Final Report

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

The views and opinions expressed in this publication are those of the authors and do not necessarily reflect those of the Australian Government, the Minister for Health or the Minister for Human Services.

© Copyright Commonwealth of Australia, 2017.

The *Final Report of the Independent Review of Health Providers' Access to Medicare Card Numbers* is licensed by the Commonwealth of Australia for use under a Creative Commons Attribution 4.0 International licence with the exception of content supplied by third parties and any images depicting people. For licence conditions see: https://creativecommons.org/licenses/by/4.0/

This report should be attributed as '*Final Report of the Independent Review of Health Providers' Access to Medicare Card Numbers*, Commonwealth of Australia 2017'.

Letter of Transmittal

The Hon Greg Hunt MP

Minister for Health

The Hon Alan Tudge MP

Minister for Human Services

Parliament House

CANBERRA ACT 2600

Dear Ministers,

In accordance with the Terms of Reference issued to me on 10 July 2017, I am pleased to provide you with the Independent Review of Health Providers' Access to Medicare Card Numbers.

As Chair of the Review, I would like to express my appreciation for the contribution made by my fellow Panel members, Dr Bastian Seidel, President of the Royal Australian College of General Practitioners and Dr Kean-Seng Lim, Deputy Chair of the Australian Medical Association Council of General Practice (representing Dr Michael Gannon, President of the Australian Medical Association).

The Panel faced the challenge of balancing diverse public policy interests. On the one hand, it is important to ensure access to treatment by all individuals entitled to subsidised Medicare services and to reduce the administrative burden placed on health professionals. On the other, it is imperative to maintain the privacy of personal information and to reduce the potential for fraud or identity theft.

After careful thought, the Review Panel has made 14 recommendations for your consideration. Our conclusions have been informed by the oral presentations and written submissions of industry and consumer organisations. We are sincerely grateful for the contributions they have made to the Review. I also express the Panel's deep thanks for the work of the secretariat that was drawn from the Departments of Human Services, Health and Attorney-General's. They provided exceptional support.

Yours faithfully,

Professor Peter Shergold AC

29 September 2017

Table of Contents

1 Introduction

1.1 Rationale for Review

On 10 July 2017, the Australian Government commissioned a Review of Health Providers' Access to Medicare Card Numbers (the Review), to consider the balance between appropriate access to Medicare card numbers for health professionals[1] and the security of patients' Medicare card numbers. The Review has considered 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 or subsidised through Medicare. Under current arrangements, health professionals are able to obtain their patients' Medicare card numbers from the Department of Human Services using online and telephone channels. These arrangements ensure healthcare remains accessible even for 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 reports 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 incident was referred to the Australian Federal Police, which has commenced an investigation.

This Review, which is separate to the investigation, was established to provide 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 Review has considered 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 has examined and advised on:

[1] In this report, '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.

- 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 professional'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 Health Professional Online Services (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.

The full Terms of Reference can be found at Appendix A.

Based on the examination of the issues above, the Review has made 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 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 to enable ineligible individuals to access Medicare funded health services. While there has been no risk to patients' health records as a result of the reported sale, there is a danger that inappropriate access to Medicare card numbers might reduce public confidence in the security of government information holdings, such as the My Health Record system.

The Review focused on the channels identified in the Terms of Reference: HPOS and the Department of Human Services' telephone channels. Drawing on stakeholder consultation, the Review has scrutinised the effectiveness of existing controls surrounding the provision of Medicare card numbers and the adequacy of compliance systems to identify inappropriate access. It has also considered 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.

1.2 Review process

The Review was led by Professor Peter Shergold AC, supported by Dr Bastian Seidel, President of the Royal Australian College of General Practitioners (RACGP), and Dr Kean-Seng Lim, Deputy Chair of the Australian Medical Association (AMA) Council of General Practice (representing Dr Michael Gannon, President of the AMA).

The Review Panel met in person and by teleconference throughout the course of the Review. They also had technical briefings from the Department of Human Services, the Department of Health, the

Attorney-General's Department and the Australian Digital Health Agency, as well as demonstrations of HPOS and the Department of Human Services' call centre operations, and a site visit to a general practice.

The Review Panel released a Discussion Paper (which also comprised the interim report for the Review) on 18 August 2017 as the basis for public consultation. Interested stakeholders were invited to provide written submissions by 8 September 2017, and the Review received a total of 24 submissions. A list of organisations and individuals who provided submissions is at Appendix B.

In addition to receiving written submissions, the Review Panel and Secretariat met with a broad cross-section of stakeholder organisations. A list of stakeholder meetings is at Appendix C.

On 9 August 2017, the Senate Finance and Public Administration References Committee announced an inquiry into 'the circumstances in which Australians' Medicare information has been made available on the 'dark web''. While the Review is separate to the Senate inquiry, the Review Panel has considered public submissions and evidence provided to the inquiry where they relate to the Terms of Reference for this Review.

The Review Panel was supported by an Intergovernmental Committee including senior executives from the Department of Human Services, the Department of Health, the Attorney-General's Department and the Australian Digital Health Agency. Secretariat support for the Review was provided by staff from the Department of Human Services, the Department of Health and the Attorney-General's Department.

1.3 Summary of recommendations

The Independent Review faced the challenge of balancing diverse public policy interests. On the one hand, it is important to ensure access to treatment by all individuals entitled to subsidised Medicare care and to reduce the administrative burden placed on health professionals; on the other, it is imperative to maintain the privacy of personal information and to reduce the potential for fraud or identity theft.

After weighing these considerations, the Review Panel has made 14 recommendations. In forming its recommendations, the Review Panel has been mindful of the need for recommendations to be proportionate to the level of risk. This reflected comments from submissions:

> *The Government's response to the alleged sale of a small number of Medicare numbers on the dark web needs to be proportionate. In developing any policy changes, it must ensure that patients, particularly vulnerable patients, do not have their access to medical care reduced. It must also recognise the significant red tape burden already faced by medical practices and not add significantly to this.* – Australian Medical Association

However, the Review Panel has recognised that there is a need to strengthen the security of some of the arrangements for access to Medicare card numbers. This, too, reflected the perspective of a number of submissions:

> *While I appreciate the policy considerations around making this information available to healthcare providers, consideration must also be given to the security of that information and whether the use of personal information in this manner strikes an appropriate balance between achieving policy goals and any impact on privacy.* – Office of the Australian Information Commissioner (OAIC)

Recommendation 1: It is recommended that the Medicare card be retained as a form of secondary evidence for identity purposes.

Recommendation 2: It is recommended that the Department of Human Services, working with industry and consumer organisations, undertakes a public awareness campaign encouraging individuals to protect their Medicare card details, and reminding organisations that hold that information of their obligation to protect it.

Recommendation 3: It is recommended that as a condition of claiming Medicare benefits on behalf of patients, health professionals should be required to take reasonable steps to confirm the identity of their patients when they are first treated.

Recommendation 4: It is recommended that health professionals should be required to seek the consent of their patients before accessing their Medicare numbers through Health Professional Online Services (HPOS) or by telephone.

Recommendation 5: It is recommended that individuals should be able to request the audit log of health professionals who have sought access to their Medicare card number through the HPOS ‘Find a Patient’ service.

Recommendation 6: It is recommended that the Department of Human Services undertake a Privacy Impact Assessment when implementing the Review recommendations, identifying the impact of changes on the privacy of individuals.

Recommendation 7: It is recommended that delegations within HPOS should require renewal every 12 months, with a warning to providers and their delegates three months before the delegation expires.

Recommendation 8: It is recommended that batch requests for Medicare card numbers through HPOS should be more tightly controlled (50 card numbers per batch request, and only one batch request per day), unless healthcare providers apply in writing to the Chief Executive Medicare, demonstrating a clear business need for a higher limit.

Recommendation 9: It is recommended that authentication for HPOS should be moved from Public Key Infrastructure (PKI) to the more secure Provider Digital Access (PRODA) expeditiously, with the transition completed within three years.

Recommendation 10: It is recommended that HPOS accounts that have been inactive for a period of six months should be suspended, following a warning to users after three months of inactivity.

Recommendation 11: It is recommended that the process of opening and reactivating a HPOS account should be administratively straightforward.

Recommendation 12: It is recommended that the Terms and Conditions for HPOS, PKI and PRODA should be simplified and presented to users in a form that ensures that they fully appreciate the seriousness of their obligations.

Recommendation 13: It is recommended that, in order to provide greater security and availability, the Department of Human Services should actively encourage health professionals to use HPOS as the primary channel to access or confirm their patients' Medicare card numbers, and that telephone channels be phased out over the next two years except in exceptional circumstances.

Recommendation 14: It is recommended that, during the phasing down of the telephone channels, conditions for the security check for the release or confirmation of Medicare card information by telephone should be strengthened, with additional security questions having to be answered correctly by health professionals or their delegates.

Detailed findings, including the rationale for each recommendation, are in the following sections of this report.

2 Medicare cards

Medicare is Australia's universal health care system, which gives eligible people access to affordable medical, optometry and hospital care, and, in certain circumstances, other allied health services. A Medicare card demonstrates a person's eligibility to receive Medicare services and lower cost medications under the Pharmaceutical Benefits Scheme (PBS). In 2016-17, the Department of Human Services processed 399.4 million Medicare services and paid Medicare benefits totalling $22.4 billion. In addition, under the PBS, the Department of Human Services processed 207.9 million services and paid benefits totalling $12.4 billion.

2.1 Medicare eligibility

For eligible individuals, Medicare provides access to:

- Free or subsidised treatment by health professionals such as general practitioners, specialists, optometrists, and, in specific circumstances, dentists and other allied health practitioners
- Free treatment and accommodation for public patients in a public hospital
- 75 per cent of the Medicare Benefits Schedule (MBS) fee for services and procedures for private patients in a public or private hospital (not including hospital accommodation and items such as theatre fees and medications)
- Lower cost medications through the PBS.

To be eligible for Medicare, an individual must live in Australia or Norfolk Island, and be:

- An Australian citizen
- A New Zealand citizen
- An Australian permanent resident
- An applicant for permanent residency (conditions apply)[4]
- Covered by a Ministerial order[5]
- A Resident Return visa holder[6].

Citizens or permanent residents of Australian dependency islands (Cocos or Keeling Islands, Christmas Island and Lord Howe Island) are also eligible for Medicare services in Australia.

[4] Applicants for permanent residency must be on a visa allowing them to work, or be able to prove that their parent, spouse or child is an Australian citizen, permanent resident or New Zealand citizen. This does not apply to applicants for Parent visas, who are ineligible unless they are covered by a Reciprocal Health Care Agreement. An applicant for permanent residency whose application is refused by the Department of Immigration and Border Protection remains eligible for Medicare while appealing the decision, as long as they are on a visa allowing them to work or have a parent, spouse or child who is an Australian citizen, permanent resident or New Zealand citizen.

[5] Section 6(1) of the *Health Insurance Act 1973* provides that the Minister for Health can order that a particular person or group of persons be eligible for Medicare even though they would not, by usual eligibility rules, be regarded as eligible. Current Ministerial orders grant eligibility to groups including holders of particular visa types and Australian citizens who have been absent from Australia for up to five years.

[6] A resident return visa is required by current Australian permanent residents, some former Australian permanent residents, and some former Australian citizens, where the travel facility on their current visa has expired or is about to expire, and they want to travel overseas and retain their permanent residency.

Most visitors from Reciprocal Health Care Agreement (RHCA) countries[7] may also receive a Medicare card to cover the cost of essential medical treatment.[8]

Australian residents receive a green Medicare card providing access to full Medicare benefits. Cards are generally issued for a period of five years.

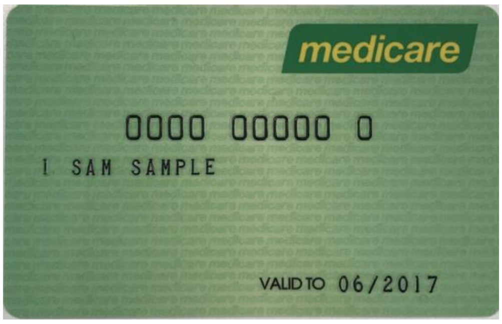


Figure 1: Sample Medicare card

Applicants for permanent residency status and individuals covered by Ministerial orders receive a blue card, which also provides access to full Medicare benefits. The period for which the card is issued is determined by the policy and procedures relating to the particular entitlement type.

Eligible individuals covered by RHCAs may receive a yellow card which entitles them to medically necessary treatment, including treatment as a public patient in a public hospital, depending on the respective arrangements under each RHCA. The period for which the card is issued is determined by the policy and procedures applying to each RHCA country.

At 30 June 2017, 24.9 million individuals were eligible for Medicare, and there were 14.1 million active Medicare cards. The number of Medicare cards is lower than the number of eligible persons because Medicare cards are issued to families, so not every individual has their own Medicare card. 1.4 million individuals were on two Medicare cards. Situations in which an individual may be on two cards include:

- Individuals aged 15 years or older who have their own Medicare card but still remain on their family's card
- Individuals who have their own Medicare card but also appear on their spouse or partner's card
- Children who appear on the Medicare cards of both parents, if the parents have separate Medicare cards.

[7] Australia has RHCAs with Belgium, Finland, Italy, Malta, the Netherlands, New Zealand, Norway, the Republic of Ireland, Slovenia, Sweden and the United Kingdom.

[8] Most holders of subclass 410 (Retirement) visas and subclass 405 (Investor Retirement) visas are not eligible for Medicare under RHCAs. Students from Norway, Finland, Malta and the Republic of Ireland are also not covered by RHCAs. These groups must make their own arrangements to fund their healthcare costs in Australia.

2.1.1 Who is not eligible?

Individuals who are not eligible for Medicare include:

- Australian citizens who have been living overseas for more than five years and cannot provide proof that they have returned to Australia to live
- Visitors to Australia from countries without a RHCA with Australia
- Individuals from RHCA countries who were issued with a subclass 410 (Retirement) visa or a subclass 405 (Investor Retirement) visa after 1998
- People living or working in Australia whose visa type does not entitle them to Medicare, including those on student visas
- Applicants for Parent visas (subclass 103 or 804), unless they are eligible under a RHCA
- Visitors to Australia who have overstayed their visa
- Individuals whose application for permanent residency has been refused and who have not lodged an appeal, unless they are eligible under a RHCA.

Holders of some visa types are required to hold adequate health insurance for the duration of their stay in Australia. All residents and visitors to Australia are encouraged to have adequate health insurance to meet their health needs while in Australia.

2.1.2 Enrolment requirements

When enrolling or re-enrolling in Medicare, individuals have to provide documentation that proves their identity and confirms their eligibility for Medicare. The specific documentation required varies depending on the situation. Required documents may include evidence of identity (such as a birth certificate or passport), evidence of birth (such as a birth certificate or hospital certification), evidence of relationship (such as a marriage certificate or joint bank account), and residency documents demonstrating that an individual is living in Australia or is no longer living in another country. Documents are sighted by Department of Human Services staff during the enrolment process. A full list of acceptable documents is at Appendix D.

Although individuals must be enrolled in Medicare with their legal name, they may choose to have a preferred name printed on their Medicare card. In this case they must supply documents demonstrating that this is a name that they are using in the community.

2.2 Uses of Medicare cards

2.2.1 Intended uses

Medicare cards provide evidence of eligibility for Medicare services. They are designed to be used by those listed on the card for:

- Claiming Medicare benefits
- Seeking medical or hospital treatment, or eye examinations by an optometrist
- Seeking service at a Department of Human Services service centre
- Filling PBS prescriptions.

Medicare cards and Medicare card numbers are administrative. There is no requirement within legislation for the Department of Human Services to issue Medicare cards.

2.2.2 Use as evidence of identity

Although the Medicare card is widely accepted as an identity document, it was not designed to be used as a form of identification. While the *National Health Act 1953* provides a definition of Medicare cards and refers to their use for certain purposes, nothing in that Act or the *Health Insurance Act 1973* refers to a Medicare card as a form of identity verification.

Unlike some countries, Australia does not have a national identity card. Instead, we have a non-centralised 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 main purpose of these credentials was in most cases not intended 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. They have been recognised as a secondary form of evidence of identity in identity verification guidelines for over ten years, most recently in the 2014 National Identity Proofing Guidelines (NIPGs).[9] The NIPGs superseded the 2007 Gold Standard Enrolment Framework[10] and the '100 point check'[11] 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.

The NIPGs recommend a combination of primary and secondary documents be used in verifying a person's identity. Medicare cards are accepted as secondary evidence of identity by the Commonwealth and state and territory governments, as well as by private organisations. For example, Medicare cards can be used in combination with primary forms of identity to obtain a passport, a driver licence, mobile phone contracts, bank accounts, personal loans, rental contracts, police checks and security clearances. Other commonly used forms of secondary evidence include bank statements and utility bills which, like the Medicare card, provide a level of assurance that a particular identity operates in the community.

In recognition of their widespread use as evidence of identity, Medicare cards were added to the Attorney-General's Department's Document Verification Service (DVS) in 2011. 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. In addition to helping to strengthen the integrity of Medicare cards, the DVS provides a government-endorsed method for their verification, including for private sector organisations such as banks and telecommunications providers which have legislated customer identification requirements. The DVS operates 24 hours a day and can provide verification of identity documents within seconds.

[9] Available at https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/NationalIdentityProofingGuidelines.PDF.

[10] 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.

[11] 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 ten years.

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 card data. More than half (55 per cent) of these checks were conducted by the private sector.

Review Panel Recommendation: Medicare cards as evidence of identity

For many Australians, the Medicare card plays an essential role in helping to establish their identity, be it with government or the private sector. Submissions to the Review noted that, in some cases, the Medicare card may be the only form of official identification available:

> *Many of our Aboriginal patients use their Medicare card as their only form of identification – many do not have a Drivers' Licence or a Proof of Identity card. If this was no longer available for use as a form of identification, this would make access to essential welfare services extremely difficult for our patients.* – National Aboriginal Community Controlled Health Organisation

It is the Review Panel's view that any measure taken to prevent Medicare cards being used as a recognised form of secondary evidence of identity, as some submissions have suggested, has the potential to disadvantage certain vulnerable members of the community. It would also have significant impacts on a range of government and private sector organisations, and have a flow on effect on consumers, particularly in the telecommunications sector which has legislated customer identification requirements for pre-paid mobile phones. The education sector would also be significantly affected considering the Medicare card is used to support the issuance of a large number of Unique Student Identifiers.

While Medicare card numbers do hold a degree of value to identity thieves and those that seek to profit from their illegal collections and sale, a Medicare card number cannot be used in isolation to commit identity fraud. Restricting their use as a secondary identifier is therefore unlikely to reduce the prevalence of identity crime. Moreover, other forms of identification commonly used are no more secure.

Nevertheless, identity crime is a serious and growing concern and, due to their widespread use as secondary evidence, Medicare cards are often targeted by identity criminals. A small number of submissions suggested enhancing the security features on the card to reduce the prevalence of their misuse:

> *…the Australian Government should consider moving toward the implementation of more secure Medicare cards similar to those used in Canadian provinces.* – Australian Healthcare and Hospitals Association (AHHA)

The Review Panel noted that while adding a photograph or other security feature such as a hologram might have a short term beneficial impact on the illegal reproduction of Medicare cards, such changes are not likely to have a lasting effect. A more practical and immediate measure is for organisations that accept Medicare cards as evidence of identity to utilise the DVS to confirm that the card and/or number being presented corresponds with a valid and current record held by the Department of Human Services.

Recommendation 1: It is recommended that the Medicare card be retained as a form of secondary evidence for identity purposes.

2.3 Illicit uses of Medicare card numbers

There are a number of ways in which Medicare card numbers that have been obtained inappropriately could be used, such as:

- Access to health services by those who are not eligible for Medicare
- Support for a fraudulent identity
- Fraudulent claiming.

2.3.1 Access to healthcare

Individuals who are not eligible for Medicare may have an incentive to fraudulently obtain a Medicare card number. While Medicare provides access to health services for most Australian residents, some people (as outlined in section 2.1.1) are not eligible for Medicare. These people are responsible for funding their own healthcare, which can involve significant costs. Fraudulently obtaining a Medicare card number could enable them to access subsidised health services, lower cost prescriptions or free care as a public patient in a public hospital.

A related issue is that individuals who are eligible for Medicare could use stolen card details in order to obtain additional services for which they are not eligible; for example, where there are limitations on the number of some services that can be received in a 12 month period, or where individuals are trying to obtain large quantities of prescription medication.

2.3.2 Identity fraud

As outlined in section 2.2.2, it is common practice to accept Medicare cards as a document supporting identity as they provide evidence of an identity operating in the community. While the Medicare card is not sufficient on its own to establish identity, it could be used in conjunction with other documentation to verify an identity. The Medicare card is therefore a known target for identity theft.

Identity theft is a type of fraud that involves the purloining of personal information. This information can be used for many purposes including opening bank accounts, obtaining credit cards or applying for passports. Identity crime continues to be one of the most prevalent crimes in Australia, with an annual economic impact exceeding $2.2 billion.[12] Recent surveys suggest that around four to five per cent of Australians experience a financial loss from identity crime each year.[13]

2.3.3 Fraudulent claiming

Stolen Medicare card numbers could be used to lodge fraudulent claims for services that have not been provided, with Medicare benefits directed into the bank account of the person carrying out the fraud. However, a Medicare number on its own is not sufficient for this type of fraud, as it would require changes to a health professional or individual's bank account details. There are additional safeguards in place against these changes, and the Department of Health and the Department of Human Services have fraud detection programmes in place to assist in identifying this kind of fraud.

[12] Attorney-General's Department 2016 *Identity Crime and Misuse in Australia 2016*, available at https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Trends-in-Identity-Crime.aspx

[13] Ibid.

2.3.4 Limitations of stolen Medicare card numbers

While the theft of Medicare card numbers is a serious issue, it is important to note 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. Some media commentary on the alleged sale of Medicare card numbers associated the availability of Medicare card numbers with the risk of unauthorised access to clinical information or the My Health Record. The Review Panel is not aware of any evidence that this has occurred.

The information for sale through the dark web was limited to individual Medicare card numbers, Individual Reference Numbers (IRNs)[14] and expiry dates. This information is not sufficient to establish or access an existing My Health Record. In addition, this information is not sufficient to access the information that the Department of Human Services holds about an individual, such as details of services, claims or prescriptions received. The Department of Human Services does not hold any clinical information linked with Medicare card numbers.

Review Panel Recommendation: Public awareness

In this information age, Australians are well used to providing information about themselves. It is part of their everyday lives. Yet many do not understand that the information they give out can be taken by others and used in ways they might not have considered. As recent media reports have highlighted, Medicare cards and card numbers are valuable commodities and can be used for a range of illicit purposes. While government and health professionals have the primary responsibility for protecting Medicare card information, individuals should also understand they, too, have a responsibility to protect their own information.

Individuals are often asked to provide their Medicare card information. This could be as a form of identification, or in order to support access to healthcare in emergency situations (for example, when information such as a child's Medicare number is requested by schools, childcare centres or sporting clubs). In most cases, collection of Medicare information will be for legitimate purposes. However, it is not certain that organisations will have appropriate measures in place to protect the information they hold.

Individuals should be encouraged to ask questions about whether their Medicare card information is really required and how it will be protected, including how it will be stored and whether it will be destroyed when it is no longer required.

Review Panel Finding: Information (including personal information about ourselves or our health) is a valuable commodity, yet many Australians readily hand such information to others. Australians are often unaware about what is done with this information, including how it is stored and handled. The Review Panel considers that there is a need for the public to be reminded of the importance of protecting personal information and for organisations to be apprised of their obligation to protect the information they hold.

Most submissions to the Review Panel agreed that people expect government to protect information supplied to them and to maintain systems and security protocols with sufficient safeguards:

[14] The IRN appears next to the cardholder's name and distinguishes each individual named on the card.

> *The security of personal information is not only about ensuring compliance with the requirements of the Privacy Act. It is also essential to ensuring public trust and confidence in the handling of personal information. This is important as the Australian community is increasingly aware of privacy issues, especially in light of new technological advances and information sharing initiatives. People expect government to act transparently when handling their personal information and to keep that information secure. –* Office of Australian Information Commissioner

There was also acknowledgement that there is a need for individuals and organisations to be reminded of issues around security of information and the need to be vigilant in managing records held:

> *The Australian public has a role in reducing the risk of identity theft by safeguarding information. Investment in public awareness and education campaigns on personal information protection strategies will assist in strengthening the security of Medicare information. –* Royal Australian College of General Practitioners

> *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. –* Consumers Health Forum of Australia (CHF)

The Review Panel notes that it will be important for the Department of Human Services to work with peak health and consumer bodies and other stakeholder groups, many of which already have information programmes in place. Agencies such as the Attorney-General's Department have also established information campaigns aimed at protecting identity and the security of information.

While it would be important to use a range of strategies and communication platforms, many of these would be low cost and small in scale. The Review Panel considers that a small investment in public awareness could have a substantial impact, especially if it complements and leverages the information programmes already in place.

Recommendation 2: It is recommended that the Department of Human Services, working with industry and consumer organisations, undertakes a public awareness campaign encouraging individuals to protect their Medicare card details, and reminding organisations that hold that information of their obligation to protect it.

3 Health professional access to Medicare card numbers

3.1 Verifying Medicare eligibility

Health professionals require access to 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.[15] 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. This is particularly important for vulnerable Australians who may not be able to present their card, such as:

- Indigenous Australians in remote localities
- People experiencing homelessness
- People leaving domestic violence situations
- Young people who are still on a family Medicare card and may wish to access health services without their parents' knowledge
- Children in out of home care.

It is important to emphasise that healthcare is still available to those who are not eligible for Medicare or where the health professional is unable to confirm their Medicare eligibility. The health professional may bill the patient in full for the service. If patients are eligible for Medicare, they will be able to lodge a claim with the Department of Human Services to receive their Medicare or PBS entitlements, as long as they can provide a correctly itemised receipt for the services or medications. The receipt does not need to include the patient's Medicare card number. However, the requirement to pay for the service in full, or the longer wait before a rebate is paid, could cause additional problems for individuals who are already experiencing financial hardship.

3.1.1 Proof of Medicare eligibility

Currently there is no specific requirement for patients to provide identification in order to demonstrate they are using their own Medicare card or Medicare details. Correct identification of patients is a priority in healthcare settings, although the focus is patient safety, rather than confirmation that a patient's identity matches the details on the Medicare card. The *National Safety and Quality Health Service Standards*, issued by the Australian Commission on Safety and Quality in Health Care, include a standard specifically related to patient identification, 'Standard 5: Patient Identification and Procedure Matching'.[16] The intention of this Standard is to ensure correct identification of all patients whenever healthcare is provided and correctly match patients to their

[15] 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 practice if the health professional offers 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, claims for 97.1 per cent of all Medicare services were lodged electronically.

[16] Available at https://www.safetyandquality.gov.au/wp-content/uploads/2012/10/Standard5_Oct_2012_WEB.pdf.

intended treatment. In order to meet the Standard, health services are required to use at least three approved patient identifiers when providing care. Approved identifiers include:

- Patient name (family and given names)
- Date of birth
- Gender
- Address
- Medical record number
- Individual Healthcare Identifier.

Similarly, the RACGP 'Standards for General Practice' require three approved patient identifiers, and explicitly note that a Medicare card number is not an accepted identifier.[17]

The problem is that these standards do not require that patients present any form of identification, either to validate their identity details or to confirm that the Medicare card details being presented are consistent with other identification. There is a distinction in healthcare settings between information that is collected to ensure correct patient identification for clinical purposes and that which is collected for billing and administrative purposes.

Review Panel Recommendation: Identity requirements when accessing health services

In the Review Discussion Paper, the Review Panel put forward a possible 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 using their own Medicare card number. Responses to this proposal from the submissions were mixed. Several stakeholders were firmly opposed to the idea:

> *The NT does not support introducing additional identity requirements for this purpose as this has the potential to put added pressure on remote clinics and impact disproportionately on remote (particularly Aboriginal) people. … In short, it would be logistically challenging and impractical to require all patients to provide more than one type of identification aligning to their Medicare card. Further, any such requirement must not be able to be used as a reason to deny access to essential health care.* – Northern Territory (NT) Department of Health

> *It would place an additional administrative burden on practices and put in place an unnecessary barrier to care for patients.* – Australian Medical Association

> *At the outset the Foundation emphasises the fundamental importance of trust as a basic of the delivery of health services to all Australians, including in instances where a recipient may not hold a card or other token of entitlement to services. Respect for that trust through a coherent, principled and effective privacy regime is not antithetical to good governance, efficiency and responsiveness to individual needs.* – Australian Privacy Foundation

[17] Available at http://www.racgp.org.au/your-practice/standards/standards4thedition/safety,-quality-improvement-and-education/3-1/patient-identification/.

> *It is critically important to our member health services, particularly in remote areas, that they continue to have access to clients' Medicare numbers which imposes no additional requirement for identifying people, since many clients do not carry identification.* – National Aboriginal Community Controlled Health Organisation

However, other stakeholders were supportive:

> *To reduce the risk of fraudulent use of Medicare card details, requiring patients to present another form of identification on first registering with a healthcare organisation may be a useful strategy.* – Royal Australian College of General Practitioners

> *The Guild believes that when a Medicare card is used for the first time to receive health services from a prescriber it would not be onerous for that patient to provide some proof as to their identity. This would certainly be helpful to ensure that stolen Medicare cards were not used for 'doctor shopping' or other illegal activity. If a prescriber were to check the identity of the health consumer before writing a prescription then the pharmacist would have confidence that the patient presenting with a PBS prescription were indeed who they claimed to be.* – Pharmacy Guild of Australia

> *An appropriate control to verify whether an individual is eligible to access Medicare funded services is for the individual to present their Medicare card and a proof of identity. … The AHHA supports the review panel's proposal whereby an individual presents identification in order to obtain Medicare benefits for non-urgent or long-term treatment, but allows for urgent or emergency treatment claims if the individual is unable to verify that they are using their own Medicare details. … Such a requirement should be a legal condition required to be met in order to lodge a Medicare claim.* – Australian Healthcare and Hospitals Association

The Review Panel takes the concerns of stakeholders seriously, particularly in relation to not increasing barriers to access to healthcare for disadvantaged populations. However, it also recognises that patient identification is already central to the delivery of healthcare. As outlined above, patient identification is widely recognised as essential in healthcare settings, though the focus is on patient safety, rather than confirming that a patient's identity matches the details on the Medicare card.

Review Panel Finding: Existing requirements around patient identification for clinical safety purposes would be consistent with a requirement that health professionals should be confident of the identity of their patients for Medicare billing purposes, and this should not pose a barrier to care. This would provide assurance that patients are using their own identity to access healthcare, and that they are eligible to receive a Medicare benefit.

Nevertheless, the Review Panel also recognises the additional barriers that may be faced by vulnerable people if they are required to present an additional identity document, noting the concerns raised by many stakeholders including those in favour of the proposal. Therefore, the Review Panel is not proposing specific mandatory identification requirements when accessing health services, such as the presentation of photographic identification (though this would be good practice where it is available). Rather, the Review Panel is recommending that health professionals should be required to take reasonable steps to confirm a patient's identity.

Recommendation 3: It is recommended that as a condition of claiming Medicare benefits on behalf of patients, health professionals should be required to take reasonable steps to confirm the identity of patients when they are first treated.

A requirement that health professionals take 'reasonable steps' would allow health professionals to exercise their discretion about what steps would be appropriate for particular patients, including those who do not hold any form of photographic identification. The Review Panel recognises that some stakeholders may seek definitive guidance on what would constitute acceptable evidence of identity:

> *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.* – Consumers Health Forum of Australia

However, the Review Panel considers that health professionals, supported by their professional bodies, will be best placed to develop guidelines about what would constitute 'reasonable steps' in their particular healthcare settings and for particular cohorts of patients.

It may be appropriate for different standards to apply for emergency or urgent treatment as opposed to non-urgent or ongoing care. When care is planned in advance (for example, when patients are seeking secondary care from a specialist or undergoing a procedure in hospital), the Review Panel considers it would be reasonable to expect that a patient would provide photographic identification in addition to a Medicare card or number in most cases.

This requirement would only apply where the health professional is lodging a claim on behalf of a patient. If a patient who is eligible for Medicare was unable to confirm their identity to the satisfaction of the health professional, they would still be able to claim their Medicare benefit through other claiming channels, including the Express Plus Medicare app, Medicare online accounts (for selected item numbers), by mail or by lodging the claim at a Department of Human Services service centre.

It is important to note that this requirement would not affect patients who wish to access health services anonymously or using a pseudonym. The recommendation only applies to health professionals who are claiming a Medicare benefit on behalf of a patient, which would not be possible under current arrangements if a patient is using a name that does not match their Medicare card.

3.2 Access channels overview

There are a number of channels that health professionals can use to find a patient's Medicare card number when they are unable to present their card, including HPOS (directly or through practice software) or the Department of Human Services' Medicare telephone lines. The Department of Human Services also has online claiming channels that allow health professionals to confirm Medicare card details, but it is not possible to search for a Medicare number through these channels.

3.2.1 Health Professional Online Services

The ‘Find a Patient’ functionality within HPOS allows health professionals to search for or confirm a patient’s Medicare card number and concessional eligibility. To search for a Medicare card number, 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, IRN, first name and card expiry date. HPOS Find a Patient also allows health professionals to upload a batch request for multiple details. Each file can contain up to 500 requests with a response provided within 24 hours to the secure HPOS mail centre.

Providers may delegate their HPOS access; for example, to administrative staff.

In 2016-17, approximately 10.2 million Medicare card number searches and confirmations were undertaken via HPOS Find a Patient. This includes successful and unsuccessful searches.

Further information on HPOS can be found in section 5.

3.2.2 Practice software

The Department of Human Services also offers integration for approved third party software products to facilitate claiming, billing and reporting, as well as information exchange with health professionals.

Software developers can choose to embed a link to HPOS within their software. Alternatively, software developers can utilise the Department of Human Services Business to Business (B2B) Patient Verification Services. If the product has a link to HPOS embedded in its product, the user is still required to access HPOS using an authentication mechanism, either a PKI certificate or PRODA account (discussed further in section 5). B2B accesses the same patient search service offered through HPOS directly from the third party software. While B2B removes the requirement to login via HPOS, it still requires a PKI certificate (individual or site) to access. The B2B functionality is currently not available with PRODA authentication.

3.2.3 Telephone channels

Health professionals can obtain Medicare card numbers by calling the Department of Human Services’ Medicare provider enquiries line or the PBS general enquiries line.

To obtain a Medicare card number through the Medicare provider enquiries line, the caller must pass a security check and provide sufficient patient information to identify the patient with their first name, surname, date of birth and address. Up to seven Medicare card numbers can be requested per phone call.

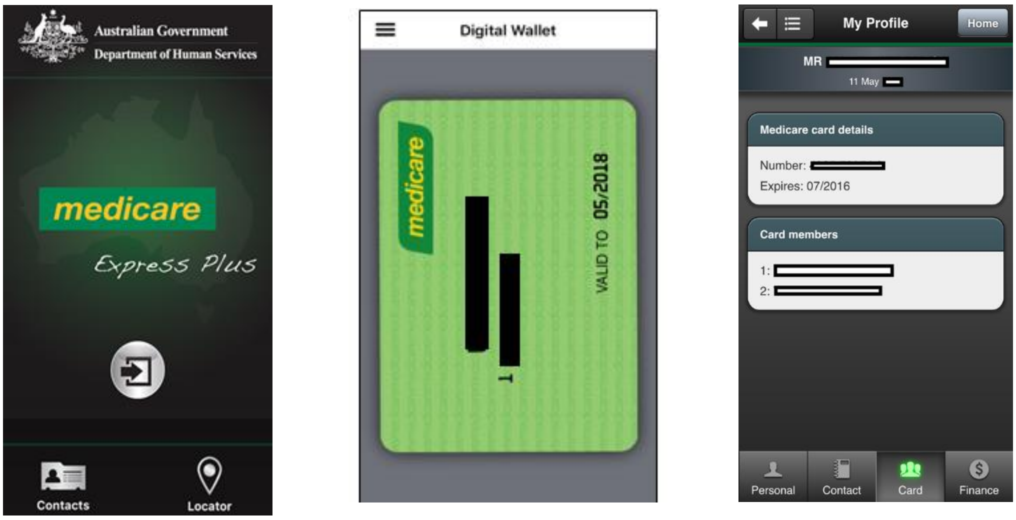
To obtain a Medicare number through the PBS general enquiries line, the caller is asked to provide their name and to identify the pharmacy or public hospital from which they are calling. They must then provide sufficient patient information to identify the patient. Up to five Medicare card numbers can be requested per call.

In 2016-17, over 500,000 calls were received through the Medicare provider enquiry line, and over 400,000 were received through the PBS general enquiries line (the majority of calls to the PBS line are to confirm an individual's concessional eligibility and do not relate to Medicare card enquiries).

Further information on the telephone channels can be found in section 6.

3.2.4 Individual access

Individuals can access their own Medicare card details if they do not have their card with them. They can attend a Department of Human Services 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. Alternatively, individuals who have downloaded the Express Plus Medicare mobile app can view an image of their Medicare card in the 'Digital Wallet' section.



[redacted]

MR [redacted]

11 May [redacted]

Medicare card details

Number: [redacted]

Expires: 07/2016

Card members

1: [redacted]

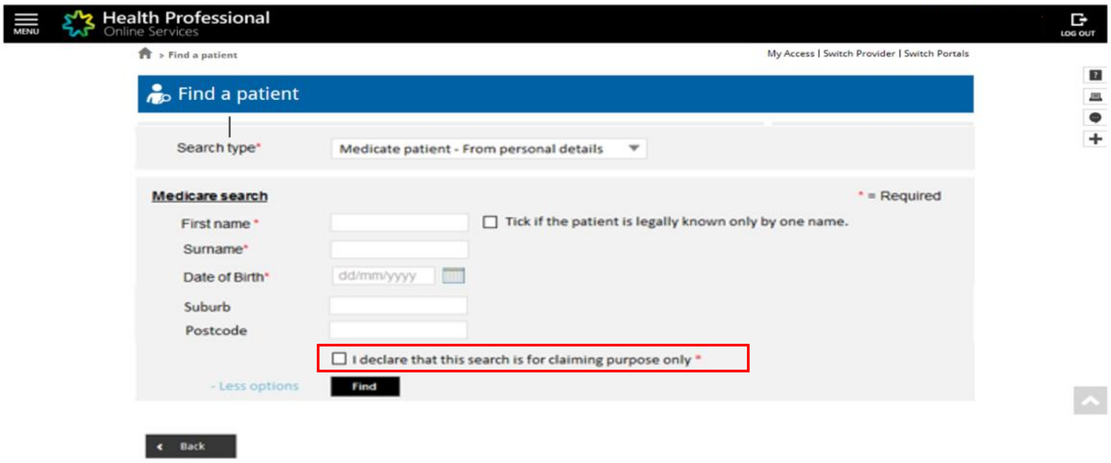
2: [redacted]

Figure 2: Express Plus Medicare app home screen, digital wallet and profile

3.3 Patient control and notification

Under current arrangements, health professionals do not have to explicitly 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. Callers to the PBS general enquiries line are asked if they have the patient's permission to obtain and store the Medicare card number.

When using Find a Patient, the health professional performing the search must first tick a box declaring 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 benefit).



Find a patient

Search type* Medicate patient - From personal details

Medicare search

* = Required

First name *

□ Tick if the patient is legally known only by one name.

Surname*

Date of Birth* dd/mm/yyyy

Suburb

Postcode

□ I declare that this search is for claiming purpose only *

Figure 3: HPOS Find a Patient screen

Although there are audit logs of access to Medicare card numbers through HPOS, these are not currently available to individuals. There is no audit log recording which health professionals have requested Medicare card numbers through the telephone channels.

Individuals are not notified when a search is conducted for their Medicare card details. However, they can review their claiming history (available through Medicare online accounts[18]) 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, either online or by telephone, to the Department of Human Services or the Department of Health for further investigation.

Review Panel Recommendation: Patient consent

As noted above, there is currently no requirement for health professionals to explicitly obtain consent before seeking their patients' Medicare card numbers through HPOS Find a Patient or the provider enquiries' line. This is inconsistent with the PBS general enquiries line, which requires callers to confirm that they have obtained the patient's consent to request and store their Medicare card details.

A number of submissions proposed that there should be a requirement to obtain consent:

> *Consent should be a requirement for a health service provider to access an individual's Medicare card details in non-urgent or long-term treatment care.* – Australian Healthcare and Hospitals Association

[18] 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. Further information is at https://www.humanservices.gov.au/customer/services/medicare/medicare-online-accounts.

> *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.* – Consumers Health Forum of Australia

Review Panel Finding: Requiring health professionals to obtain consent before seeking their patients' Medicare card numbers from the Department of Human Services will provide patients with more control over their Medicare information and ensure that they know when that information is given to others.

A case could be made that there is already an implied consent from the patient. Searches for Medicare numbers through HPOS Find a Patient and the provider enquiries line are intended to be for claiming purposes only, and in most cases the patient will be aware that a health professional is lodging a claim on their behalf.

The Review Panel is unconvinced that this is sufficient. It believes that it would be more appropriate for health professionals to obtain explicit consent from the patient, either orally or in writing. In addition to providing patients with more control, this would also increase consumer awareness about how their Medicare information is used and shared, and how health professionals interact with the Department of Human Services on their behalf.

Recommendation 4: It is recommended that health professionals should be required to seek the consent of their patients before accessing their Medicare numbers through HPOS or by telephone.

The Review Panel does not expect that the requirement to obtain consent would create an excessive burden for healthcare organisations. It should be straightforward to incorporate a request for consent into existing patient registration procedures, with a clear statement that the consent applies to future requests for Medicare card details relating to the patient's treatment at the practice. Submissions to the Review emphasised the importance of a streamlined process:

> *The manner in which consent is obtained should be with as little administrative burden as possible while balancing the need for integrity of the health system and of Medicare cards. For example, upon being admitted to a public hospital consent could be obtained when the individual presents to the hospital and remains in force throughout the individual's treatment.* – Australian Healthcare and Hospitals Association

> *The form of this consent should be meaningful, but 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 commonplace for practices to take a record of a patient's Medicare number and could refer to that in order to access it. –* Consumers Health Forum of Australia

As part of the consent process, health professionals would need to ensure that consumers are adequately informed about how their Medicare card number will be handled. The Review Panel believes that this could be incorporated into existing processes to inform patients about the handling of their personal information.

Where consent is not provided, this should not be a barrier to accessing a health service; however, the patient should be informed that the health professional will not be able to lodge the Medicare claim on their behalf unless they provide their current Medicare card.

To reflect the requirement for consent, the Department of Human Services would need to update its processes for the provider enquiry line to include a question about whether the caller has obtained the patient's consent. The declaration to which health professionals must agree before conducting a search using HPOS Find a Patient would also need to be updated to reflect that the search is for claiming purposes only and that the health professional has obtained the patient's consent for the search.

Review Panel Recommendation: Patient access to audit logs

As outlined above, there are audit logs of access to Medicare card numbers through HPOS, but these are not available to individuals.

Individuals are currently able to access their Medicare claiming history for the past three years through their Medicare online account (accessed through myGov) or the Express Plus Medicare app, and can request details of older claims from the Department of Human Services by completing a form. This allows individuals to see which health professionals have lodged claims on their behalf, which may assist in identifying any discrepancies (such as a claim for a service that they did not receive). Individuals are encouraged to report any concerns, as this is a valuable source of information when identifying fraudulent activity.

Individuals can also access details of who has looked up their Individual Healthcare Identifier, through their Medicare online account, by calling the Healthcare Identifiers Service or by asking at a Department of Human Services service centre.[19]

However, there is no equivalent access to information about which health professionals or organisations have searched for a patient's Medicare card details. Submissions, including those from the AHHA, the Australian College of Nursing and Queensland Health, called for patients to have access to these audit logs. The Western Australian Department of Health (WA Health) linked access to audit logs to individuals taking an active role in protecting their Medicare information:

> *Government should encourage individuals to take a more active role in safeguarding their Medicare information, but also in monitoring its usage. As such, it would be preferable if individuals could have access to the HPOS log for their Medicare number.* – Western Australian Department of Health

The OAIC made similar comments:

> *Making this information available to individuals will increase their control over the use of their Medicare card number and may increase the chance of fraudulent activity being identified by the individual. This arrangement may go beyond the identification of Medicare fraud to identity theft generally.* – Office of the Australian Information Commissioner

[19] Further information is available at https://www.humanservices.gov.au/individuals/services/medicare/healthcare-identifiers.

The Review Panel does not believe that there would be significant demand for this information, but it also considers that individuals should be informed that they are able to access it if they wish; for example, if they are concerned that their Medicare number may have been retrieved for an illegitimate purpose.

Review Panel Finding: Access to audit logs for searches for Medicare card numbers through HPOS will support patients who wish to play an active role in monitoring access to their Medicare details.

The Review Panel is concerned that there are no audit logs of access to Medicare card numbers through the telephone channels. While the ideal would be that access through the telephone channels was also recorded and made available to individuals on request, the Review Panel understands that introducing this functionality within Medicare's computer systems would incur significant costs. The Review Panel considers that the risk of illegitimate access to Medicare card numbers through the telephone channel would be reduced by in implementation of recommendations 13 and 14 below, which are aimed at increasing the security of the telephone channel and reducing the number of telephone requests. The Department of Human Services should continue to monitor the risk associated with the absence of audit logs on its telephone channels and implement appropriate mitigation strategies if required.

Recommendation 5: It is recommended that individuals should be able to request the audit log of health professionals who have sought access to their Medicare card number through the HPOS 'Find a Patient' service.

The Review Panel understands that the Department of Human Services has existing processes in place for the release of the personal information that it holds through administrative access arrangements.[20] The Review Panel considers that any requests for access to HPOS audit logs could be accommodated under these arrangements, as the demand is unlikely to be sufficient to justify making these audit logs available to view through Medicare online accounts or the My Health Record, as suggested in some submissions.

Review Panel Recommendation: Taking privacy into account

The Review Panel recognises the privacy concerns held by some stakeholders in relation to the release of Medicare card numbers to health professionals. The Review Panel has noted the comments from the OAIC:

> *I would recommend that the Department conducts a Privacy Impact Assessment (PIA) to assist it in the implementation of Review recommendations. A PIA is an assessment tool that describes the personal information flows in a project and analyses the possible privacy impacts that those information flows, and the project as a whole, may have on the privacy of individuals. In this situation, a PIA would highlight any privacy impacts associated with implementing the Review recommendations and identify proactive measures required to mitigate those impacts, including security considerations.* – Office of the Australian Information Commissioner

[20] Further information is at https://www.humanservices.gov.au/organisations/about-us/access-information.

Recommendation 6: It is recommended that the Department of Human Services undertake a Privacy Impact Assessment when implementing the Review recommendations, identifying the impact of changes on the privacy of individuals.

The Review Panel accepts the Information Commissioner’s proposal. It notes that the Department of Human Services’ existing Project Management Framework and Standards already recognise the importance of incorporating privacy into project planning and delivery. Any project that involves managing personal information including the collection, storage, use, disclosure or alteration of personal or protected information requires a Privacy Threshold Assessment to be undertaken. The Privacy Threshold Assessment is used to determine whether further privacy assessment is required. This could involve a full PIA, or a Privacy Assurance Advice about a specific element of a project.

4 Security and compliance

4.1 Compliance controls

Legislation is in place which outlines controls over access, security, usage and transmission of Medicare information, including via HPOS. Health professionals can access the HPOS channel after being authenticated via either the PRODA or PKI mechanisms, which are discussed in detail in section 5.3.

The HPOS Terms and Conditions indicate that they ‘apply to all access and use of the HPOS’, regardless of which authentication mechanism a practice or health professional uses to access HPOS. In these Terms and Conditions, a person or representative of an organisation confirms they will ‘not make a record of, divulge or communicate protected information (as defined in section 130 of the *Health Insurance Act 1973* (Cth)) other than in the course of your duties as a healthcare provider’. Further, they confirm that failure to do so may be an offence under the *Health Insurance Act 1973*. Similar requirements are stated for the *National Health Act 1953* (section 135A). These two Acts combined manage all programmes under which a health service organisation or provider can make claims on the MBS or PBS.

Section 130 of the *Health Insurance Act 1973* (which legislates the Medicare programme) states 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 PBS) has similar provisions.

Breaching these requirements is therefore an offence under law, which supports control and compliance initiatives across the channels. The aim of compliance activity is to promote the sustainability of Australia’s health system by protecting the integrity of health programmes through prevention, identification and treatment of misuse, fraud and inappropriate practice by health professionals, the public and suppliers.

Compliance staff in the Department of Health and the Department of Human Services monitor claiming channel activity to detect possible non-compliant claiming.

The Health Provider Compliance Model at Figure 4 highlights that the vast majority of health professionals try to do the right thing. For those trying to get things right, the aim is to make it easy to claim properly and support health professionals through information and education.

Moving up the pyramid, different action is taken to detect incorrect or inappropriate claiming and respond proportionately – from targeted feedback letters for broader compliance issues, to audits and Professional Review for individuals where specific issues of larger value are detected.

Fraud control processes are deliberately focused on the most serious cases of non-compliance, rather than on people making honest mistakes. It should also be noted that non-compliance can be as a result of incorrect billing by providers, but equally may result from poor administrative practices or deliberate action by administrative staff in medical practices to lodge incorrect claims.

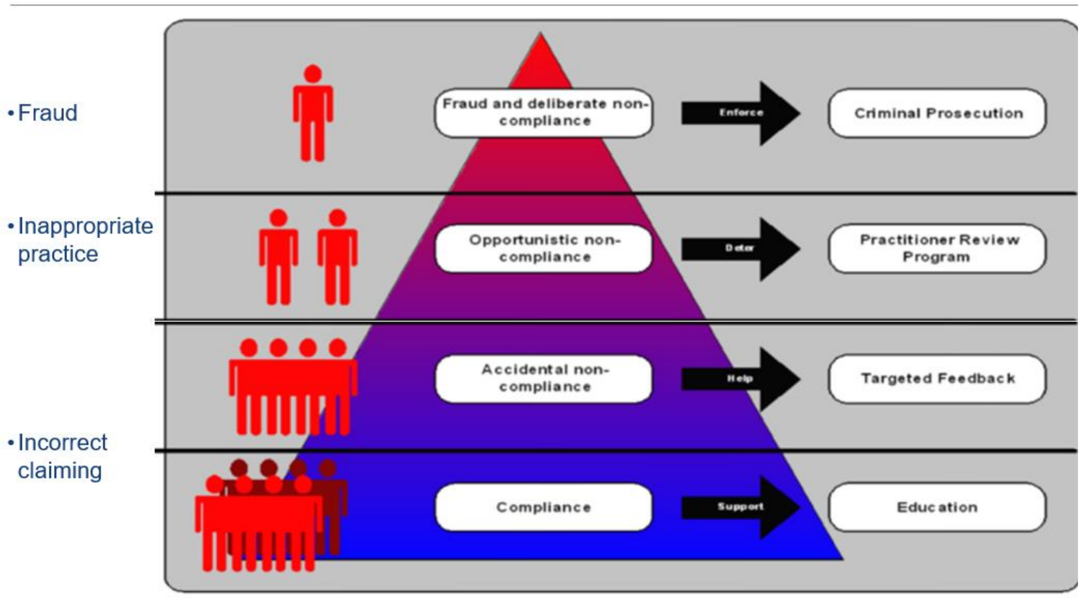


Figure 4: Health Provider Compliance Model

4.2 Security of Medicare data

The Department of Human Services holds a large volume of Medicare information and other personal data. It has implemented sophisticated cyber security and internal fraud control protections in order to ensure the security of this information.

4.2.1 Cyber security

The Department of Human Services is the custodian of significant data holdings relating to all Australians, including information that can be used to identify, contact or locate an individual. It has risk controls in place that recognise the increasing threat of cyber attacks. It works with national and international agencies to ensure that its cyber security protections are in line with global best practice.

The Department of Human Services' cyber security activities include:

- Monitoring and assessment of cyber activity including vulnerabilities, threats and incidents that could damage its business operations
- Conducting penetration testing and security code review to detect vulnerabilities in its online systems to prevent security breaches and the leaking of sensitive data
- Working collaboratively with the broad cyber security community, nationally and internationally, to share information, ensure best practice and enhance cyber security strategies
- Triaging incidents, managing real-life events and preventing malicious content with a range of tools
- Development, implementation and monitoring of cyber security policies, standards and frameworks that list applicable Information Security Manual, Protective Security Policy Framework, and Department of Human Services controls to safeguard its data.

The Australian National Audit Office (ANAO) has scrutinised the Department of Human Services' cyber protections, including its implementation of the mandatory strategies in the *Australian*

Government Information Security Manual (Top Four mitigation strategies). In its 2016-17 *Cybersecurity Follow-up Audit* (ANAO Report No. 42 2016-17), the ANAO found that the Department of Human Services was 'cyber resilient'.[21] The report noted that:

> *The Department of Human Services had security controls in place to provide protection from external attacks, internal breaches and unauthorised information disclosures. This was achieved by prioritising activities that were required to implement the Top Four mitigation strategies and by strengthening supporting governance arrangements. It is now positioned in the* 'cyber resilient' *zone.*[22]

4.2.2 Internal fraud controls

Staff play an essential role in the security of the information held in government systems, as many of them have access to extensive personal information in their day to day work. All Department of Human Services staff are encouraged to undertake annual Fraud Awareness training, which outlines both the risks involved and what staff can do to ensure security of systems and information. This training also outlines the responsibilities of staff to access only that information required to undertake their role and not for any personal reasons. This training outlines the possible ramifications of unauthorised access, up to and including termination of employment.

The Department of Human Services also proactively monitors systems and uses intelligence gathering techniques to monitor internal fraud and unauthorised access (including access to a staff member's own record or records of family members). The Department of Human Services Fraud Control Plan includes fraud prevention controls, with a team in place to undertake assessments, reviews and investigations into any allegations made into fraudulent activity by staff.

[21] Cyber resilience is the ability to continue providing services while deterring and responding to cyber attacks. Cyber resilience also reduces the likelihood of successful cyber attacks.

[22] The full report is available online at https://www.anao.gov.au/work/performance-audit/cybersecurity-follow-audit. This audit was a follow-up to Audit Report No. 50 2013-14, *Cyber Attacks: Securing Agencies' ICT Systems* (available at https://www.anao.gov.au/work/performance-audit/cyber-attacks-securing-agencies-ict-systems).

5 Health Professional Online Services

5.1 HPOS Overview

HPOS was implemented by the Department of Human Services in 2009 with the aim of enhancing and improving the delivery of services to health professionals through a single entry point. HPOS offers health professionals a single secure web portal which provides real-time access to a number of online services.

HPOS is one of four digital channels or services that health professionals use to interact with the Department of Human Services, along with Medicare Online, Easyclaim and the Electronic Claim Lodgement and Information Processing Service Environment (ECLIPSE). Most of these channels are accessed through medical practice software, but HPOS allows direct access to online claiming in addition to other functions such as Find a Patient and secure mail.

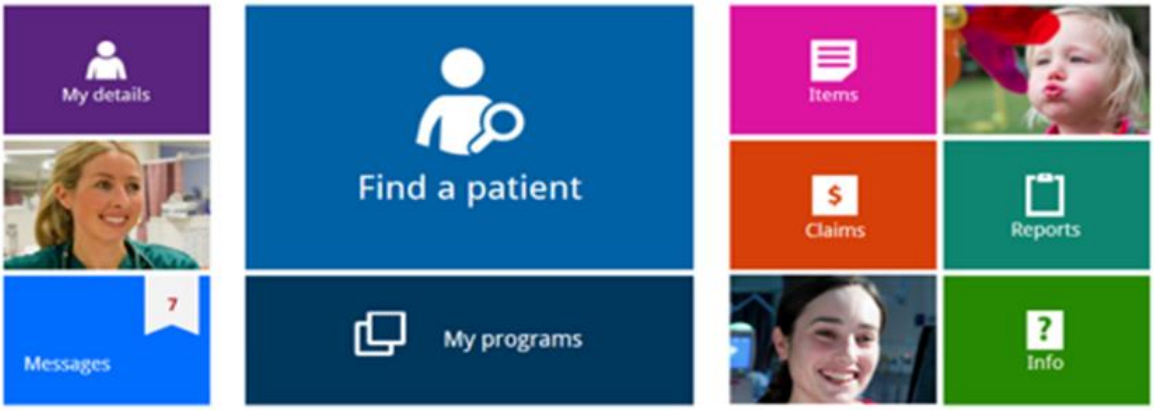


Figure 5: HPOS home screen for user with 'Find a Patient' access

Health professionals who use HPOS include general practitioners, specialists, allied health professionals, optometrists, dentists and nurse practitioners. The largest user base is allied health professionals, particularly optometrists, psychologists and dentists. HPOS is used more frequently by administrative staff than the actual providers, as these staff are more likely to undertake the work of maintaining patient details, claiming and reconciliation of claims.

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, outlined further below) before they can be nominated as a delegate. Delegate arrangements provide delegates with access to a larger range of services and tasks that would not otherwise be available to them (see Appendix E for more information). Health professionals are able to view a list of their delegates within HPOS and delete any who are no longer required.

Review Panel Recommendation: Delegate arrangements

As outlined above, HPOS has functionality which allows providers to nominate administrative staff to act as a delegate on their behalf. While delegates must also have their own authentication credential, either a PKI certificate or PRODA account, the Review Panel considers there are still existing risks inherent with the delegation model. Most importantly, delegate arrangements do not currently expire. If a health professional does not remove a delegation when it is no longer required, it will remain in place, which means that the delegate could continue to perform functions in HPOS even if they have left the practice.

Review Panel Finding: The risk of delegate arrangements remaining in place when they are no longer required could be reduced by introducing an expiry period for delegations after which they must be renewed, and providing additional prompts to health professionals encouraging them to review their delegates and remove any who are no longer required.

Submissions commenting on this recommendation were largely supportive.

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

> *The time period is dependent on the 'level of risk tolerance for potential opportunity for fraud'. A twelve month period of inactivity would seem appropriate*. – Queensland Health

In some cases, support was contingent on sufficient notification and ease of renewal.

> *Extensive consultation will be needed with healthcare providers to establish a reasonable timeframe before an account expires and a suitable process for notification of expiry dates.* – Royal Australian College of General Practitioners

The Review Panel recognises that some health professionals may want to put delegations in place for a shorter time period, so has recommended 12 months as a maximum period for delegate arrangements.

Should this recommendation be accepted, the revised renewal process for delegate arrangements should be made straightforward for health professionals and incorporate a reasonable notification period.

Recommendation 7: It is recommended that delegations within HPOS should require renewal every 12 months, with a warning to providers, health professionals and their delegates three months before the delegation expires.

One submission suggested that, instead of introducing time limits on delegate arrangements, the Department of Human Services could periodically provide a list of delegates to health professionals for them to review. The Review Panel noted that health professionals are already able to view and manage a list of their delegates within HPOS.

5.2 HPOS Find a Patient

In HPOS, the Find a Patient function allows a health professional to search and immediately confirm a patient's Medicare card number and concessional eligibility. This information assists health professionals to correctly claim for Medicare services provided to their patients. A health professional can use the Find a Patient service to:

- Confirm patient details
  - The Confirm function uses a patient's existing Medicare card number details to verify eligibility before a claim is submitted. A successful search result will confirm the correct Medicare card number, IRN and first name for the patient.
- Search for patient details
  - When a patient's Medicare card number is not available, health professionals can use the search function. This requires entry of the patient's first name, surname and date of birth. If more than one person matches the information entered, the patient's postcode or locality/suburb can be used to further refine the results. A successful search will return the correct Medicare card number, IRN, first name (as it appears on the card) and card expiry date. Results will only display if a unique match is found.
- Submit a request to search for Medicare card numbers or confirm Medicare eligibility for multiple patients
  - HPOS Find a Patient allows users to upload a batch request for multiple details using either the search or confirm functionality. Each file can contain up to 500 requests. A response will be returned securely through HPOS within 24 hours. There is a limit of one batch request per individual or site per day.
- Confirm concessional eligibility
  - A health professional can also confirm a patient's concessional eligibility for Medicare services using Find a Patient. The check will return the full name of the patient, the date of the service that has been entered, the concessional entitlement result at that date and the verification receipt number.

The Find a Patient functionality was added to HPOS to improve health professionals' access to necessary information, and to assist them to transition to online services instead of telephone channels when interacting with the Department of Human Services.

Review Panel Recommendation: Batch requests

There was considerable discussion about the HPOS functionality that allows users to request large volumes of patient Medicare numbers via 'batch requests' of up to 500 Medicare numbers at a time.

Views from the Review Panel's discussions with different stakeholder groups were mixed, with many indicating that being able to request 500 Medicare numbers at one time posed a risk.

> *The ability to make 500 requests at a time appears excessive, particularly where the request comes from a GP or a small practice, compared with a hospital. Agree that batch requests should be subjected to a higher level of scrutiny.* – Queensland Health

However, in discussions with other state and territory health departments, the view was expressed that the batch facility was crucial to the efficient running of larger operational areas such as hospitals.

> *…in general any system that results in the inability to submit bulk requests is likely to have a substantial impact on the current workload of hospitals.* – Victorian Department of Health and Human Services

Review Panel Finding: While batch 'Find a Patient' requests should be retained, the current limit of 500 records per batch is unwarranted in most cases.

The Review Panel recognises that the facility to search for multiple Medicare card numbers may be required in hospital settings to speed up admissions or in primary healthcare centres hosting visiting specialist services:

> *As many patients access multi-specialty care and the NT primary health care centres provide or host specialist services (especially in remote communities), batch requests are required to streamline processes.* – Northern Territory Department of Health

> *The batch Find a Patient functionality should be maintained in some form for timeliness and administrative purposes however WA Health acknowledges the security benefit of limiting access to this function.* – Western Australian Department of Health

> *The proposed "Batch number limit" should consider the type and size of requesting organisation. There could be a different limit set based on the type of organisation, which should be configured as part of the initial establishment.* – New South Wales Health

One jurisdiction argued for the larger batch limits to remain:

> *The NT does not support imposing further conditions for batch Find a Patient requests. Operations staff already reports on the perceived inefficiency of current limits on requests.* – Northern Territory Department of Health

In discussions with the Review Secretariat, the Northern Territory Department of Health clarified that their concern lay more with the limit of one batch request per day, rather than the number of patients that could be included in each request. The Review Panel sees the large batch requests as posing a potential security risk. It acknowledges that there may be a few instances where larger volumes of requests are required, so has recommended that there should be access to higher limits, but only in exceptional circumstances where a clear rationale has been provided.

Recommendation 8: It is recommended that batch requests for Medicare card numbers through HPOS should be more tightly controlled (50 card numbers per batch request, and only one batch request per day), unless healthcare providers apply in writing to the Chief Executive Medicare, demonstrating a clear business need for a higher limit.

5.3 Registration and authentication for HPOS

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

In order to be registered as a provider for Medicare purposes, the majority of providers must provide evidence of their Australian Health Practitioner Regulation Authority (AHPRA) registration. AHPRA registration requirements include a full criminal history, business registration including professional indemnity insurance arrangements, and recency of practice.

A small number of providers (such as Aboriginal Health Workers and Diabetes Educators) must instead provide evidence of their certification in line with the registration standards of their health profession. Provider registration is confirmed by the Department of Human Services on an annual basis, and registration status is updated daily with information received from AHPRA.

To access HPOS, health professionals must further authenticate their credentials by either applying for an individual PKI certificate or creating a PRODA account. The authentication process includes providing evidence of identity and validation of a provider number. A health service organisation can apply for a PKI site 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 their own individual PKI certificate or create their own PRODA account. These staff must also provide evidence of identity.

Access to HPOS is via:

- For PRODA users – entry of user name, password and second factor authentication code
- For PKI individual certificate users – software installed on computer, installation of PKI certificate and, after the certificate is identified, entry of their Personal Identification Code (PIC)
- For PKI site certificate users – log on to a computer with the correct software and site certificate installed and entry of PIC.

There are four different individual user roles within HPOS that provide different levels of access within the system. These are outlined at Appendix D.

There were approximately 163,000 accounts with the ability to access HPOS at 30 June 2017. This includes approximately 114,000 PKI certificates (approximately 65 per cent of which are individual certificates and 35 per cent are site certificates), and approximately 49,000 active PRODA accounts which have been linked to HPOS. Some health professionals may have both PKI certificates and PRODA accounts. The majority of the 163,000 accounts would have access to the Find a Patient function.

5.3.1 PKI Certificates

PKI is a combination of policies, practices and technologies that enables health professionals and health service organisations to authenticate their identity and securely and privately exchange information with the Department of Human Services. The Department of Human Services complies with the Commonwealth Government's Gatekeeper Public Key Infrastructure Framework[23] in delivering its online authentication services. An annual audit is carried out to ensure the Department of Human Services complies with the Framework.

Providers or administrative staff can apply for a PKI certificate by submitting a PKI individual certificate application form.[24] Health service organisations can apply for a PKI certificate by

[23] Available at https://www.dta.gov.au/standard/design-guides/authentication-frameworks/gatekeeper-public-key-infrastructure-framework/

[24] Available at https://www.humanservices.gov.au/health-professionals/forms/hw002

submitting a PKI site certificate application form.[25] The PKI application form requires applicants to provide documentation to prove their identity and relationship with the Department of Human Services.

PKI site certificates provide more limited access to HPOS functions than individual certificates, but the available functions include Find a Patient.

Following an application, a PKI certificate (a USB, smart card or pre-cut card for individual certificates, or a CD-ROM for site certificates) is created and mailed to the applicant. The PKI certificate is mailed separately from the 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 log on to a computer with the correct software and site certificate and enter the correct PIC. Site certificates can be installed with practice management software or the organisation's internet browser.

PKI certificates issued by the Department of Human Services expire after two or five years, depending on the policy under which the certificate was issued. Some practice management software automatically renews PKI certificates before they expire. However, a PKI certificate can only be automatically renewed once through practice management software.

5.3.2 PRODA

PRODA is an online authentication system that can be used to securely access certain government online services, including HPOS.

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 government issued identity documents. Identity documents are verified online in real time using the DVS. 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[26] 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 to the nominated preferred method (either SMS, email or generated on the PRODA mobile app).

The Department of Human Services is in the process of transitioning users of PKI individual certificates to PRODA. At this stage PRODA does not provide an alternative to site certificates.

[25] Available at https://www.humanservices.gov.au/health-professionals/forms/hw001

[26] Available at https://www.humanservices.gov.au/health-professionals/forms/hw080

Review Panel Recommendation: PKI and PRODA

The Review Discussion Paper put forward a proposal that the transition of users from PKI individual certificates to PRODA should be accelerated. This recognised that there are greater risks inherent in the use of PKI certificates. Although the Terms and Conditions require that certificates are kept securely and not shared, in practice there is a risk that certificates will be shared within an organisation, for example if a staff member who requires access has not yet received their certificate. There is also a risk that site certificates will be provided to third party IT service providers or practice software developers. This means that the Department of Human Services may not be aware of who is accessing HPOS using the certificate.

Review Panel Finding: PRODA provides a greater level of security than PKI certificates, due to the requirement that each individual has their own PRODA account and the strength of the two step verification process for authentication purposes. The Review Panel considers that the Department of Human Services should accelerate its current move away from PKI certificates to PRODA.

The Review Panel noted that a majority of submissions that addressed this proposal were in favour of the transition from PKI to PRODA:

> *AHHA supports the transition from an individual or site level PKI certificate to a PRODA account… AHHA supports all new HPOS users only being able to apply for a PRODA account. An expedited transition period for all PKI certificate holders to transition to PRODA would be ideal.* – Australian Healthcare and Hospitals Association

> *The RACGP supports any initiative that strengthens the security of the HPOS system, providing this is balanced with reasonable administrator access to patient Medicare information. The RACGP supports the move from PKI certificates to PRODA accounts to enhance the security of HPOS verification.* – Royal Australian College of General Practitioners

> *The NT supports moving to PRODA as it would provide an extra level of security with a three part authentication making user access more difficult to share. We also believe that a three year timeframe is reasonable.* – Northern Territory Department of Health

Recommendation 9: It is recommended that authentication for HPOS should be moved from PKI to the more secure PRODA expeditiously, with transition completed within three years.

The Review Panel notes that some support for the transition was conditional on an appropriate PRODA alternative to site certificates and on system functionality and capacity issues associated with PRODA being addressed prior to implementation. For example:

> *RDAA in principle supports transitioning providers to the PRODA system, however this should not occur until the system capability and capacity issues have been addressed.* – Rural Doctors Association of Australia (RDAA)

> *The AMA supports the move to PRODA as soon as possible. To encourage this, the Government needs to ensure that PRODA meets the needs of practices by enhancing the functionality of PRODA to enable secure messaging, business transactions and data exchange between providers and Medicare Australia and other authorised parties approved by Medicare Australia.* – Australian Medical Association

The Review Panel recognises that PRODA does not currently provide the same functionality as PKI certificates, and notes that the Department of Human Services will need to investigate and address these issues in order to ensure service delivery is uninterrupted.

> *Any plan to require a full-scale change from site based PKI to individual PRODA accounts will need a well-documented development pathway to ensure that other integrations with existing software systems are not compromised… a detailed industry consultation would be required to ascertain what was practicable.* – Medical Software Industry Association

The Review Panel takes the view that a three year timeframe is sufficient. If Government accepts this recommendation, the Department of Human Services will need to work with health professionals and the medical software industry (including their peak bodies) to ensure that their advice is taken into account during the transition.

Review Panel Recommendations: Suspending inactive accounts

The Review Panel observed that PRODA accounts do not expire, even when they are no longer active. PKI certificates issued by the Department of Human Services expire after two or five years (depending on the policy under which they were issued), but some practice management software automatically renews PKI certificates before they expire. This means that there is a risk that users will continue to have access to HPOS after it is no longer required.

Review Panel Finding: Suspending or cancelling PRODA accounts if they have not been used for a certain period would reduce the risk that these accounts could be used inappropriately.

Several submissions supported the recommendation:

> *Active, deactivated and expired accounts/certificates should be audited, reviewed and monitored. They should be deactivated if not used within a specified period of time. A 6 month period of inactivity would seem appropriate* – Queensland Health

> *PRODA accounts should expire, especially after a pre-determined period of inactivity. … While the review panel notes it is important to avoid creating administrative burdens for health professionals who have a legitimate need to access HPOS, the review panel should note that health service providers currently comply with stringent security arrangements for their financial arrangements and transactions with banks. Security requirements to access Medicare card and patient information should be just as stringent.* – Australian Healthcare and Hospitals Association

The Review Panel notes that the PKI and PRODA authentication models are not exclusively used for access to HPOS; other uses include the National Disability Insurance Scheme. If the Department of Human Services were to suspend or revoke a PKI certificate or PRODA account, it could have a detrimental impact on these other uses. For this reason, the Review Panel has recommended that inactive HPOS accounts should be suspended, rather than the authentication credential that provides access to HPOS.

Some submissions emphasised the importance of adequate warning and a straightforward reactivation process:

> *If suspensions are implemented the AMA would strongly encourage the Department to ensure that holders are appropriately notified and given the opportunity to confirm their PRODA account or PKI is still required. Any suspension should be easily reversed.* – Australian Medical Association

The Review Panel accepts this advice. It proposes that a warning should be provided after three months of inactivity. Should this recommendation be accepted, the Department of Human Services will need to work with industry to ensure that the reactivation process is streamlined and does not create an undue burden for health professionals.

Recommendation 10: It is recommended that HPOS accounts that have been inactive for a period of six months should be suspended, following a warning to users after three months of inactivity.

Recommendation 11: It is recommended that the process of opening and reactivating a HPOS account should be administratively straightforward.

5.4 Terms and Conditions

HPOS users must comply with Terms and Conditions. There are separate Terms and Conditions for HPOS itself and for each of the authentication mechanisms, PKI and PRODA.

5.4.1 HPOS Terms and Conditions

The HPOS 'Terms and Conditions of Use and Access' apply to the access and use of HPOS and are displayed on every logon to HPOS.[27]

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 confidential personal information about other persons that they upload to the system, or access from the system
- 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, which are outlined below.

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

5.4.2 PKI Terms and Conditions

Terms and Conditions of Use apply for both PKI individual and site certificates.[28] These Terms and Conditions include that the certificate holder agrees to:

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

5.4.3 PRODA Terms and Conditions

The PRODA Terms and Conditions must be accepted before creating a PRODA account and then again the first time the user logs onto the PRODA account.[29]

These include that the user agrees to:

- Keep confidential and secure at all times 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
- 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 of Human Services
- Not permit any other person to use their Secure Access Details
- Ensure they have appropriate business and security controls in place to ensure all claims, forms and other documentation submitted to the Department of Human Services are appropriately authorised
- Be responsible for all access to, and use of, the PRODA code generator undertaken on their device with the user identification and password.

Review Panel Recommendation: Terms and Conditions

The Review Panel discussed at length the issue of the Terms and Conditions under which people use HPOS, either through PKI or PRODA. During the course of the Review, the Review Panel considered each of these mechanisms and how they are used in various healthcare settings, from medical practices to hospitals to central primary healthcare centres such as in the Northern Territory.

Usage of these mechanisms differs significantly across these settings, based on the very different patient flow and staff roles.

[28] Both sets of Terms and Conditions are available at https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents.

[29] Available at https://proda.humanservices.gov.au/pia/pages/public/registration/account/createAccount.jsf

Also different are the nature and frequency of reminders provided to users the conditions under which these mechanisms are used. In the case of PKI certificates, the Terms and Conditions are provided on the initial application form, and not repeated. For PRODA, Terms and Conditions are displayed the first time a user logs in and when there are any changes to the Terms and Conditions. In contrast, the HPOS Terms and Conditions are displayed each time a user logs into HPOS.

The Review Panel gave particular consideration to the conditions relating to the protection of passwords and credentials to ensure users kept secure their or a site's access to HPOS. While this is defined in each set of conditions, it became clear to the Review Panel that these control mechanisms are not always followed. Numerous respondents cited anecdotal instances of multiple users of an individual credential, in some instances because of the delay between applying for a PKI certificate and delivery of the secure token and PIC. In short, the Review Panel was concerned that the Terms and Conditions are not always understood and complied with.

A number of respondents indicated the legal language commonly used in Terms and Conditions did not assist users to understand their obligations. In all three sets of Terms and Conditions, references are made to various pieces of Commonwealth legislation that a user would be bound by, including Section 130 of the *Health Insurance Act 1973* (which deals with the Medicare programme); section 135A of the *National Health Act 1953* (which governs the Pharmaceutical Benefits Scheme); as well the user declaration 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). In addition, legislation such as the Commonwealth's *Privacy Act 1988* and *Criminal Code Act 1995* are cited, along with various Department of Human Services policies. Added into this are various legal terms (often Latin) that are 'standard' contract law elements but are certainly not everyday terms. Respondents, faced with such detailed and arcane conditions, are likely to ignore their import.

Review Panel Finding: Not all users or organisations have a clear understanding of the security requirements surrounding PKI, PRODA or HPOS as outlined in the Terms and Conditions, or the obligations these conditions place on them as a user of these systems. This lack of clarity is exacerbated due to the use of legal and technical language in the documents setting out the conditions users must agree to before gaining system access.

Submissions were supportive of this perspective:

> *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.* – Consumers Health Forum of Australia

> *While legally sound, this information is however quite lengthy and may be unlikely to be read completely by users.* – Western Australian Department of Health

Further, the Review Panel agreed with the views expressed by the Australian Healthcare and Hospitals Association, which went further in outlining specific elements when these conditions may be breached:

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

Recommendation 12: It is recommended that the Terms and Conditions for HPOS, PKI and PRODA should be simplified and presented to users in a form that ensures that they fully appreciate the seriousness of their obligations.

The Review Panel suggests that a behavioural insights approach should be applied to the review of the Terms and Conditions. They need to be clear and succinct to ensure potential users fully understand the requirements and the significance of their obligations.

6 Telephone channels

Providers or their representatives can also obtain Medicare card details for their patients through the Department of Human Services' Medicare provider enquiries telephone line or PBS general enquiries line.

6.1 Medicare provider enquiries line

To obtain a Medicare card number through the Medicare provider enquiries line, the provider or representative must pass a security check, covering the provider's full name, provider number and practice location. This information is verified against the Department of Human Services' 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. The provider does not require consent from the patient to obtain the Medicare card number.

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 benefits (for example, if they are covered by a RHCA).

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

6.2 PBS general enquiries line

Medicare card numbers can be requested from the PBS general enquiries line under the Improved Monitoring of Entitlements (IME) measure that ensures pharmaceutical benefits are provided only to those people who are eligible to receive them. This channel is mostly used for other purposes; requests for Medicare card numbers are exceptions.

Medicare card numbers can be requested through this channel by:

- Approved pharmacists and their staff
- Admissions staff or accident and emergency staff from public hospitals participating in the Pharmaceutical Reform Arrangements.[30]

Callers are asked to provide their name and identify whether they are calling from a pharmacy or public hospital. Pharmacies must provide the pharmacy name and pharmacy approval number, and hospitals must provide the hospital name and pharmacy approval number. These details are checked against the Department of Human Services' systems. If they are correct, the call can proceed.

[30] The Pharmaceutical Reform Arrangements provide for public hospitals that are Approved Hospital Authorities under Section 94 of the *National Health Act 1953* to supply pharmaceuticals funded by the PBS for specific categories of patients. Where these arrangements are not in place, state and territory governments are responsible for funding pharmaceuticals provided to hospital patients.

When Medicare card details are sought, the caller is asked if they have the patient's consent to obtain and store their Medicare card details. They are then asked for the patient's name and address, with further patient details requested if required to uniquely identify the patient. Once the patient has been uniquely identified, the following information can be released:

- Medicare card number and IRN
- Medicare card expiry date
- Patient name (as held on the Medicare record for the patient).

Review Panel Recommendation: Encouraging use of HPOS

As outlined above, the Review Panel has identified a number of changes that can be made to improve the security of HPOS. Overall, however, it is clear to the Review Panel that HPOS provides significantly greater security than the Department of Human Services' telephone channels.

Review Panel Finding: The authentication and verification required before individuals can access HPOS, combined with the audit logs that capture all activity on HPOS, provide a higher level of assurance about the legitimacy of requests for Medicare card information than telephone requests.

The Review Panel notes that it has not seen any evidence of fraudulent requests for Medicare numbers through the telephone channels, but it remains concerned about the potential risks presented by these channels. There are improvements that can be made to the telephone channel procedures to reduce the risks, which are discussed below. However, the Review Panel believes that HPOS should be the default channel through which health professionals seek Medicare card numbers.

Submissions were supportive of this perspective:

> *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.* – Consumers Health Forum of Australia

> *As the provider enquiries line is far less secure than the online option, the RACGP supports the Review Panel's recommendation that HPOS is the default mechanism for requesting patient Medicare card numbers, and the recommendation that the provider enquiry line is available in a reduced capacity.* – Royal Australian College of General Practitioners

The Review Panel recognises that there will continue to be circumstances in which access to the telephone channels is required, including when HPOS Find a Patient is not available or does not return a result, or where internet access is not available to the health professional. Submissions emphasised the importance of continuing access to telephone channels in certain circumstances:

> *There are a number of contexts in which an optometrist will be unable to access a patient's physical Medicare card and won't have access to online services. This is most common in outreach clinics, including in remote Indigenous communities where patients may not present with the Medicare card or have access to their card and internet access may be limited. In these circumstances, it would be most appropriate for the provider line to be made readily accessible and for relevant information to be provided in a timely manner. –* Optometry Australia

> *It is critically important to our member health services, particularly in remote areas, that they continue to have access to clients' Medicare card numbers which is available by telephone if internet coverage or computer systems are down.* – National Aboriginal Community Controlled Health Organisation

> *Where access cannot be gained through online systems, or it proves difficult to find a Medicare card number via that route, the health professional needs an alternative option to obtain the required information, viz. the provider enquiries line.* – Northern Territory Department of Health

> *The Department is aware that Health Service Providers in rural and remote regions are more vulnerable to failure of internet-based systems and hence reliant upon telephone access. For this reason, the option of telephone access to Medicare information needs to be maintained.* – Western Australian Department of Health

The Review Panel is therefore not proposing that the telephone channels should be closed down. However, it believes that the Department of Human Services should aim to move health professionals' requests for Medicare card details away from the telephone channels to the greatest extent possible over the next two years. Telephone channels should only be available in exceptional circumstances. This would require the Department of Human Services to work with health professional groups who are not currently using HPOS, to support them to transition to HPOS. For example, in its submission to the Review, the Pharmacy Guild of Australia noted that pharmacists do not currently have access to HPOS, and that it '*would be a more efficient use of the Department and pharmacist time if pharmacies had access*'. The Review Panel is also aware of anecdotal reports that some providers, such as certain groups of medical specialists, make only limited use of the Department of Human Services' online services and are more likely to use the telephone channels.

The Department of Human Services should also continue to identify and implement enhancements to increase the useability of HPOS to further encourage uptake.

Recommendation 13: It is recommended that, in order to provide greater security and availability, the Department of Human Services should actively encourage health professionals to use HPOS as the primary channel to access or confirm their patients' Medicare card numbers, and that telephone channels be phased out over the next two years except in exceptional circumstances.

Review Panel Recommendation: Strengthening telephone security checks

The Review Panel gave considerable attention to the release of Medicare card information through the Department of Human Services' telephone channels. It noted that the telephone channels represented a smaller percentage of the total Medicare card access requests (roughly 588,000 calls to the provider enquiry line and a proportion of the 440,000 calls to the PBS general enquiries line, compared to 10.2 million HPOS searches). While the Review Panel has recommended that health professionals should be encouraged to use HPOS instead of the telephone channels, it recognises that some continued access to the telephone channel will be required in certain circumstances, especially where health professionals may not have access to reliable internet.

The challenge, as observed by the Review Panel, is that the current security check for release of Medicare card information provides a much lower level of confidence than the security requirements for the HPOS channel.

Review Panel Finding: The Review Panel observed that the information required in the provider security check to access a Medicare card number could be accessible by someone other than the provider. This information could potentially be obtained through a combination of sources.

This view is reflected in the submission from the Australian Medical Association:

> *The AMA believes that the Provider Enquiry Line currently represents the biggest risk for fraudulently obtaining Medicare numbers. –* Australian Medical Association

A majority of submissions supported the Review Panel's proposed recommendation to strengthen telephone security checks:

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

> *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. –* Consumers Health Forum of Australia

> *I am not aware of the current authentication tests applied to callers before Medicare card numbers are disclosed by the Department. However, in principle those tests should be as robust as those applied to access the HPOS. –* Office of the Australian Information Commissioner

The Review Panel understands that there are a number of options which the Department of Human Services could implement to strengthen the security checks. One option that would be supported by the Review Panel is the introduction of additional security questions based on information already held within the Department of Human Services' systems but which is not publicly available. This option would provide an added level of security but would not be onerous for health professionals.

Recommendation 14: It is recommended that, during the phasing down of the telephone channels, conditions for the security check for the release or confirmation of Medicare card information by telephone should be strengthened, with additional security questions having to be answered correctly by health professionals or their delegates.

7 Review Panel conclusions

Throughout the Review process, the Review Panel members have been mindful of the need to balance competing public interests. We believe that we have done so. We have been aided by the considered arguments put forward in face to face meetings and written submissions by health professionals and industry experts, and we thank all stakeholders for their valued input.

The Australian public can be confident in the protections that are already in place for their Medicare information. The recommendations put forward in this report aim to mitigate some areas of risk identified during the course of the Review.

We recognise that some of the recommendations will require changes in practice for individuals, health professionals and software developers. The Department of Human Services will need to work closely with stakeholders on the implementation of any recommendations accepted by Government.

We commend this report and its recommendations to Government.

Appendices

Appendix A: 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.

Appendix B: Submissions to the Review

Australian College of Nursing
Australian Healthcare and Hospitals Association
Australian Medical Association
Australian Privacy Foundation
M. Byrne
Consumers Health Forum of Australia
C. Culnane, B. Rubinstein and V. Teague (University of Melbourne)
eHealth Privacy Australia
Law Society of New South Wales
Medical Software Industry Association
National Aboriginal Community Controlled Health Organisation
New South Wales Health
Northern Territory, Department of Health
Office of the Australian Information Commissioner
Optometry Australia
Paediatrics at Burnside
Pharmacy Guild of Australia
Queensland Health
Royal Australian College of General Practitioners
Rural Doctors Association of Australia
Victorian Department of Health and Human Services
Western Australian Department of Health

The Review also received two confidential submissions.

Appendix C: Stakeholder meetings

Australian Association of Practice Managers
Australian College of Nursing
Australian Health Ministers’ Advisory Council
Australian Healthcare and Hospitals Association
Australian Privacy Foundation
Consumers Health Forum of Australia
MedicalDirector
National Aboriginal Community Controlled Health Organisation
New South Wales Health
Northern Territory Department of Health
Office of the Australian Information Commissioner
Queensland Health
Rural Doctors Association of Australia
Tasmanian Department of Health and Human Services
Victorian Department of Health and Human Services
Western Australian Department of Health

Appendix D: Acceptable Medicare Enrolment Documents

Purpose of document	**Acceptable documents**
Proof of identity	Birth certificate or extract Marriage certificate Current passport, travel document or Immicard Current driver's license Change of name certificate Proof of age card
Proof of birth	Birth certificate or extract Hospital certification FA081 Centrelink confirmation of birth (where permission to access the Centrelink record has been given by the applicant)
Proof of relationship	Birth certificate Marriage certificate Joint bank account Joint utility account Joint home ownership
Residency documents *Residency documents must be comprised of:* • *two Australian residency documents, or* • *one Australian residency document and one residency document from the applicant's previous country of residence*	*Acceptable Australian residency documents* Employment contract Rental or lease agreement for property Rental or lease bond paid for property Bank statement Evidence of children enrolled in an Australian school/childcare Private health insurance Property or contents insurance Gas, electricity, water or rates account. *Acceptable overseas residency documents* Evidence of sale of property Cessation of lease agreement for rental of property Proof of termination of employment Transit document for household goods and/or furniture Statement showing closure of bank account Cancellation of health insurance Cancellation of contents insurance
Residency documents – for visitors to Australia enrolling under Reciprocal Health Care Agreements *Where an applicant is being enrolled under a Reciprocal Health Care Agreement, both residency documents must be currently dated documents from the country which the applicant is enrolling under*	Employment contract Rental or lease agreement for property Rental or lease bond paid for property Bank statement Evidence of children enrolled in childcare, school or university Property or contents insurance Gas, electricity, water or rates account

Appendix E: HPOS User Roles

User Role One: Administrative staff

- Send/Receive messages and form upload
- Practice Inventive Program, if Registration Authority (RA) number is registered
- Practice Nurse Incentive Program, if RA number is registered
- Healthcare Identifiers Service, if RA number is registered
- Department of Veterans' Affairs (DVA) Website – opens the public DVA website
- My access history – An access log for the user

User Role Two: Administrative staff (Authorised by provider but not yet selected provider function to act on behalf of provider)

- All of the above and;
- Select provider – allows user to select a provider to act on their behalf
- Find a patient – allows user to search and confirm Medicare care details and check concessional entitlement

User Role Three: Delegated user (Authorised by provider and user has selected provider function)

- All of the above and;
- Find a patient – also allows the user to search, confirm and Multiple details request
- Submit/View Bulk Bill, Patient Claim and DVA Webclaims Claims
- Request and view report
- View provider personal details, add, view and update provider numbers
- National Bowel Cancer Screening Program
- Prescription Shopping Patient Summary reports
- MBS Items Online Checker
- MBS Partial Payment Calculator
- Child Dental Benefits Schedule
- Messages

User Role Four: Provider

The user can access all services, programmes and functions they are registered with. This is defined by the authorisation they have acquired in relation to the different programmes based on their identifiers and RA numbers. The user needs to have registered for the programme and been granted access.

Appendix F: Acronyms and Key Terms

AHHA – Australian Healthcare and Hospitals Association

AHPRA – Australian Health Practitioner Regulation Agency

AMA – Australian Medical Association

ANAO – Australian National Audit Office

B2B – Business to Business

CHF – Consumers Health Forum of Australia

DVS – Document Verification Service

Health professional – In this report, ‘health professional’ is used to refer to health service providers (such as doctors or allied health professionals) as well as administrative staff.

HPOS – Health Professional Online Services

IRN – Individual Reference Number

MBS – Medicare Benefits Schedule

My Health Record – a secure online summary of an individual’s health information.

NIPGs – National Identity Proofing Guidelines

NT – Northern Territory

OAIC – Office of the Australian Information Commissioner

PBS – Pharmaceutical Benefits Scheme

PIA – Privacy Impact Assessment

PIC – Personal Identification Code

PKI – Public Key Infrastructure

PRODA – Provider Digital Access

RA number – Registration Authority number

RACGP – Royal Australian College of General Practitioners

RDAA – Rural Doctors Association of Australia

Review – Independent Review of Health Providers’ Access to Medicare Card Numbers

RHCA – Reciprocal Health Care Agreement

WA Health – Western Australian Department of Health