Australian Government

Australian Government Response to the Senate Finance and Public Administration References Committee Report:

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

February 2018

Introduction

The Australian Government welcomes the opportunity to respond to the Senate Finance and Public Administration References Committee's report on its Inquiry into 'the circumstances in which Australians' personal Medicare information has been compromised and made available for sale illegally on the "dark web"' (the Report).

The Australian Government thanks the individuals and organisations who contributed to the Senate Inquiry in preparing written submissions and/or appearing at the public hearing.

The Australian Government provided input to the Senate Inquiry through submissions from the Department of Human Services and the Australian Digital Health Agency, and evidence from officials from the Department of Health, Department of Human Services and Australian Digital Health Agency at a public hearing on 15 September 2017.

The Australian Government notes that the majority report and additional comments from the Coalition Senators made no recommendations; however, a dissenting Australian Greens report made four recommendations. The Government response addresses issues noted in the majority report and Coalition Senators' additional comments, as well as responding to the recommendations from the Australian Greens.

As the custodian of significant data holdings relating to all Australians, the Australian Government is committed to protecting the privacy and security of personal information, and takes the security of Medicare information and other personal data it holds seriously.

The Government's commitment to protecting the security of Medicare information is demonstrated by the establishment of an Independent Review of Health Providers' Access to Medicare Card Numbers (the Review) following media reports that personal Medicare card details were allegedly for sale illegally on the 'dark web'. The Review was established prior to the referral of this matter to the Finance and Public Administration References Committee, and the timing of the Review overlapped with the Senate Inquiry.

The Review panel, led by Professor Peter Shergold AC and supported by the Presidents of the Australian Medical Association and the Royal Australian College of General Practitioners, presented its report to Government on 5 October 2017. The report contains 14 recommendations that seek to improve the security of Medicare card details without placing undue burden on the health sector or limiting access to health services. The Australian Government formally responded to the Review in February 2018, agreeing or agreeing in-principle to all 14 recommendations. A copy of this response is included at Attachment A.

Response to Report and Coalition Senators' Additional Comments

The Australia Government notes that the majority report did not make any recommendations, and also that the Committee expressed concern about some matters, which are addressed below. The Australian Government has also provided further comments below on some issues that were explored in the majority report, including the use of Medicare cards as evidence of identity, and the implications for the My Health Record roll-out.

Department of Human Services information security

At paragraph 1.42 (page 56), the report raises the issue of potential identity fraud, stating:

> *The submissions from the department do not indicate that this risk is fully understood, or has been addressed.*

The Australian Government, and the Department of Human Services, take the security of personal information and the risk of identity fraud very seriously.

The Department of Human Services has a comprehensive, integrated and systematic approach to fraud control, including strict controls 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. The Department of Human Services can detect unauthorised attempts by staff to release official information, including Medicare data, via email.

As noted in paragraph 1.2 of the Coalition Senators' Additional Comments, the Department of Human Services has implemented all five recommendations from the 2013-14 Australian National Audit Office (ANAO) audit into the Integrity of Medicare Customer Data, including ensuring compliance with the mandatory requirements of the Information Security Manual. This audit also found that overall the Department has a comprehensive framework for managing Medicare customer privacy, with processes, guides and policies in place to support compliance with secrecy and confidentiality provisions under the *National Health Act 1953* and the *Health Insurance Act 1973*; obligations under the *Privacy Act 1988*; and Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programmes.

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

During 2016, the Department of Human Services completed a self-assessment against the Top Four mitigation strategies and assessed the Department as cyber resilient.

In 2017, the ANAO also confirmed the Department of Human Services as cyber resilient in the report of its Cybersecurity Follow-Up Audit (which was a follow-up to its 2014 report, Cyber Attacks: Securing Agencies' ICT Systems). The ANAO 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.*

Contact with affected individuals

At paragraph 1.43 (page 56), the report suggests that the Australian Government did not act quickly enough to inform people who had their Medicare details compromised.

The Department of Human Services has robust service recovery processes in place to mitigate any potential risk of lost, stolen or damaged Medicare cards. When unauthorised activity or fraudulent behaviour is detected, the Department of Human Services transfers all affected individuals to a new Medicare card number; contacts them by telephone or letter; and sends the new Medicare card to the contact details held on the customer's record.

In line with this process, the Department of Human Services immediately referred the matter to the Australian Federal Police (AFP). The Department commenced service recovery, including contacting all 165 affected people, as soon as possible once the AFP authorised it to do so and issued new Medicare cards. The Department of Human Services also implemented processes to escalate enquiries from any customer calling or attending a service centre with concerns about their card details.

The Department of Human Services confirmed at the public hearing that there was no evidence of any inappropriate Medicare claiming activity or other transaction on any identified Medicare card.

Use of Medicare cards as evidence of identity

The Australian Government acknowledges the committee's view that identity theft is a serious issue, and that Medicare card numbers do hold a degree of value to identity thieves and those that seek to profit from their illegal collection and sale (1.39).

The Australian Government also notes that a Medicare number is rarely used in isolation to commit identity fraud, and that the Government response to the Independent Review of Health Providers' Access to Medicare Card Numbers notes that organisations that accept Medicare cards as secondary evidence of identity should (where appropriate) use the Document Verification Service (DVS) to confirm that the details on the card correspond with a valid and current Medicare record.

The Australian Government supports the Committee's view that the Medicare card should be retained as a form of secondary evidence of identity, and for the credential to continue to be verifiable through the DVS.

Implications for My Health Record roll-out

The Committee notes at paragraph 1.28 that some stakeholders providing evidence to the Inquiry were 'concerned that the compromise of some Medicare data numbers potentially undermined the public's confidence in Australian government digital services, which may slow the roll-out'. To assist in mitigating these concerns, some further information about the My Health Record, including the security arrangements to protect personal information contained in the system, is at Attachment B.

Response to Dissenting Report by the Australian Greens

Recommendation 1

The Australian Greens recommend that the use of Medicare numbers under the Attorney-General's Document Verification Service (DVS) scheme should be reviewed.

Government Response: Not supported.

The Australian Government's view is that a review of this nature is not required, for the reasons outlined below.

1. The DVS helps to strengthen the integrity of Medicare cards by providing a government endorsed method for their verification. Taking into consideration that Medicare cards are now the second most commonly verified document through the DVS, with around 4.6 million (or 15 per cent) of all transactions conducted using Medicare data during 2016-17 alone, it is probable that verifying Medicare information in this way does more to *prevent* identity fraud than increase the risk of misuse of people's personal information.
2. Medicare information is not sufficient on its own to verify an individual's identity. Medicare cards are not considered primary evidence of identity documents due to the absence of a photograph or other means of providing a 'linkage' between the card and its purported owner. They do however play an important part as a form of secondary evidence—that is, they help to establish that an identity is being used in the community. The National Identity Proofing Guidelines require a combination of primary and secondary documents be used in the identity verification process.
3. Withdrawing Medicare cards as a recognised form of secondary evidence from the DVS would have significant impacts for a range of government agencies and private sector organisations which would need to find alternative ways to verify evidence of a person's identity operating in the community, which may be less reliable than Medicare cards. The education sector would be particularly impacted given the high volume of DVS checks involving Medicare cards that are undertaken to support the issuance of Unique Student Identifiers. There would also be significant regulatory impacts for private sector organisations, particularly in the telecommunications and financial sectors who would find it harder to meet legislated customer identification requirements, with flow on impact on consumers who may also incur greater time and cost in verifying their identities.

The Department notes that the Independent Review of Health Providers' Access to Medicare Card Numbers recommended that Medicare cards should be retained as a form of secondary evidence for identity purposes (recommendation 1).

Recommendation 2

The Australian Greens recommend that the security and privacy issues raised in this inquiry are addressed by DHS and ADHA to bring security of HPOS and My Health Record up to world best-practice.

Government Response: Not supported.

The Australian Government does not support this recommendation, as both the Department of Human Services and Australian Digital Health Agency already have robust processes in place to ensure personal information is protected.

Department of Human Services

The Department of Human Services is the custodian of significant data holdings, including information that can be used to identify, contact or locate an individual. It works with national and international agencies to ensure that the protections in place for this information are in line with global best practice.

The Department of Human Services proactively monitors risks of unauthorised access to Medicare records and high-risk transactions. The Department of Human Services' controls include detection of unauthorised attempts to release official information via email, including the release or theft of Medicare data. It also examines access to Medicare data across a wide variety of systems, including backend systems and access outside the organisation by health professionals and similar organisations (including through Health Professional Online Services).

The 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'. The report noted that (page 10 of the ANAO report):

> *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.*

The Department of Human Services has also implemented all five recommendations from the ANAO's 2013-14 audit report, *Integrity of Medicare Customer Data*, including ensuring compliance with the mandatory requirements of the Information Security Manual. This report found that overall, the Department of Human Services has a comprehensive framework for managing Medicare customer privacy.

Australian Digital Health Agency

The Australian Digital Health Agency employs a 'Defence in Depth' approach to the security of the My Health Record system, which enables multiple layers of security – both technical and non-technical controls – that work simultaneously to protect critical data.

The My Health Record system complies with the Australian Government requirements for storing and processing protected information including:

- the Australian Government Information Security Manual, produced by the Australian Signals Directorate
- the Protective Security Policy Framework, administered by the Attorney General's Department
- Information Security Standards – ISO 27000 series
- Risk Management Standard – ISO 31000.

The Australian Digital Health Agency actively monitors and responds to threats and risks within the cyber security environment, and has a program of continuous improvement using the internationally recognised management framework, Information Technology Infrastructure Library.

Recommendation 3

The Australian Greens recommend that DHS and ADHA report on their knowledge, actions, and outcomes in regards to the prior incidents of fraud related to Medicare numbers, as raised in October 2015 Estimates.

Government Response: Not supported.

The Australian Government does not support this recommendation as providing details of the outcome of previous fraud cases and the actions taken to address these cases may impede future investigations. However, some general information is provided below.

During 2015, the Department of Human Services became aware of potential fraudulent claiming of Medicare benefits. As a result, the Department of Human Services has investigated matters where identified individuals made false claims on their own record, the record of a family member or the record of another individual using information illegally obtained elsewhere, such as a medical practice.

The Department of Human Services has taken a number of steps to strengthen the integrity of the Medicare system in the online environment. Following the implementation of these steps, the Department of Human Services has seen a reduction in suspected claims received and benefits paid. The Department of Human Services continues to be vigilant using its data analytic capability to monitor Medicare claiming trends.

Recommendation 4

The Australian Greens recommend that the government implements the recommendations of the "Independent Review of Health Providers' Access to Medicare Card Numbers" as soon as possible.

Government Response: Agree in principle.

On 14 October 2017 (prior to the release of the Senate Inquiry report on 16 October 2017), the Australian Government gave its in-principle support to all 14 recommendations. A detailed response to the Review's recommendations was released in February 2018, setting out an ambitious timetable for implementation. Of the 14 recommendations, seven will be fully implemented by 30 June 2018, with a further four fully implemented by 31 December 2018 and one by mid-2019. The remaining two require no change to current practice.

The full response, including details of the Australian Government's plans for implementation, is at Attachment A.

Attachment A

Australian Government Response to the Independent Review of Health Providers' Access to Medicare Card Numbers

February 2018

Introduction

On 10 July 2017, the Minister for Health, the Hon Greg Hunt MP, and the then Minister for Human Services, the Hon Alan Tudge MP, announced an Independent Review of Health Providers' Access to Medicare Card Numbers. The Review was commissioned following media reports that Medicare card numbers were available for sale on the 'dark web'. These reports were referred to the Australian Federal Police, and its investigation is ongoing.

The Review Panel was led by Professor Peter Shergold AC, and 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 delivered two papers, a Discussion Paper (comprising the interim report for the Review), which was released for public consultation on 18 August 2017, and a Final Report containing 14 recommendations, which was presented to the Minister for Health and the then Minister for Human Services on 5 October 2017.

The Review Panel considered how to balance appropriate access to Medicare card numbers for health professionals to confirm patient eligibility for health services with the security of patients' Medicare information. The Final Report provided recommendations that aimed to improve the security of access to Medicare card numbers, including through the Department of Human Services' Health Professional Online Services (HPOS) system and its telephone channels, while also continuing to support access to health services without unnecessarily increasing the administrative workload faced by health professionals.

The Government takes the security of Australian's personal information seriously, and welcomes the Review Panel findings. The Government also acknowledges the valuable input from stakeholder groups which informed the Review recommendations.

This response acknowledges the need for immediate practical improvements to the security of Medicare card numbers while continuing to ensure people have access to the health care they need in a timely manner. It also recognises medium to long term changes required to reinforce the security of the HPOS system.

The case for change presented by the Review Panel

The Review Panel recognised the inherent value of a mechanism by which medical and other health practitioners can search for or confirm the Medicare number of a patient in order to assist with ensuring that all Australians have access to timely and affordable healthcare. The Panel noted that the current HPOS and telephone channels are critical in ensuring healthcare remains accessible including for vulnerable individuals who may not be able to present their Medicare card. However, the system has to balance convenience with security.

The Review Panel recommended several changes and improvements to existing HPOS access controls, including transitioning healthcare providers away from the Public Key Infrastructure (PKI) certificates which enable access to Department of Human Services systems to the more modern and secure Provider Digital Access (PRODA) authentication; suspending inactive accounts to prevent inappropriate use; and introducing time limits for delegate arrangements.

The Review Panel identified the need to build public awareness of the importance of protecting Medicare information, recognising the role Medicare numbers play not only in supporting access to health services, but in Australia's identity proofing processes. The Review Panel also made recommendations targeted at giving patients greater control and awareness of access to their Medicare card numbers, requiring that

health professionals have their consent before accessing their Medicare details and giving patients information about how to request access to the audit logs of health professionals who have sought access to their Medicare card numbers through HPOS held by the Department of Human Services.

In keeping with the broader theme of identity security, the Review Panel also recommended that health professionals ensure that appropriate identity checks are made when individuals first present to a health service. This would reduce the potential for individuals to fraudulently claim benefits using another person's Medicare details.

The Government's plans to implement the recommendations

The Government welcomes the opportunity to respond to the Review and acknowledges the excellent work of Professor Shergold and the Review Panel. The Panel's recommendations are practical, evidence-based and in keeping with the Government's mandate to preserve Medicare as the cornerstone of public healthcare in Australia.

The Government agrees without qualification to 13 recommendations put forward by the Review Panel, and confirms its in-principle agreement to recommendation 13, pending further examination of implementation options. This recommendation requires further stakeholder engagement to develop a robust implementation plan, given its potential impact on the health sector and consumers.

Overall, the Government will fully implement seven of the recommendations by 30 June 2018, with a further four to be fully implemented by 31 December 2018 and one by mid-2019. The remaining two require no changes to current practice.

Further description of the Government's approach to each recommendation appears in the table below.

A progress report on the implementation of the recommendations will be provided to Government in mid-2018.

What these changes will mean for health professionals and consumers

All Australians, including those delivering health services and those accessing these services, have a role to play in protecting the security of Medicare information. Health professionals and consumers alike will see some changes as a result of the Government's implementation of these recommendations.

Health professionals are likely to have to make changes to their administrative arrangements as new requirements are implemented. They will be supported by detailed information and educational materials, and the Government will work closely with professional colleges and organisations to assist their members with the transition.

Consumers may find that they will begin to be asked to provide identification when first accessing Medicare services at a healthcare provider. This should not be onerous, and should not serve as a barrier to health care. By providing identification, consumers will be playing an essential role in supporting the ongoing integrity of the Medicare system. The Government will also empower consumers to protect their own Medicare card information by building public awareness and supporting consumers to access information about how their Medicare card number is used.

The Government will work closely with health peak bodies on the implementation of specific recommendations. The Office of the Australian Information Commissioner will also be consulted on the implementation of recommendations relating to establishing appropriate privacy and security controls for personal Medicare information.

The Government takes seriously its obligation to protect the significant personal information of Australians, and is working to maintain and strengthen its defences against ever more sophisticated cyber and criminal attacks. While the implementation of the recommendations set out below may involve short term inconvenience during the transitional stages, it will bring greater security to a system that benefits all Australians.

Recommendations and Government response

Recommendation	Government response
1. It is recommended that the Medicare card be retained as a form of secondary evidence for identity purposes.	**Agreed.** Statement The Government agrees with the Panel's view that Medicare cards should continue to be permitted to be used as secondary evidence of identity, albeit with appropriate checks. Medicare cards are widely used as evidence of identity throughout the community in engagement with both the public and private sectors. Moreover, Medicare cards are not sufficient on their own to verify an individual's identity. Implementation Approach There will be no changes to existing processes involving the use of Medicare cards as secondary evidence of identity. The Government notes that organisations that accept Medicare cards as evidence of identity should, where appropriate, use the online Document Verification Service to confirm that the details on the card correspond with a valid and current Medicare record.

Recommendation	Government response
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.	**Agreed.** Statement The Government recognises the important role of the Medicare card in providing access to subsidised healthcare services and subsidised pharmaceuticals, as well as its role in Australia's proof of identity processes. The Government agrees with the Panel's recommendation to encourage further public awareness and will work to implement this recommendation immediately. Implementation Approach The Department of Human Services is developing a Communications Plan and associated Stakeholder Engagement Strategy, to outline public awareness activities to be implemented throughout 2018 and 2019 and on an ongoing basis. These activities will encourage members of the public to take a more active role in protecting their Medicare information, including asking why their Medicare information is being collected, and how it will be used and protected. Activities targeted at organisations will remind them of their obligation to protect Medicare information, and consider whether they really need to collect it and how they will store it safely. The Department will use existing communication channels to promote these messages to individuals and organisations, including its social media accounts, website, letters and stakeholder liaison. It will also identify government agencies and organisations which are undertaking related communications activities, so that communications activities can be combined for greater impact and similar messaging can be leveraged.

Recommendation	Government response
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.	**Agreed.** Statement The Government supports this recommendation. The Government's preferred approach is to achieve this recommendation by working with the health sector to establish profession-led guidance materials for medical professionals to follow. Implementation Approach The Departments of Health and Human Services will work collaboratively with health professional bodies to ensure their existing guidance and educational materials are reviewed and enhanced to address patient identification responsibilities under Medicare as well as within the context of the doctor-patient relationship. The aim is to ensure that health sector peak bodies have assessed, and updated if necessary, their existing guidance materials by the middle of 2018. Ongoing monitoring of the implementation of this recommendation will occur through the compacts established between the Government and health sector bodies.
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.	**Agreed.** Statement The Government recognises the right of individuals to have control over their Medicare information. The Government will empower individuals through its implementation of this recommendation, which it envisions will also increase the integrity of health services. Implementation Approach Work to implement this requirement has commenced, with changes to be implemented in the first half of 2018. The Department will communicate the new requirements to health professionals through its usual information channels.

Recommendation	Government response
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.	**Agreed.** Statement The Government supports the Panel's recommendation to increase patient control and allow access to audit logs of health professionals who have sought access to the Medicare card number. The Government believes this will further empower patients as well as assisting in identifying potential fraudulent activity. Implementation Approach Information about requesting audit logs will be added to the Department of Human Services' 'Personal Information' webpage, and internal processes updated to enable these requests to be fulfilled. Education will be provided to staff about the changes so that they are able to provide customers with accurate information about access to audit logs. These changes will be implemented in the first quarter of 2018.
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.	**Agreed.** Statement The Government notes the Department of Human Services is compliant with mandatory requirements of the Australia Government Security Policy Framework and relevant legislation. The Government remains committed to improving the privacy and security of personal information and notes the Department's robust frameworks and standards that incorporate privacy into project planning and delivery. Implementation Approach The Department will undertake appropriate privacy assessments as part of the implementation process for any recommendation involving the handling of personal information. As noted by the Review Panel, this is already part of the Department's Project Management Framework and Standards.

Recommendation	Government response
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.	**Agreed.** Statement The Government recognises the importance of delegate arrangements to health professionals, but agrees with the Panel's view that the delegate function would benefit from additional security enhancements. The Department of Human Services will ensure that any change to the delegate arrangements will minimise the administrative burden on health professionals. Implementation Approach Work has commenced to implement this recommendation, and this change will be introduced within HPOS in the second half of 2018. The Department will communicate the changes to health professionals through its usual information channels.

Recommendation	Government response
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.	**Agreed.** Statement The Government recognises that there are exceptional circumstances in which the ability to search for multiple Medicare card numbers may be required. The Government acknowledges that consultation will be required with regular users in order to implement this recommendation with minimal impact. Implementation Approach The Department of Human Services has commenced work to implement this recommendation, with changes to be implemented in the second half of 2018. As part of the implementation process, the Department will engage with the small number of healthcare providers that are regular users of batch requests (generally large hospitals and centralised administrative centres) to ensure that they are aware of the new limits and have an opportunity to implement changes to their administrative practices. The Department will introduce a new process for healthcare providers to apply for a higher limit, and prepare guidance on what would constitute acceptable justification. The Department will also develop policies that identify circumstances in which the Government or the Chief Executive Medicare may allow a higher limit on their own motion, such as in the case of an emergency or natural disaster. The Department will communicate the changes to health professionals through its usual information channels.

Recommendation	Government response
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.	**Agreed.** Statement As noted by the Review Panel, the Department of Human Services has already commenced transitioning HPOS authentication from PKI to PRODA, and in response to this recommendation will accelerate this process. Implementation Approach The transition will be implemented in stages. The Department has already ceased issuing PKI individual certificates where PRODA provides the required functionality, and is actively encouraging health professionals to revoke their PKI certificate once they have established a PRODA account. Stages of the transition will include: - Revoking existing PKI certificates for deregistered health professionals, for health professionals with duplicate certificates and for health professionals who hold a PRODA account - Ceasing renewals for PKI individual certificates - Eventual revocation of all existing PKI individual certificates - Eventual revocation of all existing PKI site certificates. There will be communication and engagement with stakeholders throughout the planning and implementation of the transition process. The Department aims to transition 85 per cent of all PKI individual certificates within 18 months. The Department will transition the remaining PKI individual certificates and all PKI site certificates by December 2020.

Recommendation	Government response
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.	**Agreed.** Statement The Government supports the Panel's recommendation that inactive HPOS accounts should be suspended in order to minimise risk of inappropriate use. The Government also notes the feedback in relation to this recommendation highlighted in the Final Report and will work with peak bodies to ensure the notification period is sufficient. Implementation Approach The Department of Human Services has commenced work to implement this recommendation, with changes to be implemented in the second half of 2018. The Department will communicate the changes to health professionals before and after the change through its usual information channels.
11. It is recommended that the process of opening and reactivating a HPOS account should be administratively straightforward.	**Agreed.** Statement The Government notes the emphasis provided by peak bodies that recommendation 10 must not increase administrative burden on health professionals. The Department of Human Services' process for opening or reactivating accounts will be streamlined to ensure no further documentation is required by health professionals who have already been authenticated. Implementation Approach The Department of Human Services will review its current process before working with health professional groups to ensure the process is administratively straightforward. This recommendation will be implemented in conjunction with recommendation 10.

Recommendation	Government response
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.	**Agreed.** Statement The Government recognises it is important for health professionals to fully understand and appreciate the Terms and Conditions for HPOS, PKI and PRODA in order to be aware of their obligations and responsibilities when interacting with the Department of Human Services and Medicare information. Implementation Approach Work has commenced to implement this recommendation. Updated Terms and Conditions will be published and promoted to health professionals in the first half of 2018.
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.	**Agreed in principle.** Statement The Government agrees with the intent of this recommendation, that HPOS should be the primary channel for health professionals accessing or confirming their patients' Medicare card numbers. Further work with the health sector will be required before implementing changes to the telephone channels. Implementation Approach The Department of Human Services already engages with health professional groups to identify current barriers for HPOS access and develop solutions to address these. These activities will be increased, and the Department of Human Services will continue to take a user-centred approach to resolving barriers to using HPOS and encouraging use of the digital channel, including user research. The Department will undertake data collection about usage of its telephone channels, and consult with health professional groups to identify the circumstances in which access to the telephone channels is required. Based on the results of this research and consultation, the Department will develop a strategy to minimise usage of the telephone channel without disadvantaging particular practices or vulnerable groups. This strategy would be implemented by the middle of 2018 with the aim of phasing out the telephone channel by mid-2019 in line with the recommendation.

Recommendation	Government response
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.	**Agreed.** Statement The Government agrees with the Panel's view that the telephone line should not be closed immediately and recognises the importance of the telephone line in enabling health professionals to confirm Medicare eligibility where internet access is unavailable. Implementation Approach Work has commenced to implement this recommendation. Internal processes will be updated to incorporate new security questions. These changes will be implemented in the first quarter of 2018. The Government will provide early notification to health professionals about the changes through its usual information channels.

My Health Record

What is My Health Record?

My Health Record is a secure online summary of an individual's health information. An individual can control what goes into it, and who is allowed access. Individuals can choose to share their health information with their doctors, hospitals and other healthcare providers.

Why is there a need for a digital record system?

One in three general practitioners (GPs) will see a patient for whom they have little or no health information. Many patient records are created as paper files. They are regularly transmitted between healthcare providers using unsecure email, fax machines and by post. The My Health Record offers health professionals secure digital access to a patient's record at the point of care, wherever that may be.

There are significant benefits of My Health Record for all Australians. These include avoided hospital admissions, fewer adverse drug events, reduced duplication in diagnostic tests, better coordination of care for people seeing multiple healthcare providers, and better informed treatment decisions.

The health sector supports My Health Record

The Australian Medical Association's policy position for maximising My Health Record, states:

> *We all want the My Health Record to work. It has the potential to support much better patient care, particularly when your patients see another doctor or healthcare provider.*

The Royal Australian College of General Practitioners (RACGP) includes helpful case studies on their website on the benefits of My Health Record for GPs:

> *The RACGP has been an advocate for a national shared electronic health record system and understands the clinical benefits of healthcare providers accessing healthcare information not available via normal communications channels.*

The Pharmacy Guild of Australia supports the My Health Record in community Pharmacy:

> *Community pharmacy, as the most accessible community health care destination, has always been at the forefront of digital innovation and an opt-out model for the operation of My Health Record will enable community pharmacies to enhance their patient care.*

Bringing forward the benefits of My Health Record – transition to opt out in 2018

In April 2017, all State and Territory governments agreed the benefits of My Health Record should be made available to all Australians, and the fastest way to achieve these benefits was to transition to an 'opt out' model. In the 2017 Budget, the Federal Government announced a commitment of $374.2 million over two years to the My Health Record to continue and expand the system, including that a My Health Record would be created for every Australian by the end of 2018, unless they choose not to have one and 'opt out'.

Of the total funding to continue and expand My Health Record over the two years, $181.53 million is allocated to the expansion program, including:

- $27.75 million for comprehensive communication and engagement activities with both consumers and healthcare providers.
- $52.38 million to raise awareness, educate and train healthcare providers and jurisdictions to use My Health Record.

The Australian Digital Health Agency (the Agency) is implementing a comprehensive communication strategy to inform the Australian public and healthcare providers about My Health Record, including how they can exercise their choice not to have a record created for them in 2018. The strategy has been developed in partnership with a range of stakeholders including consumer and healthcare peak organisations, Primary Health Networks, states and jurisdictions, healthcare providers and other Government agencies.

Communication activities over the 'opt out' period will include thousands of face-to-face briefings at community events around the country, distribution of collateral through consumer peak organisations and the provision of information at the point of care and other community places (such as doctors' surgeries, hospitals and libraries).

In the lead-up to the transition to opt out, the Agency is building its library of resources to ensure consumers and healthcare providers understand the security features and privacy settings available within My Health Record. Work is already underway with a range of healthcare provider peak organisations to raise awareness of My Health Record and educate their members on its operation.

How does My Health Record system protect people's health information?

My Health Record legislation provides protections for privacy of medical information in the system. The Agency, as the System Operator, is responsible for the security of the My Health Record system.

The Agency has in place a comprehensive set of people, process, and technology controls to protect health records from a cyber-attack. The system has strong security which ensures information is stored and accessed by only trusted connected health systems.

The system complies with the Australian Government requirements for storing and processing protected information, and is regularly tested and audited to confirm that these requirements are met.

The Agency's Cyber Security Centre continually monitors the system for evidence of unauthorised access. This includes utilising specialist security real-time monitoring tools that are configured and tuned to automatically detect events of interest or notable events. Examples of this include:

- Overseas access by consumers and healthcare providers
- Multiple failed logins from the same computer
- Multiple logins within a short period of time
- Logins to the same record from multiple computers at the same time
- High transaction rate for a given Healthcare Provider
- Certain instances of after business hours access and all instances of emergency access.

The Cyber Security Centre regularly reviews the events of interest based on its knowledge of the likely threats to the My Health Record and updates them accordingly.

How do healthcare providers protect your health information?

Every time a healthcare provider accesses a My Health Record, a log is automatically created. This allows an individual to monitor every access to their My Health Record in real time, with complete transparency.

An individual's Medicare card number does not allow My Health Record information to be accessed; additional information is required to authenticate consumers and healthcare providers.

Healthcare organisations can only access an individual's My Health Record if they:

1. are directly involved in the individual's care;
2. have a healthcare provider certificate installed (either with NASH HPI-I or HPI-O certificate[1]) on the device that they are using to access the record;
3. a valid username and password; and
4. have the Record Access Code, if an individual has enabled restrictions.

Any software that connects to the system undergoes automated checks to ensure that it conforms to the system requirements and has authority to access the information. The ability to update a patient's My Health Record is only available to healthcare provider organisations via approved clinical software.

If a person were to deliberately access an individual's My Health Record without authorisation, criminal penalties may apply. These may include up to two years in jail and up to $126,000 in fines.

What controls do individuals have?

A person can arrange to be notified by email or SMS when a healthcare provider organisation accesses their record for the first time. The individual can also view a real time log of every access to their My Health Record by a provider organisation.

Individuals can control what information is in their My Health Record, and which healthcare provider organisations can access their record.

A range of privacy controls are available including:

- Setting a Record Access Code which the individual can give to their healthcare provider organisation to allow access to their record, and prevent other healthcare providers from access unless in an emergency
- Flagging specific documents in their record as 'limited access', and controlling who can view
- Removing documents from view within their record
- Asking healthcare providers not to upload information (under the *My Health Records Act 2012*, healthcare providers must comply with this request).

About the Australian Digital Health Agency

The Australian Digital Health Agency is the system operator of the My Health Record. The Agency provides the leadership, coordination and delivery of a collaborative and innovative approach to utilising technology to support and enhance a clinically safe and connected national health system. This will give individuals more control of their health and their health information, and support healthcare professionals to provide informed healthcare through access to current clinical and treatment information.

[1] National Authentication Service for Health Healthcare Provider Identifier – Individual or Organisation certificate