Department of Human Services

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

Privacy Impact Assessment

September 2018

HWL EBSWORTH
LAWYERS

Table of Contents

Executive Summary

1. Project Overview

1.1 On 10 July 2017, the Australian Government announced the Independent Review of Health Providers' Access to Medicare Card Numbers (**Review**), to examine access by health professionals to Medicare card numbers by using the Health Professional Online Services (**HPOS**) system or by calling the Medicare provider enquiries line. The Review was intended to provide the Government with an independent, external perspective on current vulnerabilities in the system, and how these could be addressed so that Medicare card information is better protected. The Review was not intended to investigate the specific details of the Dark Web incident.

1.2 Professor Peter Shergold AC led the Review. Dr Kean-Seng Lim (representing Dr Michael Gannon, President of the Australian Medical Association (**AMA**)) and Dr Bastian Seidel, President of the Royal Australian College of General Practitioners (**RACGP**), were also members of the review panel (**Review Panel**).

1.3 The Review was intended to consider the balance between appropriate access to a patient's Medicare card number for health professionals to confirm Medicare eligibility, with the security of patients' Medicare card numbers. It was anticipated that the Review:

(a) would make recommendations 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; and

(b) might 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.

1.4 A discussion paper was released on 18 August 2017, inviting stakeholders to respond to a series of consultation questions. Consultation closed on 8 September 2017 and 24 submissions were received. The Review Panel also met with a number of stakeholder organisations.

1.5 This Privacy Impact Assessment (**PIA**) Report:

(a) assesses whether there are any risks to individual privacy presented by the Project;

(b) considers compliance with the *Privacy Act 1988* (**Privacy Act**), including the Australian Privacy Principles (**APP**s);

(c) informs stakeholders about the Project, and illustrates the focus and value being given to privacy risks and risk mitigation; and

(d) considers the safeguards that are or will be in place to secure personal information from misuse, interference or loss, or from unauthorised access, modification or disclosure.

1.6 The Office of the Australian Information Commissioner (**OAIC**) published APP Guidelines on 21 February 2014. The APP Guidelines outline the mandatory requirements of the APPs, how the OAIC will interpret the APPs, and matters that may be taken into account when assessing the department's compliance with the Privacy Act and the APPs. The APP Guidelines are referred to and discussed where appropriate in this PIA Report.

1.7 This PIA Report 'tells the story' of the Project from a privacy perspective. It has been developed in accordance with the OAIC's Privacy Impact Assessment Guide, and will help DHS and other stakeholders to manage any privacy impacts arising from the Project.

2. Summary of Findings

2.1 HWL Ebsworth has identified certain privacy risks related to the Project, and believes that these risks may be further mitigated by implementing the PIA recommendations set out in paragraph 3 below. HWL Ebsworth has not identified any breaches of the APPs requiring urgent attention. Each of the PIA recommendations below is capable of being addressed prior to the commencement of the Project.

2.2 HWL Ebsworth has relied on DHS for the description of the Project and has drafted the PIA Report on the assumption that the description of the Project accurately reflects the proposed handling of personal information.

3. PIA Recommendations

3.1 This PIA Report makes the following recommendations:

Recommendation 1.
The department should consider whether it is feasible for an email or text message to be sent to an individual informing them that their medicare number has been provided to a healthcare provider soon after the medicare number has been provided to a healthcare provider by the department.
Response
The department considered the feasibility of email or text message notifications to individuals and determined that it is not feasible for the following reasons: 1. No formal consent model is in place to allow individuals to opt in or opt out of an SMS service. 2. Individual contact information may not be available as it is not a mandatory requirement for Medicare enrolments. 3. There is no requirement for email and/or mobile phone contact information for individuals (where provided) to be kept up to date. The currency of information cannot be guaranteed, potentially resulting in privacy breaches. 4. The department has an existing process in place if customers require this information. The existing process allows consumers to request their information held by the department, including patient verification searches. This process has now been simplified to allow consumers to specifically request information on HPOS patient verification searches (Review recommendation 5). Information about the simplified service has been published on the department's website. 5. Sending a notification to an individual via email or text would incur significant ICT costs. The Medicare Provider enquiry line does not currently record or store calls including Patient verification requests this functionality, in addition to a notification facility would need to be built. 6. The security for patient verification requests via the telephony channel has been strengthened to reduce the risk of illegitimate access (Review recommendation 14) and the channel will be phased

Recommendation 1.
down by June 2019 (Review recommendation 13). 7. To date the demand for this information has been minimal and does not justify departmental investment in a notification service. 8. In conclusion demand for this to date has been low, which means there is insufficient evidence to justify the investment required to support this recommendation.

Recommendation 2.
The department should review any privacy or security notice that is on the 'Find a Patient' portal to determine whether it provides sufficient warnings to the healthcare providers to ensure that they acknowledge and comply with their privacy and security obligations. If there is no such notice at present, the department should consider inserting that type of notice.
Response
The department has undertaken a review of the HPOS Terms and Conditions under Review recommendation 12 and they were updated accordingly to strengthen the privacy and security responsibilities for a HPOS user. While there is no specific HPOS privacy or security notice, the user requirements for utilising all services and functions in HPOS is clearly stipulated in the HPOS Terms and Conditions, which a user must accept prior to obtaining access to the HPOS system. In relation to the Find a Patient service, we believe that the following additional notices and updates ensures that users are informed and acknowledge their privacy and security obligations when using the service: 1. On 23rd June 2018, a new notice was added to the HPOS Find a Patient service portal on the screen confirming the requirements for users to have consent of their patients before using the service (Recommendation 4). 2. From September, the Find a Patient service will also have new declaration message and check box specifically requesting the user to confirm they have the patient consent prior to performing the search (Recommendation 4). 3. The recently updated HPOS Terms and Conditions also clearly stipulates that HPOS is only be to access information after obtaining consent and for claiming purposes. Additionally a specific clause has now been included to reiterate the consent requirement for the Find a Patient Service (Recommendation 12). As part of normal business practice, privacy and security issues are regularly reviewed and addressed on an ongoing basis, with business processes and systems updated where required.

4. Glossary

Acronyms	
AAT	Administrative Appeals Tribunal
APP	Australian Privacy Principle
DHS	Department of Human Services
HPOS	Health Professional Online Services
OAIC	Office of the Australian Information Commissioner
PIA	Privacy Impact Assessment
PSPF	Australian Government Protective Security Policy Framework

Definitions	
APP Guidelines	The APP Guidelines published by the OAIC on 21 February 2014 at http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/.
personal information	Has the meaning given to it by section 6 of the Privacy Act.
Privacy Act	The *Privacy Act 1988*.
Privacy Impact Assessment Guide	The OAIC's Privacy Impact Assessment Guide, available at https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.pdf
sensitive information	means: (a) information or an opinion about an individual's: (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record; that is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.

5. Background

5.1 On 4 July 2017, media outlets reported that a vendor was illegally selling Medicare card numbers on the 'Dark Web'. 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 reported to the Australian Federal Police, which commenced an investigation.

5.2 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 is therefore susceptible to theft for identity fraud and other illicit activities. Illegally obtained Medicare card numbers could also potentially be used for fraudulent Medicare claiming or enable ineligible individuals to access Medicare related health services.

5.3 On 10 July 2017, the Australian Government announced the Independent Review of Health Providers' Access to Medicare Card Numbers (**Review**), to examine access by health professionals to Medicare card numbers by using the Health Professional Online Services (**HPOS**) system or by calling the Medicare provider enquiries line. The Review was intended to provide the Government with an independent, external perspective on current vulnerabilities in the system, and how these could be addressed so that Medicare card information is better protected. The Review was not intended to investigate the specific details of the Dark Web incident.

5.4 Professor Peter Shergold AC led the Review. Dr Kean-Seng Lim (representing Dr Michael Gannon, President of the Australian Medical Association (**AMA**)) and Dr Bastian Seidel, President of the Royal Australian College of General Practitioners (**RACGP**), were also members of the review panel (**Review Panel**).

5.5 The Review was intended to consider the balance between appropriate access to a patient's Medicare card number for health professionals to confirm Medicare eligibility, with the security of patients' Medicare card numbers. It was anticipated that the Review:

(a) would make recommendations 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; and

(b) might 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.

5.6 A discussion paper was released on 18 August 2017, inviting stakeholders to respond to a series of consultation questions. Consultation closed on 8 September 2017 and 24 submissions were received. The Review Panel also met with a number of stakeholder organisations.

6. Existing mechanisms for health professionals to access Medicare card numbers

6.1 Health professionals can use existing channels to find a patient's Medicare card number when the patient is unable to present their card, including the Health Professional Online Services

(**HPOS**), the Medicare provider enquiries telephone line, and practice software. Health professionals can confirm that Medicare card details are correct through other online claiming channels operated by the Department of Human Services (**department**), but are unable to search for Medicare card details through these channels.

6.2 Administrative staff are more likely than the actual health care providers to seek Medicare card numbers for patients, as they do more of the administrative tasks within a practice such as claiming and maintaining patient details.

HPOS

6.3 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 to telephone channels for a health professional to verify a patient's eligibility for Medicare benefits.

6.4 HPOS offers health providers a single secure web portal giving real-time access to a number of online services provided by the department, including looking up or verifying a patient's Medicare number. The 'Find a Patient' functionality within HPOS allows a health professional to search and confirm a patient's Medicare card number, concessional eligibility and patient details. The health professional is required to enter the patient's first name, surname and date of birth to conduct a search. If more than one person matches the information entered, the individual's postcode and/or suburb/locality must be entered to further refine the search. Information will only be displayed if a unique match is found. Once found, the screen will return the correct Medicare card number, Individual Reference Number (**IRN**), first name and card expiry date.

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

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

6.7 Although there are audit logs of access to Medicare card numbers through HPOS, individual Medicare card holders do not have immediate access to these logs. Individual Medicare card holders could obtain that information through personal information release or FOI processes. However, while an individual Medicare card holder cannot immediately view who has accessed their Medicare card details, individuals can review their claiming history (available through Medicare online accounts) to see which health professionals have lodged claims on their behalf. If individuals identify discrepancies (for example, a claim for a service that they have not received), these can be reported to the department (for suspected customer fraud) or the Department of Health (for suspected provider fraud) for further investigation online or by telephone.

Medicare Provider Enquiries Line

6.8 To obtain a Medicare card number using the Medicare provider enquiries line, the caller must pass a security check confirming the provider details. s37(2)(b), s47E(d)

6.9 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 by the department to the caller:

(a) Medicare card number and IRN;

(b) Medicare card expiry date;

(c) confirmation that the patient is either eligible or not eligible for Medicare on the date of service; and

(d) any restrictions in relation to Medicare services available to the patient.

6.10 s47E(d)

PBS General Enquiries Line

6.11 Medicare card numbers can also be requested through the PBS general enquiries line. s37(2)(b), s47E(d)

Practice Management Software

6.12 Practice management software is not linked to HPOS. A practice may use its PKI site certificate to access HPOS and when the practice is accessing HPOS, there are no links to the practice management software.

Access by individuals to their Medicare card number

6.13 Alternatively, there are mechanisms by which individuals can access their own Medicare card details if they do not have their Medicare card with them. This includes through the Express Plus Medicare mobile app, where an image of the Medicare card can be viewed in the 'Digital

Wallet' section. Individuals can also attend a department service centre and request a temporary paper copy of their card. Individuals can also call the Medicare general enquiries line and request their Medicare card number but they must first pass a security check before that information is released.

7. Shergold Review

7.1 The Review Panel considered the submissions received in response to the discussion paper and released a report on 29 September 2017. The Review made 14 recommendations. In the Australian Government Response to the Independent Review of Health Providers' Access to Medicare Card Numbers (**Government Response**), released on 16 February 2018, the Government agreed to implement 13 of those recommendations without qualification, and confirmed its in-principle agreement to Recommendation 13 pending further consideration of implementation options. Implementation of Recommendation 1 requires no changes to existing processes. The scope of this PIA is limited to the implementation of Recommendations 4-14 inclusive.[1]

7.2 The Review acknowledged that 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. The review determined that health professionals should continue to be able to access Medicare card numbers for patients who are unable to present their Medicare card, so that they can access subsidised treatment. This was considered to be particularly important for vulnerable groups in the community.

Review Panel - Recommendation 4

7.3 The Review Panel noted that 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 Medicare provider enquiries line. This is inconsistent with the procedures adopted for the PBS general enquiries line, which require callers to confirm that they have obtained the patient's consent to request and store their Medicare card details. The Review Panel found that requiring health professionals to obtain consent before seeking their patients' Medicare card numbers from the department will provide patients with more control over their Medicare information and ensure that they know when that information is given to others.

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

7.5 The Review Panel envisaged that it would 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. 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 believed that this could be incorporated into existing processes to inform patients about the handling of their personal information.

7.6 The Review Panel considered that to reflect the requirement for consent, the department would need to update its processes for the Medicare provider enquiry line to include a question about whether the caller has obtained the patient's consent. The declaration to

[1] See further [7.18] below.

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. This consideration of the Committee is not being progressed as the Department is initiating a strategy to replace phone patient verification with an alternate solution such as IVR messaging.

7.7 The department will implement changes to give effect to Recommendation 4 in the first half of 2018. The department intends to implement the measures specifically discussed by the Review Panel, namely by updating its ICT systems for the HPOS Find a Patient service to introduce a new 'check box' confirming that the provider has obtained the patient's consent for the search.

Review Panel - Recommendation 5

7.8 The Review Panel observed that there are audit logs of access to Medicare card numbers maintained through HPOS, but these logs are not available to individual Medicare card holders.

7.9 Individuals are currently able to access their Medicare claiming history for the past three years through their Medicare online account (through myGov) or the Express Plus Medicare mobile app, and can request details of earlier claims from the department 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 to the department, as this is a valuable source of information when identifying fraudulent activity.

7.10 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 service centre.

7.11 However, there is no equivalent means of access to information about which health professionals or organisations have searched for a patient's Medicare card details. The review panel found that 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. Patients can access those records through existing personal information release or FOI. The Department is considering how to facilitate an access request through the development of a special purpose form.

7.12 Recommendation 5 is 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.

7.13 s47E(d)

7.14 The department will implement Recommendation 5 by updating its existing 'Personal Information' webpage to include information about how an individual can obtain an audit log of requests for access to their Medicare card details. The audit logs will be available for the period commencing in 2009, when HPOS was introduced. The department will also update its

internal processes to develop a work flow procedure which will enable these requests to be fulfilled. It is anticipated that the department will verify the identity of the person requesting the log (to ensure that the log is being provided to the individual to whom it relates), before running an audit log report and providing it to the individual.

7.15 The department will provide training to its 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.

Review Panel - Recommendation 6

7.16 Recommendation 6 is that the department undertake a Privacy Impact Assessment (**PIA**) when implementing the Review recommendations, identifying the impact of changes on the privacy of individuals.

7.17 Recommendation 6 responds to the submission of the Office of the Australian Information Commissioner to the Review, which recommended that the department conduct a PIA to assist it in the implementation of the review recommendations. The OAIC submitted that 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.

7.18 Consistent with its existing Project Management Framework and Standards, the department agreed to undertake appropriate privacy assessments as part of the implementation process for any recommendation involving the handling of personal information. The department determined that those recommendations are Recommendations 4-14 inclusive, and has commissioned this PIA to implement Recommendation 6.

Review Panel - Recommendation 7

7.19 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 Provider Digital Access (**PRODA**), outlined further below) before they can be nominated as a delegate in HPOS. The Review Panel considered that there are nonetheless risks inherent with the current delegation model. Most importantly, delegation arrangements do not expire, meaning that a delegate could continue to perform functions in HPOS even if they had left the practice. The Review found that the risk of delegations 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 delegations and remove any that are no longer required.

7.20 Recommendation 7 is 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.

7.21 The department has commenced work on implementing Recommendation 7, which is expected to be introduced in the second half of 2018. The department will introduce a change to its ICT systems which will involve a pop-up prompt to health providers advising them that one or more of their delegations will soon expire, and asking them to confirm whether the delegation is still required. If they answer 'yes', the delegation will be renewed. If not, the delegation will expire.

Recommendation 8

7.22 The Review found that while the availability of batch 'Find a Patient' requests through HPOS should be retained, the current limit of 500 records per batch is unwarranted in most cases. The Review acknowledged 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.

7.23 Recommendation 8 is 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 for a higher limit, demonstrating a clear business need.

7.24 The department has commenced work to implement Recommendation 8, with changes to be implemented in the second half of 2018.

7.25 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 limit and have an opportunity to implement changes to their administrative practices.

7.26 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 for the purposes of demonstrating a business need. The department anticipates that when approval is granted for a higher limit in a particular case, it will be subject to monitoring by the department. 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.

7.27 The department will communicate the changes to health professionals through its usual information channels.

Recommendation 9

7.28 To access HPOS, health professionals must 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 acceptable evidence of identity in that application process.

7.29 Access to HPOS occurs via one of the following means:

(a) for PRODA users – entry of user name, password and second factor authentication code;

(b) 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**); or

(c) for PKI site certificate users – log on to a computer with the correct software and site certificate installed and entry of PIC.

7.30 The Review found that PRODA provides a greater level of security than the use of PKI certificates, due to the requirement that each individual have their own PRODA account and the strength of the two-step verification process for authentication purposes. The Review Panel considered that the department should accelerate its current move away from PKI certificates to PRODA.

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

7.32 The department is already in the process of transitioning away from PKI certificates. This 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.

7.33 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; and
- eventual revocation of all existing PKI site certificates.

7.34 The department will communicate and engage with stakeholders throughout the planning and implementation of the transition process.

7.35 The department aims to transition 85 per cent of all PKI individual certificates to PRODA within 18 months. The department will transition the remaining PKI individual certificates and all PKI site certificates by December 2020.

Recommendations 10 and 11

7.36 The Review Panel observed that PRODA accounts do not expire, even when they are no longer active. PKI certificates issued by the department 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 that access is no longer required. The Review Panel found that suspending or cancelling HPOS accounts if they have not been used for a certain period would reduce the risk that these accounts could be used inappropriately.

7.37 Recommendation 10 is 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.

7.38 The department has commenced ICT work to give effect to Recommendation 10, with changes to be implemented in the second half of 2018. The department will communicate the changes to health professionals before and after implementation through its usual information channels.

7.39 Recommendation 11 is that the process of opening and reactivating a suspended HPOS account should be administratively straightforward.

7.40 The department will review its current process before working with health professional groups to ensure the process of reactivating a suspended HPOS account is administratively straightforward. Recommendation 11 will be implemented in conjunction with Recommendation 10.

Recommendation 12

7.41 The Review Panel noted that there are separate Terms and Conditions of use for HPOS itself and for each of the underlying authentication mechanisms, PKI certificates and PRODA. The Review Panel was concerned that the Terms and Conditions are not always understood and complied with.

7.42 The Panel found that not all users or organisations have a clear understanding of the security requirements surrounding PKI certificates, PRODA or HPOS as outlined in the various Terms and Conditions, or the obligations these conditions place on them as a user of these systems. The panel considered that 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.

7.43 Recommendation 12 is 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.

7.44 The department has commenced work to implement this recommendation. Updated Terms and Conditions are expected to be published and promoted to health professionals in the first half of 2018.

Recommendation 13

7.45 The Review Panel identified a number of changes that could be made to improve the security of HPOS. Overall, however, it was clear to the Review Panel that HPOS provides significantly greater security than the department's telephone channels. The Review Panel found that the authentication and verification processes 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 when compared with telephone requests.

7.46 While improvements could be made to the department's telephone channels, the Review Panel's view was that HPOS should be the default channel through which health professionals seek Medicare card numbers. However, the Review Panel recognised that there will continue to be circumstances in which access to the telephone channels is required, including when the HPOS Find a Patient service is not available or does not return a result, or where internet access is not available to the health professional. Accordingly, the Review Panel did not propose that telephone channels be closed down.

7.47 Recommendation 13 is that, in order to provide greater security and availability, the department 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.

7.48 In response to Recommendation 13, it was noted that the department 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 will continue to take

a user-centred approach to resolving barriers to using HPOS and encouraging use of the digital channel, including user research.

7.49 The department will undertake data collection to analyse the usage of its telephone channels, and consult with health professional groups to identify the circumstances in which access to the telephone channels is required.

7.50 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 Recommendation 13.

Recommendation 14

7.51 The Review Panel noted that telephone access requests represented a smaller proportion of overall requests for access to Medicare card details when compared with the number of requests made via HPOS. Nonetheless, the Review Panel considered that the current security check for release of Medicare card information using the Medicare provider enquiries line provides a much lower level of confidence than the security requirements for the HPOS channel.

7.52 The Panel observed that the information that a caller must provide in order to pass the security check to access a Medicare card number using a telephone channel could be accessible by someone other than the provider. This information could potentially be obtained through a combination of sources.

7.53 Recommendation 14 is 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.

7.54 The Panel commented that one option that it would support is the introduction of additional security questions based on information already held in the department's systems but which is not publicly available. This option would provide an added level of security but would not be onerous for health professionals.

7.55 The department has commenced work to implement Recommendation 14. 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.

8. Community expectations and attitudes to privacy

8.1 One of the matters which must be taken into account when conducting a PIA is how consistent the project is with community values about privacy. To assess this question, APP entities can conduct consultations, review community responses to similar projects, or consider research into community attitudes about privacy.

8.2 The OAIC commissioned the Australian Community Attitudes to Privacy Survey 2017, which can assist in understanding contemporary community expectations regarding the management of personal information. The following findings are of relevance to this Project:

(a) Australians believe that the biggest privacy risks facing the community are online services, including social media sites (32%), ID fraud and theft (19%), data security breaches (17%) and risks to financial data (12%);

(b) more than eight in ten respondents (83%) believe the privacy risks are greater when dealing with an organisation online compared with other means;

(c) the four pieces of information Australians are most reluctant to provide are financial details (42%), address (24%), date of birth (14%) and phone numbers (13%). These figures are similar to those obtained when the OAIC last conducted the survey in 2013;

(d) when the community was asked how trustworthy they considered different types of organisation to be, the highest levels of trust were recorded for health service providers (79%), financial institutions (59%) and state and federal government departments (58%);

(e) while nearly half of Australians (46%) are comfortable with government agencies using their personal details for research or policy-making purposes, four in ten are not comfortable (40%), and the balance are still unsure;

(f) one-third (34%) of the community is comfortable with the government sharing their personal information with other government agencies;

(g) 86% of respondents considered that the use of their personal information for a purpose other than the one it was provided for amounts to misuse of that information; and

(h) only 16% would avoid dealing with a government agency because of privacy concerns, compared with 58% who would avoid dealing with a private company.

8.3 These findings are considered where relevant below.

Analysis

9. Assessment of privacy impacts

9.1 The OAIC recommends that APP entities identify and critically analyse how a project impacts upon privacy, both positively and negatively. This analysis is not confined to an assessment of compliance with the APPs, which is set out below. Rather, this analysis should be broader and identify the answers to a range of key questions.

9.2 The Project is to implement a range of measures designed and intended to reduce privacy and security risks. The very nature of this Project is privacy positive.

10. Assessment of compliance with the APPs

10.1 Planning a PIA involves determining how detailed the PIA needs to be, based on a broad assessment of the project and its privacy scope.

10.2 This Project is not expected to introduce the collection of significantly different or changed categories of personal information, or to permit significantly different uses or disclosures of personal information when compared with the current framework.

10.3 The core functions of the health professionals and health practices will remain largely consistent.

10.4 For these reasons, this PIA does not assess compliance of the Project with every individual APP. Rather, this PIA is focused on those APPs of most relevance in the context of this Project. The full text of the APPs is set out at Schedule 2.

APP 1 — Open and transparent management of personal information

10.5 The obligations imposed on APP entities under APP 1 may be grouped as follows:

(a) the obligation to take reasonable steps to implement practices, procedures and systems to comply with the APPs, and to enable the entity to deal with inquiries or complaints from individuals about its compliance with the APPs (**APP 1.2**);

(b) the obligation to have a clearly expressed and up-to-date policy about the management of personal information by the entity (**APP 1.3 and 1.4**); and

(c) the obligation to take reasonable steps to make the entity's privacy policy available free of charge, and in such form as is appropriate (**APP 1.5 and 1.6**).

10.6 APP 1.2 is a general and constant obligation and applies to the functions and activities of the department as a whole. It is beyond the scope of this PIA to assess the department's compliance with APP 1.2 in respect of all of its many functions and activities. Accordingly, this PIA Report is limited in its consideration of APP 1.2 to whether, in the context of the Project, the requirements of that APP have been complied with.

10.7 The commissioning of this PIA by the department is a reasonable step to ensure compliance with the APPs (as well as one of the recommendations of the Review Panel). The department will continue to apply its pre-existing privacy processes and policies to the management of its compliance with the APPs in relation to the Project. The information security measures to be

taken in respect of the Project (discussed in relation to APP 11 below) are also relevant to compliance with APP 1.2.

10.8 Whenever personal information is collected for a particular purpose, there is a risk of function creep. The Project is not expected to introduce any significantly different collections, uses or disclosures of personal information from those in place under the current arrangements. Accordingly, we consider the risk of function creep to be low. In fact, the measures that are proposed to be implemented in department's response to the recommendations of the Review Panel are privacy enhancing and will result in greater control and security arrangements in relation to a patient's personal information with less opportunity for future function creep.

10.9 The implementation of the department's response to the recommendations of the Review Panel will also offer an opportunity to provide staff with refresher training on privacy compliance and to reinforce the importance of privacy compliance among those staff with a supervisory role, to ensure that they can assist their team members to comply with their obligations. To the extent possible, privacy compliance training should be tailored to the role and seniority of the attendees and use practical examples which are relevant to those roles.

Analysis of the department's compliance with APP 1.3, 1.4 and 1.5

10.10 As is the case with APP 1.2, the obligation in APP 1.3 to have a clearly expressed and up-to-date policy about the management of personal information is one of general application, and arises at a departmental level. Accordingly, the assessment of whether the department's privacy policy complies with the APPs would ordinarily be beyond the scope of this PIA. However, it is noted that to comply with APP 1.3 and 1.5, the department has adopted a Privacy Policy, which is available free of charge from its website. The department's Privacy Policy is clearly expressed, and was last revised on 30 October 2017, suggesting that it is up-to-date.

10.11 APP 1.4(a), (b) and (c) are of most relevance to this Project. Compliance with APP 1.4(a) only requires an APP entity to describe the kinds of personal information it collects and holds in 'general terms'.[2] (The privacy policy is to be distinguished from a privacy notice provided under APP 5, which provides more specific information about a particular collection of personal information.) This PIA Report finds that the department's general Privacy Policy does describe the kinds of personal information which may be collected and held about its customers, in terms which are sufficient to meet that obligation in the context of this Project. This is because it lists the kinds of personal information the department collects from a healthcare provider, including name, address and date of birth. These items of information are necessary to the matching of a person to their Medicare records.

10.12 The DHS Privacy Policy provides adequate information about why the department will collect, use and disclose personal information for the purpose of checking a person's Medicare card details and providing those to a third party healthcare provider and how that information will be stored, in order to comply with APP 1.4(c). For example, the Privacy Policy states that:

> We may collect your personal information when it is reasonably necessary for delivering payments or services. For example, we may collect your personal information to:
>
> - confirm your identity

[2] APP Guidelines, Chapter 1, paragraph 1.17.

- communicate with you, including by SMS or email via our electronic messaging service
- ensure correct payments are made
- verify data provided in relation to claims and reviews with third parties
- investigate fraud, including internal fraud and the assessment of payment eligibility
- manage complaints and feedback
- participate in merits and judicial review matters
- manage and respond to requests for information. …

We take reasonable steps to protect your personal information against misuse, interference and loss, and from unauthorised access, modification or disclosure. These steps include:

- storing paper records securely as per Australian government security guidelines
- only accessing personal information on a need-to-know basis and by authorised personnel
- monitoring system access which can only be accessed by authenticated credentials
- ensuring our buildings are secure, and

Conclusion on compliance with APP 1

10.13 Recommendation 4 - health professionals should be required to seek the consent of their patients before accessing their Medicare card numbers through HPOS or by telephone.

10.14 This step in the process is within the control and responsibility of the healthcare provider. The department will implement a checkbox on the Find a Patient portal where a healthcare provider has to confirm that it has the consent of the patient to provide their personal information to the department and be provided with that person's Medicare number. Healthcare providers.

10.15 The department should review any privacy or security notice that is on the 'Find a Patient' portal to determine whether it provides sufficient warnings to the healthcare providers to ensure that they acknowledge and comply with their privacy and security obligations. If there is no such notice at present, the department should consider inserting that type of notice. (**PIA Recommendation 1**).

10.16 Recommendation 5 - 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.

10.17 The department is taking measures to implement this recommendation. The department is considering how to facilitate an access request through the development of a special purpose

form. Individuals will be informed through the DHS Privacy Policy and access to information page on the department's website.

10.18 MyGov is the easiest way an individual can get details about themselves. However, understandably given the timing, there is no current express reference to how a person may access an audit log regarding the use of their Medicare number.

10.19 The Review was conducted in the context of an investigation into measures that would limit the scope of potential unlawful activities. Individuals may not know whether their Medicare number has been sought and used by a healthcare provider and may not be checking or requesting an audit log as a matter of routine. It would appear to be a sound proactive measure for the department for the department to notify an individual of the use of their Medicare number by a third party and provide them with the opportunity to raise any concerns.

10.20 The department should consider whether it is feasible for an email or text message to be sent to an individual informing them that their medicare number has been provided to a healthcare provider soon after the medicare number has been provided to a healthcare provider by the department (**PIA Recommendation 2**).

10.21 The discussion on APP 1 is not relevant to the following recommendations of the Review.

(a) Recommendation 6 - the department undertake a Privacy Impact Assessment (PIA) when implementing the Review recommendations, identifying the impact of changes on the privacy of individuals.

(b) Recommendation 7 - 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.

(c) Recommendation 8 - batch requests for Medicare card numbers through HPOS should be more tightly controlled.

(d) Recommendation 9 - authentication for HPOS should be moved from PKI to the more secure PRODA expeditiously, with transition completed within three years.

(e) Recommendation 10 - 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.

(f) Recommendation 11 - the process of opening and reactivating a suspended HPOS account should be administratively straightforward.

(g) Recommendation 12 - the Terms and Conditions for HPOS, PKI and PRODA should be simplified and presented to healthcare provider users in a form that ensures that they fully appreciate the seriousness of their obligations.

(h) Recommendation 13 - in order to provide greater security and availability, the department 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.

(i) Recommendation 14 - 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.

10.22 This PIA has found that, subject to implementation of the recommendations set out above, the department will comply with APP 1 in their delivery of the Project.

APP 5 — Notification of the collection of personal information

10.23 APP 5 requires that where an APP entity collects personal information about an individual, the entity takes reasonable steps to notify the individual of certain matters (**APP 5 Matters**) or otherwise, ensures that the individual is aware of those matters. Such a notification must occur at or before the time of the collection, or as soon as practicable afterwards.

10.24 Whether the department has taken reasonable steps is to be determined objectively. The relevant test is whether a reasonable person would agree that in the circumstances, they had acted reasonably in providing notice or ensuring awareness of the APP 5 Matters.

10.25 According to the APP Guidelines, the reasonable steps for an APP entity to take will depend upon circumstances that include:

- the sensitivity of the personal information collected. More rigorous steps may be required when collecting 'sensitive information' or information of a sensitive nature;
- the possible adverse consequences for an individual as a result of the collection. More rigorous steps may be required as the risk of adversity increases;
- any special needs of the individual. More rigorous steps may be required if personal information is collected from an individual from a non-English speaking background who may not readily understand the APP 5 matters;
- the practicability, including time and cost involved. However, an entity is not excused from taking particular steps by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances.[3]

10.26 The key consideration in the context of this Project is that where there will be little change in the way personal information is collected as a result of the implementation of the Review Panel's recommendations. A healthcare provider will be required to represent to the department that they have obtained the consent of the patient and there are limitations on the numbers of medicare numbers that may be made available at any particular time, but the type of personal information and the dealing with that personal information remains the same.

10.27 The department will collect the personal information of patients from the healthcare provider for the purposes of notifying the provider the Medicare number of the patient. The healthcare provider is obliged to have the consent of the patient to approach the department in the first place so it is reasonable for the department to assume that it is collecting the personal information of the patient with that patient's consent and for primary purpose of the department disclosing that patient's Medicare number to the healthcare provider.

10.28 Recommendation 4 - health professionals should be required to seek the consent of their patients before accessing their Medicare card numbers through HPOS or by telephone.

[3] APP Guidelines, Chapter 5, paragraph 5.4.

10.29 This is a responsibility of the health professional or the administrative staff at the healthcare provider. As noted by the Review Panel, that could be undertaken at the time of the patient's initial registration. The healthcare provider will be required to confirm that it has obtained the consent of the person but the collection, and notification to the patient at that time, is the responsibility of the healthcare provider.

10.30 Recommendation 5 of the Review - request the audit log of health professionals who have sought access to their Medicare card number through the HPOS 'Find a Patient' service. This Recommendation has been discussed above under APP 1 and the PIA Recommendation 1 is also applicable to this APP 5.

10.31 The discussion on APP 5 is not relevant to the following recommendations of the Review.

(a) Recommendation 6 - the department undertake a Privacy Impact Assessment (PIA) when implementing the Review recommendations, identifying the impact of changes on the privacy of individuals.

(b) Recommendation 7 - 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.

(c) Recommendation 8 - batch requests for Medicare card numbers through HPOS should be more tightly controlled.

(d) Recommendation 9 - authentication for HPOS should be moved from PKI to the more secure PRODA expeditiously, with transition completed within three years.

(e) Recommendation 10 - 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.

(f) Recommendation 11 - the process of opening and reactivating a suspended HPOS account should be administratively straightforward.

(g) Recommendation 12 - 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.

(h) Recommendation 13 - in order to provide greater security and availability, the department 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.

(i) Recommendation 14 - 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.

10.32 This PIA Report finds that the department will comply with APP 5 in relation to the Project.

APP 6 — Use and disclosure of personal information

10.33 The intent of APP 6 is that an APP entity will generally use and disclose an individual's personal information only in ways the individual would expect or where one of the exceptions

applies. APP 6 provides that an entity that holds personal information about an individual can only use or disclose the information for a particular purpose for which it was collected (known as the 'primary purpose' of collection), unless an exception applies. Where an exception applies the entity may use or disclose personal information for another purpose (known as the 'secondary purpose').

10.34 As noted above under APP 5, the healthcare provider is obliged to have the consent of the patient to approach the department in the first place so it is reasonable for the department to assume that it is collecting the personal information of the patient with that patient's consent and for primary purpose of the department disclosing that patient's Medicare number to the healthcare provider.

10.35 The Review Panel recommended the department will include a tick box on the HPOS 'Find a Patient' service for the healthcare provider to complete to confirm that it has obtained the consent of the patient for the provider to conduct the search. Itf the department has that confirmation then the subsequent steps in disclosing the patient's medicare number to the requesting healthcare provider are consistent with APP6 (and section 130 of the *Health Insurance Act 1973*).

10.36 This PIA concludes that, assuming that the department's response to the Review Panel's recommendations are implemented as planned, the measures discussed above would be characterised as 'reasonable' steps for the purposes of meeting the obligations of DHS under APP 11.

APP 11 — Security of personal information

10.37 APP 11.1 requires that the department takes such steps as are reasonable to protect personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. APP 11.1 is of particular relevance in the context of the Project, which involves the implementation of measures designed to protect personal information from misuse and interference.

10.38 The obligation in APP 11.1 only applies to personal information that an APP entity 'holds'. An entity holds personal information if the entity has possession or control of a record that contains the personal information.[4]

10.39 The term 'reasonable' is not defined in the Privacy Act. The APP Guidelines provide that the term bears its ordinary meaning, as being based upon, or according to, reason and capable of sound explanation. What is reasonable is a question of fact in each individual case. It is an objective test that has regard to how a reasonable person, who is properly informed, would be expected to act in the circumstances. What is reasonable can be influenced by current standards and practices.[5] The reasonable steps that an APP entity should take under APP 11.1 are influenced by the following considerations:

(a) the nature of the APP entity. Relevant considerations include an APP entity's size, resources, the complexity of its operations and its business model;

(b) the amount and sensitivity of the personal information held. Generally, as the amount and/or sensitivity of personal information that is held increases, so too will the steps that it is reasonable to take to protect it;

[4] Privacy Act subsection 6(1).
[5] APP Guidelines, Chapter B, paragraph B.105.

(c) the possible adverse consequences for an individual in the case of a breach. More rigorous steps may be required as the risk of adversity increases;

(d) the practical implications of implementing the security measure, including time and cost involved. However an entity is not excused from taking particular steps to protect information by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances; and

(e) whether a security measure is in itself privacy invasive. For example, while an APP entity should ensure that an individual is authorised to access information, it should not require an individual to supply more information than is necessary to identify themselves when dealing with the entity.

10.40 Departmental officers who administer the MBS are already subject to existing security controls and secrecy provisions of the Health Insurance Act which can be expected to continue to have a deterrence factors and reduce the risk of unauthorised disclosure of personal information.

10.41 The Review Panel recommended the department will include a tick box on the HPOS 'Find a Patient' service for the healthcare provider to complete to confirm that it has obtained the consent of the patient for the provider to conduct the search.

10.42 This PIA concludes that, assuming that the department's response to the Review Panel's recommendations are implemented as planned, the measures discussed above would be characterised as 'reasonable' steps for the purposes of meeting the obligations of DHS under APP 11.

10.43 The PIA recommendations we have recommended would also assist in the security of personal information.

Schedule 1: Text of the Australian Privacy Principles

Australian Privacy Principle 1 — open and transparent management of personal information

1.1 The object of this principle is to ensure that APP entities manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles etc.

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

a. will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and

b. will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

APP Privacy policy

1.3 An APP entity must have a clearly expressed and up to date policy (the ***APP privacy policy***) about the management of personal information by the entity.

1.4 Without limiting subclause 1.3, the APP privacy policy of the APP entity must contain the following information:

a. the kinds of personal information that the entity collects and holds;

b. how the entity collects and holds personal information;

c. the purposes for which the entity collects, holds, uses and discloses personal information;

d. how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;

e. how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

f. whether the entity is likely to disclose personal information to overseas recipients;

g. if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

Availability of APP privacy policy etc.

1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

a. free of charge; and

b. in such form as is appropriate.

Note: An APP entity will usually make its APP privacy policy available on the entity's website.

1.6 If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

Australian Privacy Principle 2 — anonymity and pseudonymity

2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

2.2 Subclause 2.1 does not apply if, in relation to that matter:

a. the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or

b. it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

Australian Privacy Principle 3 — collection of solicited personal information

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

a. the individual consents to the collection of the information and:

i. if the entity is an agency — the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

ii. if the entity is an organisation — the information is reasonably necessary for one or more of the entity's functions or activities; or

b. subclause 3.4 applies in relation to the information.

3.4 This subclause applies in relation to sensitive information about an individual if:

a. the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

b. a permitted general situation exists in relation to the collection of the information by the APP entity; or

c. the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or

d. the APP entity is an enforcement body and the entity reasonably believes that:

i. if the entity is the Immigration Department — the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or

ii. otherwise — the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

e. the APP entity is a non-profit organisation and both of the following apply:

i. the information relates to the activities of the organisation;

ii. the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Note: For permitted general situation, see section 16A. For permitted health situation, see section 16B.

Means of collection

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

a. if the entity is an agency:

i. the individual consents to the collection of the information from someone other than the individual; or

ii. the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

b. it is unreasonable or impracticable to do so.

Solicited personal information

3.7 This principle applies to the collection of personal information that is solicited by an APP entity.

Australian Privacy Principle 4 — dealing with unsolicited personal information

4.1 If:

a. an APP entity receives personal information; and

b. the entity did not solicit the information;

the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

4.2 The APP entity may use or disclose the personal information for the purposes of making the determination under subclause 4.1.

4.3 If:

a. the APP entity determines that the entity could not have collected the personal information; and

b. the information is not contained in a Commonwealth record;

the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

4.4 If subclause 4.3 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.

Australian Privacy Principle 5 — notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

a. to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or

b. to otherwise ensure that the individual is aware of any such matters.

5.2 The matters for the purposes of subclause 5.1 are as follows:

a. the identity and contact details of the APP entity;

b. if:

i. the APP entity collects the personal information from someone other than the individual; or

ii. the individual may not be aware that the APP entity has collected the personal information;

the fact that the entity so collects, or has collected, the information and the circumstances of that collection;

c. if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order — the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);

d. the purposes for which the APP entity collects the personal information;

e. the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;

f. any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;

g. that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;

h. that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

i. whether the APP entity is likely to disclose the personal information to overseas recipients;

j. if the APP entity is likely to disclose the personal information to overseas recipients — the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Australian Privacy Principle 6 — use or disclosure of personal information

Use or disclosure

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:

a. the individual has consented to the use or disclosure of the information; or

b. subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:

a. the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:

i. if the information is sensitive information — directly related to the primary purpose; or

ii. if the information is not sensitive information — related to the primary purpose; or

b. the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

c. a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or

d. the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or

e. the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Note: For permitted general situation, see section 16A. For permitted health situation, see section 16B.

6.3 This subclause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if:

a. the agency is not an enforcement body; and

b. the information is biometric information or biometric templates; and

c. the recipient of the information is an enforcement body; and

d. the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.

6.4 If:

a. the APP entity is an organisation; and

b. subsection 16B(2) applied in relation to the collection of the personal information by the entity;

the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with subclause 6.1 or 6.2.

Written note of use or disclosure

6.5 If an APP entity uses or discloses personal information in accordance with paragraph 6.2(e), the entity must make a written note of the use or disclosure.

Related bodies corporate

6.6 If:

a. an APP entity is a body corporate; and

b. the entity collects personal information from a related body corporate;

this principle applies as if the entity's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Exceptions

6.7 This principle does not apply to the use or disclosure by an organisation of:

a. personal information for the purpose of direct marketing; or

b. government related identifiers.

Australian Privacy Principle 7 — direct marketing

Direct marketing

7.1 If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Exceptions — personal information other than sensitive information

7.2 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

a. the organisation collected the information from the individual; and

b. the individual would reasonably expect the organisation to use or disclose the information for that purpose; and

c. the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

d. the individual has not made such a request to the organisation.

7.3 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

a. the organisation collected the information from:

i. the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or

ii. someone other than the individual; and

b. either:

i. the individual has consented to the use or disclosure of the information for that purpose; or

ii. it is impracticable to obtain that consent; and

c. the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

d. in each direct marketing communication with the individual:

i. the organisation includes a prominent statement that the individual may make such a request; or

ii. the organisation otherwise draws the individual's attention to the fact that the individual may make such a request; and

e. the individual has not made such a request to the organisation.

Exception — sensitive information

7.4 Despite subclause 7.1, an organisation may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

Exception — contracted service providers

7.5 Despite subclause 7.1, an organisation may use or disclose personal information for the purpose of direct marketing if:

a. the organisation is a contracted service provider for a Commonwealth contract; and

b. the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and

c. the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

Individual may request not to receive direct marketing communications etc.

7.6 If an organisation (the first organisation) uses or discloses personal information about an individual:

a. for the purpose of direct marketing by the first organisation; or

b. for the purpose of facilitating direct marketing by other organisations;

the individual may:

c. if paragraph (a) applies — request not to receive direct marketing communications from the first organisation; and

d. if paragraph (b) applies — request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and

e. request the first organisation to provide its source of the information.

7.7 If an individual makes a request under subclause 7.6, the first organisation must not charge the individual for the making of, or to give effect to, the request and:

a. if the request is of a kind referred to in paragraph 7.6(c) or (d) — the first organisation must give effect to the request within a reasonable period after the request is made; and

b. if the request is of a kind referred to in paragraph 7.6(e) — the organisation must, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so.

Interaction with other legislation

7.8 This principle does not apply to the extent that any of the following apply:

a. the *Do Not Call Register Act 2006*;

b. the *Spam Act 2003*;

c. any other Act of the Commonwealth, or a Norfolk Island enactment, prescribed by the regulations.

Australian Privacy Principle 8 — cross-border disclosure of personal information

8.1 Before an APP entity discloses personal information about an individual to a person (the overseas recipient):

a. who is not in Australia or an external Territory; and

b. who is not the entity or the individual;

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

a. the entity reasonably believes that:

i. the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

ii. there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

b. both of the following apply:

i. the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;

ii. after being so informed, the individual consents to the disclosure; or

c. the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

d. a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or

e. the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or

f. the entity is an agency and both of the following apply:

i. the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

ii. the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

Note: For permitted general situation, see section 16A.

Australian Privacy Principle 9 — adoption, use or disclosure of government related identifiers

Adoption of government related identifiers

9.1 An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless:

a. the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or

b. subclause 9.3 applies in relation to the adoption.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Use or disclosure of government related identifiers

9.2 An organisation must not use or disclose a government related identifier of an individual unless:

a. the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions; or

b. the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

c. the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or

d. a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or

e. the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

f. subclause 9.3 applies in relation to the use or disclosure.

Note 1: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Note 2: For permitted general situation, see section 16A.

Regulations about adoption, use or disclosure

9.3 This subclause applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if:

a. the identifier is prescribed by the regulations; and

b. the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and

c. the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

Note: There are prerequisites that must be satisfied before the matters mentioned in this subclause are prescribed, see subsections 100(2) and (3).

Australian Privacy Principle 10 — quality of personal information

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.

10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

Australian Privacy Principle 11 — security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

a. from misuse, interference and loss; and

b. from unauthorised access, modification or disclosure.

11.2 If:

a. an APP entity holds personal information about an individual; and

b. the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and

c. the information is not contained in a Commonwealth record; and

d. the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

Australian Privacy Principle 12 — access to personal information

Access

12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exception to access — agency

12.2 If:

a. the APP entity is an agency; and

b. the entity is required or authorised to refuse to give the individual access to the personal information by or under:

i. the Freedom of Information Act; or

ii. any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;

then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.

Exception to access — organisation

12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:

a. the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

b. giving access would have an unreasonable impact on the privacy of other individuals; or

c. the request for access is frivolous or vexatious; or

d. the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or

e. giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

f. giving access would be unlawful; or

g. denying access is required or authorised by or under an Australian law or a court/tribunal order; or

h. both of the following apply:

i. the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;

ii. giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

i. giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

j. giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

Dealing with requests for access

12.4 The APP entity must:

a. respond to the request for access to the personal information:

i. if the entity is an agency — within 30 days after the request is made; or

ii. if the entity is an organisation — within a reasonable period after the request is made; and

b. give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Other means of access

12.5 If the APP entity refuses:

a. to give access to the personal information because of subclause 12.2 or 12.3; or

b. to give access in the manner requested by the individual;

the entity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual.

12.6 Without limiting subclause 12.5, access may be given through the use of a mutually agreed intermediary.

Access charges

12.7 If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the personal information.

12.8 If:

a. the APP entity is an organisation; and

b. the entity charges the individual for giving access to the personal information;

the charge must not be excessive and must not apply to the making of the request.

Refusal to give access

12.9 If the APP entity refuses to give access to the personal information because of subclause 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:

a. the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

b. the mechanisms available to complain about the refusal; and

c. any other matter prescribed by the regulations.

12.10 If the APP entity refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.

Australian Privacy Principle 13 — correction of personal information

Correction

13.1 If:

a. an APP entity holds personal information about an individual; and

b. either:

i. the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or

ii. the individual requests the entity to correct the information;

the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

Notification of correction to third parties

13.2 If:

a. the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and

b. the individual requests the entity to notify the other APP entity of the correction;

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

Refusal to correct information

13.3 If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out:

a. the reasons for the refusal except to the extent that it would be unreasonable to do so; and

b. the mechanisms available to complain about the refusal; and

c. any other matter prescribed by the regulations.

Request to associate a statement

13.4 If:

a. the APP entity refuses to correct the personal information as requested by the individual; and

b. the individual requests the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;

the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

Dealing with requests

13.5 If a request is made under subclause 13.1 or 13.4, the APP entity:

a. must respond to the request:

i. if the entity is an agency — within 30 days after the request is made; or

ii. if the entity is an organisation — within a reasonable period after the request is made; and

b. must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).