to avoid creating administrative burdens for health professionals who have a legitimate need to access HPOS.

4.6 Delegate arrangements

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?

HPOS provides the ability for providers to nominate administrative staff to act as a delegate on their behalf. Delegates must apply for their own security credentials (either a PKI individual certificate or PRODA, as outlined above) before they can be nominated as a delegate.

Where health professionals nominate a staff member to act on their behalf, there is a risk that they will not remove delegations when staff members cease employment or change roles. This means that these individuals could continue to perform functions in HPOS. This risk could be reduced by introducing an expiry period for delegations after which they must be renewed (for example, 12 months), or providing additional prompts to health professionals within the system encouraging them to review their delegates and remove any who are no longer required.

4.7 Batch Find a Patient requests

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?

HPOS Find a Patient allows users to upload a request for multiple Medicare card details. Each file can contain up to 500 requests with a response provided within 24 hours to the secure HPOS mail centre. An existing control in the system means that the Department only accepts one batch request per individual or site per day.

As with other searches through Find a Patient, card details should only be requested for claiming purposes. Batch requests can be used to either obtain patients' card details or confirm the card details provided by patients.

4.8 Provider enquiries line

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?

As well as access through HPOS, providers or their representatives can also obtain Medicare card details for their patients through the Department's Medicare provider enquiries telephone line.

To obtain a Medicare card number over the telephone, the caller must pass a security check. The security check covers the provider's full name, provider number and practice location. This information is then verified against the Department's Provider Directory System. The provider or representative must then provide sufficient patient information to uniquely identify the patient, such as their first name, surname, date of birth and address. If the caller is a practice staff member, they will be asked if they have received permission from the provider to request this information. If so, the enquiry can proceed. However, callers are not required to identify themselves, only to give the details of the provider on whose behalf they are calling.

The provider does not require consent from the patient to obtain the Medicare card number. Up to seven Medicare card numbers can be requested per telephone call.

Once a provider's details are confirmed and the patient's details supplied by the provider uniquely match an individual's Medicare record, the following information can be released to the provider:

- Medicare card number and IRN
- Medicare card expiry date
- Confirmation that the patient is either eligible or not eligible for Medicare on the date of service
- Any restrictions in relation to Medicare services available to the patient.

Telephony staff are instructed never to release a patient's address or other contact details.

The volume of telephone enquiries for Medicare card numbers is comparatively low (approximately 588,000 in 2016-17) when compared to the number of Find a Patient searches through HPOS (approximately 10 million in 2016-17). However, there may be circumstances in which health professionals are unable to use online channels or when the use of telephone channels is more convenient or appropriate.

4.9 Information about health professional obligations

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?

Health professionals have legal obligations to protect their patients' Medicare information. Section 130 of the *Health Insurance Act 1973* (which legislates the Medicare program) indicates that it is an offence for a person to directly or indirectly 'make a record of, or divulge or communicate to any person, any information with respect to the affairs of another person acquired by him or her in the performance of his or her duties, or in the exercise of his or her powers or functions', except if this is required in the course of their duties. Section 135A of the *National Health Act 1953* (which governs the Pharmaceutical Benefits Scheme) has the same provisions, save for making a record of information.

Health professionals are reminded of these obligations through the HPOS Terms and Conditions of Use and Access, which are displayed on every log-on to HPOS.[10] As part of the terms and conditions, users declare that they will comply with their obligations under the *Health Insurance Act 1973* to not make a record of, divulge or communicate protected information (as defined in section 130 of that Act) other than in the course of their duties as a health professional. They also agree that failure to do so may be an offence under that Act.

HPOS users also agree to the following:

- To keep personal information about other persons that they upload to the system or access from the system confidential
- Not to access, disclose, publish, communicate, retain or otherwise deal with personal information except in the course of performing their duties directly related to their access to or use of the system.

PKI and PRODA have their own terms and conditions. The PKI Terms and Conditions[11] include that the certificate holder agrees to:

[10] Available at https://www.humanservices.gov.au/health-professionals/enablers/hpos-terms-and-conditions-use-and-access

[11] The full Terms and Conditions for PKI individual and site certificates are available at https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents.

- Only use their certificate for purposes authorised or approved by the Department
- Take all reasonable measures to keep their certificate secure
- Not provide the certificate to any other person/site
- Promptly notify the Department of the loss, destruction or theft of the certificate
- Promptly notify the Department if they suspect the certificate has been compromised.

The PRODA Terms and Conditions[12] include that the user agrees to:

- Keep their Digital Credential, system secret question and answers, user identification and passwords and secret questions and answers for the PRODA code generator, and any other security details for their access to the system, confidential and secure at all times
- Take all necessary precautions to prevent loss, disclosure, modification or unauthorised use of their Secure Access Details
- Change their system password(s) regularly and when prompted by the system and/or the Department
- Not permit any other person to use their Secure Access Details
- Be responsible for all access to, and use of, the PRODA code generator undertaken on their device with the user identification and password.

Reviewing the terms and conditions to clarify and emphasise user obligations may assist in ensuring health professionals are aware of the requirements when accessing the system. The terms and conditions may need to be more explicit in their references to the sharing of credentials and information with third parties, taking into account the possibility that health service organisations will have arrangements with IT or other service providers that require access to IT systems.

4.10 Medicare cards and identity

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

Unlike some countries, Australia does not have a national identity card. We have a complex system of identity in which around 20 government agencies manage over 50 million documents and credentials that are used as evidence of identity. While the primary purpose of these credentials was in most cases not to serve as evidence of a person's identity, over time they have become increasingly used in this way throughout the community.

In particular, Medicare cards have by convention become one of the credentials most commonly used as evidence of a person's identity, and as such have been recognised as a *secondary* form of evidence in identity verification guidelines for over ten years – most recently in the 2014 National Identity Proofing Guidelines (NIPGs). The NIPGs superseded the 2007 Gold Standard Enrolment Framework[13] and the '100 point check'[14] by providing a more comprehensive, risk-based approach to identity proofing. While the '100 point check' is no longer a mandatory legislative requirement, some businesses and even government agencies still choose to use a point based methodology as the basis for their identity proofing processes.

[12] The full Terms and Conditions for PRODA are available at https://proda.humanservices.gov.au/pia/pages/public/registration/account/createAccount.jsf.

[13] The 2007 Gold Standard Enrolment Framework was designed for the identification of people prior to issuance of government documents that are commonly used as identity documents. It was used as a best practice model for other government and non-government organisations.

[14] The 100 point check was established under the *Financial Transaction Reports Act 1988*, but has not been a mandatory requirement for businesses under Australia's anti-money laundering and counter-terrorism financing regime for over 10 years.

In recognition of their widespread use in the community as evidence of identity, Medicare cards were added to the Document Verification Service (DVS) in 2011. Not only did this help to strengthen the integrity of Medicare cards, it provided a government endorsed method for their verification, including for private sector organisations such as banks and telecommunications providers with legislated customer identification requirements. Medicare cards are now the second most commonly verified document through the DVS: during 2016-17 around 4.6 million or 15 per cent of all DVS transactions were conducted using Medicare data, with more than half (55 per cent) of these conducted by the private sector.

No single document or credential should be relied upon as the evidence of a person's identity. The NIPGs require a combination of primary and secondary documents be used in verifying a person's identity. Medicare cards are not considered as primary documents due to the relatively moderate identity proofing processes undertaken to issue the card, as well as the low-level security features of the card itself and the absence of a photo. They do however play an important part as a form of *secondary* evidence– that is, they help to establish that an identity is being used in the community.

4.11 Protecting individual Medicare card numbers

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

As recent media reports have highlighted, Medicare cards and card numbers have the potential to be used for a range of illicit purposes, such as access to health services by those who are not eligible for Medicare, support for a fraudulent identity, fraudulent Medicare claiming, and as a basis for scams. It is important to note that, however, that an individual's Medicare card number does not in isolation provide access to any clinical information or to an individual's My Health Record.

While government and health professionals have the primary responsibility for protecting Medicare card information, individuals can also play a role.

Individuals are often asked to provide Medicare card information. This could be as a form of identification, or in order to support access to health services in emergency situations (for example, when this information is provided to schools or childcare centres). In most cases, collection of Medicare card information will be for legitimate purposes, and organisations will have appropriate measures in place to protect this information. However, individuals also have a role to play in protecting their own information. They should be confident about questioning whether 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.

4.12 Other comments

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

In section 5, the Review Panel sets out some possible responses to the issues under consideration in the Review. The Review Panel would welcome comments on these areas, particularly where they present issues that are not canvassed in the other consultation questions in this paper.

The Review Panel would also welcome any other comments from stakeholders about health provider access to Medicare card numbers or other matters within the scope of the Terms of Reference for the Review.

5. Possible responses

The reported theft and sale of Medicare card information is a serious issue, which could undermine public confidence in the security of personal information that government holds. Changes will be required to current systems to ensure that this information is protected. The Review Panel has identified a number of measures that could assist in strengthening the security of Medicare card information. As the Review is still in progress, these are not final recommendations, and they may be dropped, refined or supplemented based on stakeholder consultation and further briefings. The Review Panel is keenly aware of the need to balance competing public policy objectives. In the final report, these measures may change, be removed entirely, or be supplemented by other recommendations for action.

Broadly, the areas that Review Panel intends to address in their recommendations fall into four categories:

1. Health professional channels to access Medicare card numbers
2. Protecting the security of Medicare card numbers in the community
3. Identity requirements when accessing health services
4. Use of the Medicare card as evidence of identity.

5.1 Health professional channels to access Medicare card numbers

As outlined above, the Department offers two main channels through which health professionals can obtain Medicare card numbers for their patients: HPOS and the provider enquiries line. The Review Panel has identified a number of potential areas for improvement for both channels.

HPOS

- **Moving HPOS authentication from PKI to PRODA within three years**
  The Review Panel is considering a recommendation that the Department should accelerate its current plans to move healthcare providers from PKI individual certificates to PRODA accounts, and should develop a PRODA-based alternative to PKI site certificates. Based on advice received, the Review Panel considers that three years is a reasonable timeframe for all PKI certificate holders to transition to PRODA.

- **Reviewing the HPOS Terms and Conditions**
  The current HPOS Terms and Conditions, and the Terms and Conditions for PKI and PRODA, detail users' obligations in relation to the proper use of the systems and the sharing of information. The Review Panel is considering a recommendation that these 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. The Terms and Conditions could also be strengthened to reflect user obligations when providing third parties with system access.

- **Suspending inactive PRODA accounts and PKI certificates**
  To reduce the risk that users will continue to have access to HPOS when they no longer need it, the Review Panel is considering a recommendation that PRODA accounts and PKI certificates should be suspended if they have not been used for a certain period. Views are invited as to the appropriate length of the period of inactivity which would trigger suspension.

- **Adding an expiry period for delegations in HPOS**
  To reduce the risk that HPOS delegations are not reviewed and removed when they are no longer required, the Review Panel is considering a recommendation 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. Views are invited as to the appropriate length of the period after which removal would occur.

- **Further conditions for batch Find a Patient requests**
  The Review Panel is considering 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. Views are invited as to the appropriate upper limit on the number of enquiries which can be made in a single batch request.

Provider enquiries line

- **Strengthened telephone security checks**
  The current security check on the Department's provider enquiries line is based on information that could potentially be obtained by a third party. The Review Panel is considering a recommendation that this security check should be strengthened. In addition, the Review Panel is considering introducing a requirement that all callers to the provider enquiries line, including practice staff, must be individually identified.

- **Encouraging health professionals to use HPOS for Medicare card enquiries**
  While the Review Panel recognises that there will be times when health professionals need to use the provider enquiries line, HPOS provides increased security and auditability. The Review Panel will consider how health professionals can be encouraged to make greater use of the HPOS channel, with a view to minimising the number of telephone enquiries.

5.2 Protecting the security of Medicare card information in the community

- **Building public awareness about protecting Medicare information**
  Everyone has a role to play in protecting Medicare. Members of the public need to be confident before sharing their Medicare information that it will be properly protected. The Review Panel is considering a recommendation that 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 important resource.

- **Reminding organisations of their obligations to protect Medicare information**
  The Review Panel is considering 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. This would be consistent with organisations' obligations under the *Privacy Act 1988*.

5.3 Identity requirements when accessing health services

- **Introducing new identity requirements for access to Medicare services**
  The Review Panel is considering a recommendation that individuals who wish to claim a Medicare benefit should have to present proof of identity when they first attend a health service, to verify that they are eligible for Medicare. Individuals would still be able to access Medicare benefits for urgent or emergency treatment even when they are unable to present identification, but identification would be required in most circumstances for non-urgent or longer-term treatment. Views are invited as to whether such a requirement should be regulated by industry bodies or as a legal condition required to be met in order to lodge a Medicare claim.

5.4 Medicare card as evidence of identity

- **Retaining the Medicare card as evidence of identity in the community**
  Medicare cards are widely accepted as evidence of identity in the community, and the Review Panel has considered whether it is appropriate for them to continue to be used for this purpose. Given their widespread use 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 their use as a form of evidence of identity.

The Review Panel would welcome comments on these possible action areas, particularly where they present issues that are not canvassed in the other consultation questions in this paper.

Acronyms and Key Terms

AFP – Australian Federal Police

AHPRA – Australian Health Practitioner Regulation Agency

B2B – Business to Business

Department – Department of Human Services

DVS – Document Verification Service

Health professional – In this paper, 'health professional' is used to refer to health service providers (such as doctors or allied health professionals) as well as administrative and support staff.

HPOS – Health Professional Online Services

IRN – Individual Reference Number

NIPGs – National Identity Proofing Guidelines

PIC – Personal Identification Code

PKI – Public Key Infrastructure

PRODA – Provider Digital Access

RACGP – Royal Australian College of General Practitioners