Australian Government

Department of Human Services

Circumstances in which Australians' personal Medicare information has been compromised and made available for sale illegally on the 'dark web'

Submission to Senate Finance and Public Administration References Committee

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Department of Human Services (the Department) welcomes the opportunity to provide information to the inquiry on the robustness of its processes and systems to protect the personal information it holds, including Medicare card information.

The submission will provide contextual information on the Medicare card and why health professionals require access to Medicare card numbers. Information will also be provided on the channels within the Department by which individuals and health professionals can access Medicare card numbers.

The Department continues to improve the integrity and privacy of the personal information it holds. The submission will discuss the methods by which the Department abides by secrecy provisions and the *Privacy Act 1988* in relation to the collection, use and disclosure of personal information. This includes how the Department maintains business integrity and its compliance processes. The Department takes its obligations under the *Privacy Act 1988* and relevant secrecy provisions seriously. The security of personal information is paramount to the way the Department operates.

The submission will also comment on the Ministerial and Departmental response to the alleged incident, including the Australian Federal Police (AFP) investigation, the independent Review commissioned by the Federal Government, and the Department's service recovery processes to remediate potential risks that arise as a result of lost, stolen or damaged Medicare cards.

The submission will not provide input on clause c. of the Inquiry's Terms of Reference, as this content will be provided as part of the Australian Digital Health Agency's submission.

INTRODUCTION

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. The Medicare system is founded on principles of universality, accessibility and security. Every day, thousands of Australians use Medicare to access essential medical, allied and other health services funded through the Medicare system. The Department plays an important role through Medicare in providing access to free or subsidised health and hospital care for eligible individuals.

The Department is responsible for the development of service delivery policy to ensure access to health related payments and services. These payments and services are offered through a number of programmes including; Medicare, Pharmaceutical Benefits Scheme (PBS), Aged Care and Veteran's payments, Australian Immunisation Register, Australian Organ Donor Register, External Breast Prostheses Reimbursement Program, National Bowel Cancer Screening Register, Continence Aids Payment Scheme, and Child Dental Benefits Schedule.

As at 30 June 2017, there were 24.9 million persons enrolled in Medicare on 14.1 million active cards. In 2016-17 the Department processed 399.4 million Medicare services and paid benefits totalling $22.4 billion. Under the PBS, the Department processed 207.9 million services with total benefits paid being $12.4 billion.

The Department issues Medicare cards to eligible individuals. To be eligible an individual must live in Australia or Norfolk Island and be either:

- An Australian citizen
- A New Zealand citizen
- An Australian permanent resident
- Applying for permanent resident – conditions apply
- Covered by a Ministerial Order, or
- A Resident Return visa holder.

The Department also issues Medicare cards to individuals who are visiting from a Reciprocal Health Care Agreement country.

The Department increasingly uses technology to engage with people in response to customer demand and in line with contemporary social norms. The Department is continuing to transform its services by moving towards digital service delivery so that individuals can manage their interactions with the Department through easy-to-use, secure, integrated digital channels. In 2016-17, 97.1 per cent of Medicare claims were made digitally and 46 per cent of all health practices lodged 100 per cent of their Medicare claims digitally. For PBS 99.9 per cent of PBS claims were submitted digitally as at 30 June 2017. Online claiming for health professionals and individuals continues to grow year on year, making it simpler, quicker and more efficient with 594.1 million provider 'point of service' digital service transactions in 2016-17.

The Medicare card plays an important role in Australia as it represents the eligibility of an individual to access subsidised healthcare services and subsidised pharmaceuticals. The alleged sale of Medicare card numbers highlights the reality that the Medicare card has also become an important component of Australia's proof of identity processes. The Medicare card can be used to help verify an identity and, like other evidence of identity credential, is therefore susceptible to theft for identity fraud and other illicit activities. However, it is important to note that the Medicare card alone does not provide access to personal health information or Medicare online accounts. The Department remains

committed to protecting the privacy and security of customer information through the processes and policies outlined below.

PART ONE – HEALTH PROFESSIONALS ACCESS TO MEDICARE CARD NUMBERS

Access to Medicare card numbers is required by health professionals in order to verify the eligibility of a patient to receive Medicare services, and to lodge bulk bill or electronic patient claims at the practice. Health professionals access Medicare card numbers in order to confirm eligibility, so that patients who do not have their card with them at the time of service can still access Medicare services. This is particularly important for vulnerable Australians, including:

- Indigenous Australians in remote locations
- Individuals experiencing homelessness
- Individuals in emergency situations
- Individuals leaving domestic violence situations, and
- Young people who are still on a family Medicare card and may wish to access health services without their parents' knowledge.

Individuals must be eligible for Medicare in order to receive Medicare subsidised services. It is important to note that individuals can still access health services if they are not eligible for Medicare or if a health professional cannot confirm their eligibility. However, the health professional will not be able to bulk bill the patient or lodge a Medicare claim on their behalf. If eligible for Medicare, the individual can provide a correctly itemised receipt and lodge a claim for the Medicare or PBS rebate with the Department. The receipt does not need to include the patient's Medicare card number.

There are a number of channels through which health professionals can access Medicare card numbers when an individual is unable to present their card.

HEALTH PROFESSIONAL ONLINE SERVICE (HPOS)

HPOS was implemented by the Department in 2009 to enhance and improve the delivery of services to health professionals. HPOS offers health professionals a single secure web portal entry point which provides real-time access to a number of online services provided by the Department. Health professionals can manage their details, send secure, encrypted communication with the Department as well as connect with a number of services with programmes including but not limited to the Australian Immunisation Register, Child Dental Benefits Schedule, Centrelink Forms, Practice Incentives Program and access to the Department of Veterans' Affairs website.

One of the services offered through HPOS is the 'Find a Patient' functionality. It was offered to improve timeliness and access to necessary information for health professionals such as Medicare card numbers, and to assist health professionals to transition to secure online channels as an alternative to telephone interactions with the Department.

Through Find a Patient, health professionals can search and immediately obtain or confirm a patient's Medicare card number and concessional eligibility. To search for a patient's Medicare card number the health professional is required to enter the patient's first name, surname and date of birth. A postcode and/or locality/suburb can be used to further refine a search when more than one member of the public matches the information entered. Once a unique match is found, the screen will return the correct Medicare card number, Individual Reference Number (IRN), first name and card expiry date. The health professional can also confirm a patient's Medicare card number by providing the patient's full name, date of birth and the patient's Medicare card number. A successful search result will return the correct Medicare card number, IRN and first name. When using either of these services, the health

professional performing the search must first tick a box to confirm that the search is for claiming purposes only.

In 2016-17, the majority of Medicare card related requests were conducted through HPOS Find a Patient, with over 10 million searches.

Health professionals access HPOS through a Public Key Infrastructure (PKI) certificate (individual or site based) or a Provider Digital Access (PRODA) account.

To access these authentication mechanisms, a health professional is required to provide a number of identity documents and proof of their relationship with the Department, this includes a provider number and primary and secondary evidence of identity. Applicants for the PKI site certificate must provide evidence of the business entity.

An individual PKI certificate user can then access HPOS via software installed on their computer, a PKI USB insert, and after the certificate is identified, the health professional enters a Personal Identification Code (PIC), sent separately to the certificate. PKI site certificates access HPOS via a CD-ROM.

The PRODA account is an authentication model that needs no additional hardware or software to function. This can help to mitigate the risk of fraud because the PRODA authentication is highly individualised and has a two-step authentication process.

The PRODA authentication model has greater security and privacy measures in comparison to the PKI certificate. The Department is working with health professionals and key stakeholders to encourage uptake of the PRODA model and is working to enhance the functionality within PRODA to assist organisations moving from the PKI site certificate model.

PKI and PRODA each have terms and conditions which users must agree to. These can be found on the Department's website.[1] Users must also accept the HPOS Terms and Conditions of Use and Access. These are displayed on every logon to HPOS.[2]

As part of the terms and conditions, health professionals 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 and acknowledge requirement to keep personal information about other persons that they upload to the system or access from the system confidential and 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.

---

[1] Available online at https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents and
https://proda.humanservices.gov.au/pia/pages/public/registration/account/createAccount.jsf

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

Health professionals and individuals may be subject to penalties under the *Privacy Act 1988* where personal information is not handled in accordance with the Australian Privacy Principles[3]. More information can be found in the Privacy section.
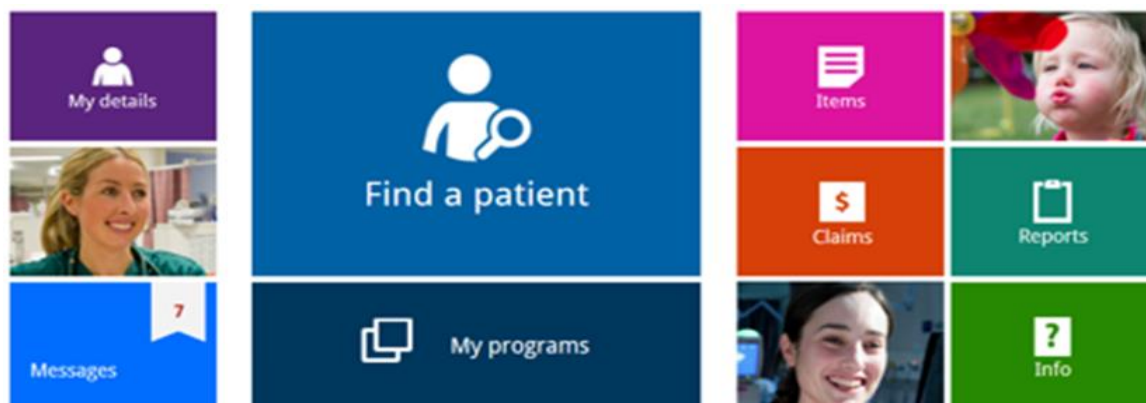
HPOS home screen for user with 'Find a Patient' access

PROVIDER ENQUIRY LINE

The Department provides a number of telephone lines to assist individuals and health professionals with access to information required to receive or administer health services. In 2016-17, the Department handled 14.8 million calls relating to Medicare programme services.

The Department offers a provider enquiry line that enables health professionals to confirm a patient's Medicare eligibility over the phone, which can be used when the patient does not have their Medicare card available. Up to seven requests for Medicare card details can be made per phone call. In 2016-17, over 500,000 requests were made through the provider enquiry line. The average length of time a caller waited for their call to be answered in 2016-17 was 1 minute and 56 seconds for the health services (provider) line.

The caller must pass a security check by confirming provider details which are verified via the Department's Provider Directory System. The caller is then required to provide sufficient patient information to uniquely identify the patient. If the caller is a practice staff member, they will be asked to confirm that they have permission from the provider to request this information.

Once the patient has been uniquely identified, Department staff can provide the patient's Medicare card number and IRN, Medicare card expiry date, and confirmation of the patient's Medicare eligibility on the date of service. Department staff are instructed never to release a patient's address or other contact details.

PRACTICE SOFTWARE

Healthcare practices can use third party software products to interact with the Department. These software products are used for practice management services such as client databases and appointment

---

[3] Possible penalties can be found under the *Privacy Act 1988*.

8

scheduling, as well as interactions with the Department including claiming, billing and reporting. In 2016-17, over 80 per cent of claims were submitted to the Department through practice software.

Software developers can choose to embed a link to HPOS within their software, which still requires a Department authentication mechanism, or utilise the Department's Business to Business (B2B) Patient Verification Services. B2B accesses the same patient search service offered through HPOS directly from the third party software using a PKI certificate (this service is not available for PRODA).

INDIVIDUAL ACCESS

Alternatively, individuals can access their own Medicare card details if they do not have their card with them. This includes through their Medicare Online account or the Express Plus Medicare mobile app, in the 'Digital Wallet' section where an image of the Medicare card can be viewed. Alternatively, individuals can call the Medicare general enquiries line and request their Medicare card number (noting they must pass a security check before their information is released) or attend a Department service centre with identity documentation and request a temporary paper copy of their card.
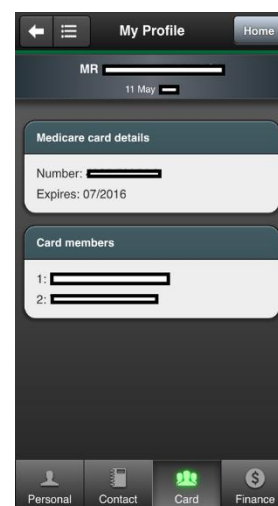
Express Plus Medicare mobile app home screen, digital wallet and profile.

PART TWO – DATA PROTECTION PRACTICES

The Department takes the security of Medicare information and other personal data that it holds seriously. This is reflected in the cyber security protections that are in place for the information the Department holds on behalf of others.

The Department is the custodian of significant data holdings relating to all Australians, including personally identifiable information that can be used to identify, contact, or locate an individual.

The Department has effective risk controls in place to ensure that it is well positioned in its approach to cyber security, and continues to assess risks and work closely with national and international agencies to ensure the safeguards follow global best practice.

The cyber security governance, management and operational practices are designed to enable the Department's business and provide assurance in response to the changing threat environment.

The Department's compliance with the mandatory requirements of the Australian Government Protective Security Policy Framework is managed through activities such as effective security risk management, monitoring and review of security plans and policies, and training and education.

The Department's protective security policy aligns with the framework and emphasises the need for security as part of the Department's culture.

In June 2014, the Australian National Audit Office (ANAO) released Audit Report No. 50 2013–14, *Cyber Attacks: Securing Agencies' ICT Systems*[4]. This examined the implementation of the mandatory strategies in the *Australian Government Information Security Manual* (Top Four mitigation strategies) by seven agencies, including the Department's implementation of these strategies. The Top Four mitigation strategies are application whitelisting, patching applications, patching operating systems and minimising administrative privileges. The audit found that none of the seven agencies were compliant with the Top Four mitigation strategies at that time.

In 2016-17, the ANAO undertook a follow-up audit of the performance of each agency and reported 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[5].*

The Department of Human Services also completed a self-assessment against the strategies and met its commitment to achieving compliance during 2016. The Department was confirmed as cyber resilient[6].

---

[4] The full report is available online at https://www.anao.gov.au/work/performance-audit/cyber-attacks-securing-agencies-ict-systems.

[5] This report can be accessed: https://www.anao.gov.au/work/performance-audit/cybersecurity-follow-audit

[6] 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.

PART THREE – MINISTERIAL AND DEPARTMENTAL RESPONSE TO JULY 2017 INCIDENT

On 4 July 2017, media outlets reported that a dark web vendor was illegally selling Medicare card numbers. The incident was subsequently referred to the AFP who have commenced an investigation.

The Department understands that investigation to be ongoing. It would be inappropriate to comment on the specific matters subject to the ongoing AFP investigation.

INDEPENDENT REVIEW

On 10 July 2017, the Commonwealth Government commissioned a Review of Health Providers' Access to Medicare Card Numbers (the Review)[7]. The Review was commissioned to consider the balance between appropriate access to Medicare card numbers for health professionals to confirm patients' Medicare eligibility, with the security of patients' Medicare card numbers. The Review will identify options to improve the security of Medicare card numbers while continuing to support access to health services without unnecessarily increasing the administrative workload faced by health professionals.

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

The Review is working with relevant stakeholders including peak health bodies (such as the AMA, the RACGP, the Australian Association of Practice Managers, the Consumers Health Forum, Australian College of Nursing and the National Aboriginal Community Controlled Health Organisation) and Australian and State and Territory Governments.

The Review released a discussion paper on 18 August 2017 and invited interested parties to provide written submissions to inform the Review's final report, which will be submitted to Government by 30 September 2017. The final report will present recommendations for immediate practical improvements, and may also identify medium to longer term changes to improve the balance between the security and accessibility of Medicare card numbers.

---

[7] Terms of Reference of the Review can be found in Appendix One

PART FOUR – PRACTICES, PROCEDURES AND SYSTEMS

SERVICE RECOVERY

The Department has robust service recovery processes in place to mitigate any potential risk of lost, stolen or damaged Medicare cards. A replacement card can be issued when the original card is worn, damaged, lost, stolen or expired. The service recovery process for the alleged incident has concluded.

Individuals can request a new Medicare card through a number of channels, including digitally through myGov or the Express Plus Medicare mobile app, or by contacting the Medicare general enquiries line. Individuals can also visit a service centre with proof of identity. Alternatively, individuals can request a card via a signed letter to the Department including their Medicare card number, address and certified copy of identification. Acceptable forms of identification include:

- Birth Certificate or extract
- Current driver's licence
- Current passport, travel document or Immicard
- Marriage certificate
- Change of name certificate, or
- Proof of age card.

If an individual requests a replacement card via the Medicare general enquiries line, they must pass a security check. This includes the provision of a number of details to verify against the information held with the Department.

In addition, the Department undertakes service recovery processes for Medicare cards where there is unauthorised activity or fraudulent behaviour.

If unauthorised activity is detected, the Department moves to prevent further fraudulent use. The Department can place a business integrity (BI) flag on a Medicare card number that is of interest to compliance activities for potential fraud abuse or inappropriate practice. When a BI flag is placed on a Medicare card number, it prevents any activity on the card, including claiming or updates to personal information. Compliance activities can be raised internally through the Department's monitoring of claiming behaviour or health professionals and individuals can provide information to the Department via a form or by phone for investigation.

Department staff will transfer all affected individuals to a new Medicare card number, contact them by phone or letter and send the new Medicare card to the contact details held by the Department. The new Medicare card number is then flagged with a MPI tier two flag which will remain on the record. This flag alerts Department staff that there has previously been unauthorised activity relating to the individual and, when conducting security checks or updating customer information, to be mindful that further attempts of unauthorised activity may occur.

It is important to note that illegally obtained Medicare card numbers are not sufficient on their own to provide access to clinical records or an individual's My Health Record.

PRIVACY

The Department takes its obligations under the *Privacy Act 1988* and relevant secrecy provisions seriously. The security of personal information is paramount to the way the Department operates.

In collecting, using and disclosing personal information of individuals, the Department must meet both the requirements of the *Privacy Act 1988*, and the secrecy provisions in legislation which apply to the Department's administration of programmes and services (such as the *Health Insurance Act 1973* and the *National Health Act 1953*). Penalties may apply where personal information is not handled in accordance with relevant secrecy obligations or the Australian Privacy Principles in the *Privacy Act 1988*.

The Department is committed to protecting privacy and has comprehensive processes to protect personal information. The Department's privacy framework is guided by the Department's Operational Privacy Policy, which includes a number of requirements with which Department staff must comply with. The policy reinforces that:

- all staff acknowledge their privacy and confidentiality responsibilities every year, and
- privacy incidents must be reported as soon as they are identified.

The Department is required to have a Privacy Policy under the Australian Privacy Principles. The Privacy Policy outlines how the Department manages personal information[8]. The Department's Privacy Policy is publicly available on the Department's website and is made available, upon request, through Department service centres free of charge.

In 2013-14, the ANAO undertook Audit No. 27, *Integrity of Medicare Customer Data*[9]. The audit examined the effectiveness of the Department's management of Medicare customer data and the integrity of the data.

The audit found that overall the Department has a comprehensive framework for managing Medicare customer privacy. Specifically, the audit found that the Department has processes, guides and policies in place to support compliance with the relevant legislative provisions under the *National Health Act 1953* and the *Health Insurance Act 1973* for secrecy and confidentiality as well as obligations under the then Information Privacy Principles, now Australian Privacy Principles under the *Privacy Act 1988*, and the Privacy Guidelines for Medicare Benefits and Pharmaceutical Benefits Programs.

The audit made five recommendations for the Department to consider and the Department has now implemented all five recommendations.

COLLECTION

The Department may collect an individual's personal information where it is reasonably necessary for, or directly related to, one or more functions or activities. The Department requests information directly from individuals or obtains it from other government agencies and third parties where authorised by law. For example, under the *Health Insurance Act 1973* the Department is authorised to collect information from health professionals for the purposes of assessing a payment of benefit under the Medicare Benefits Programme.

USE

The Department can only use personal information for the purpose for which it was collected, unless the individual to whom the information relates has consented to another use, or another use is authorised by law. Personal information is collected and used by the Department for a number of

---

[8] The Privacy Policy can be accessed at: https://www.humanservices.gov.au/corporate/publications-and-resources/privacy-policy

[9] The ANAO report can be accessed at: https://www.anao.gov.au/work/performance-audit/integrity-medicare-customer-data.

purposes including the administration of payments and services. This includes undertaking proof of identity checks and allocation of healthcare identifiers.

DISCLOSURE

Personal information can only be disclosed by the Department for the purposes for which it was collected, or for a secondary purpose if the individual consents or it is authorised by law. For example, the Department may disclose personal information to Australian Government agencies, state and territory agencies and other third parties for lawful purposes such as detecting and investigating cases of serious non-compliance and fraud.

SECURITY AND QUALITY

The *Privacy Act 1988* requires the Department to take reasonable steps to protect the personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure.

The Department must also take reasonable steps to ensure the personal information it collects is accurate, up to date and complete, and that the personal information used or disclosed is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure. The Department regularly reminds individuals to update their personal information with the Department.

BUSINESS INTEGRITY

Section 10 of the *Public Governance Performance and Accountability Rule 2014* (the Fraud Rule) requires the Department to have an appropriate mechanism for preventing fraud, which includes fraud awareness, education and communication activities, a comprehensive Fraud Control Plan, regular Fraud Risk Assessments and suspected fraud reporting mechanisms. The Department has a comprehensive, integrated and systematic approach to fraud control. Fraud awareness messaging and training is delivered to Department staff and contractors, which includes fraud risks and how to report suspected fraud.

The Department has stringent controls in place to prevent unauthorised access to information and systems regarding Medicare patient details. These controls include a detection programme, which can proactively monitor risks of unauthorised access to Medicare records and high-risk transactions. It also examines the access to Medicare data across a wide variety of systems, including backend systems and access outside the organisation by health professionals and similar organisations. The Department can detect unauthorised attempts by Department staff to release official information via email, including the release or theft of Medicare data.

The Department can examine external access to Medicare numbers, including through HPOS. HPOS has effective audit logging capabilities; all transactions made by users, including searches and account updates, are captured and stored.

The Department works closely with other Government Agencies including the Australian Taxation Office (ATO) to share identity security risks and threats, such as scams seeking to access personal identifying information.

The Department conducts investigations into internal and external fraud allegations in line with the Australian Government Investigations Standards. Examining all detected incidents and allegations involving internal fraud, unauthorised access, and unauthorised disclosure, across all programmes,

administrative functions and Departmental data. This includes incidents and allegations related to Medicare fraud conducted by a dedicated unit.

The Department collaborates with internal and external stakeholders to support and inform its investigations referring more serious and complex criminal investigations to the AFP.

COMPLIANCE

The integrity of the payments processed by the Department rely largely on health professionals to determine and claim correctly in relation to the services they provide. Compliance is a shared responsibility between the Department and the Department of Health.

'Provider compliance' which refers to the compliance activity focused on registered providers, as well as employers of the providers and their entities is a key activity. This includes, but is not limited to, receptionists, practice managers and others.

The objective of provider compliance is to ensure correct payment of benefits to an eligible patient for an eligible service by an eligible practitioner. This is governed under the *Health Insurance Act 1973* and *National Health Act 1953.*

Compliance activities aim to undertake appropriate treatment and recovery action including audits and reviews, peer reviews through Practitioner Review program, investigation, education and behavioural interventions. Investigations are conducted in line with the Department's fraud control processes, which are deliberately focused on the most serious cases of non-compliance instead of people making honest mistakes.

The compliance program ensures continual assessment and monitoring of risks for health programmes using the best available evidence. Sophisticated methods are used to detect possible inappropriate practice or claiming including:

- monitoring and comparing claiming profiles of health professionals to identify inconsistencies,
- identifying unusual patterns of item usage and item combinations, and
- investigating tip offs.

To understand emerging risks and trends, officials consult with a wide range of stakeholders, such as other Government Departments, the AMA, RACAGP and the Pharmacy Guild of Australia.

In 2016-17, the Department of Health, through provider compliance, raised debts of more than $29 million in incorrect Medicare benefits and other health support payments. The two Departments continue to achieve results from investigations, with several matters referred to the Commonwealth Director of Public Prosecutions.

GLOSSARY

AFP – Australian Federal Police

ANAO – Australian National Audit Office

AMA – Australian Medical Association

APP – Australian Privacy Principles

B2B – Business to Business

BI – Business Integrity

FOI – Freedom of Information

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

HPOS – Health Professional Online Services

IRN – Individual Reference Number

MPI – Medicare Payment Integrity

PBS – Pharmaceutical Benefits Scheme

PKI – Public Key Infrastructure

PRODA – Provider Digital Access

RACGP – Royal Australian College of General Practitioners

APPENDIX 1 - TERMS OF REFERENCE OF INDEPENDENT REVIEW

(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.

Circumstances in which Australians' personal Medicare information has been compromised and made available for sale
illegally on the 'dark web'
Submission 7

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.