Prepared for Department of Health
30 August 2021

Medical Costs Finder (MCF) Portal

Summary of Supplementary Privacy Impact Assessment

Matter number 21004000

Department of Health – MCF Portal – Supplementary PIA

Executive Summary

This is a summary of a Supplementary Privacy Impact Assessment (**PIA**) commissioned by the Department of Health (**Department**) in relation to the Medical Costs Finder (**MCF**) Portal. It is part of the Out of Pocket Costs Transparency (**OOPT**) Project (**Project**), which seeks to address the lack of transparency in relation to the out of pocket costs of specialist medical services in the private health system.

The MCF Portal is part of the second stage of the Project:

Stage	Description
Stage 1 MCF website	The MCF website uses de-identified and aggregated claims data to show the typical fees and resulting out of pocket costs charged by specialists for treatments funded under the Medical Benefits Scheme (**MBS**).
Stage 2 MCF Portal	Information about the fees for specialist medical services will be collected from providers via an online portal (**MCF Portal**) and then published on the MCF website. Participation in stage 2 of the Project is voluntary and personal information is only published with consent.

The supplementary PIA examines changed practices for the collection, use and disclosure of information via the MCF Portal. AGS previously prepared a PIA in relation to a manual process for gathering information about specialists to publish on the MCF website (**primary PIA**). The personal information flows for the MCF Portal are set out in **Part 1** of this summary.

Purpose of this PIA

Australian Privacy Principle (**APP**) 1.2 in Sch 1 to the *Privacy Act 1988* requires the Department to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs. This includes undertaking a PIA for 'high risk' projects that will have a significant impact on the privacy of individuals: see s 12(1) of the Australian Government Agencies Privacy Code (**Privacy Code**).

This summary has been prepared to provide greater transparency around the OOPT Project and privacy assurances to users as well as the broader Australian community.

Summary of findings

Part 2 summarises how the MCF Portal may impact on the privacy of individuals, including from:

- out-of-date or inaccurate links between specialists and authorised representatives
- collection of unnecessary or inaccurate data
- unauthorised access, use and disclosure of personal information.

These impacts can be substantially reduced or mitigated if AGS's recommendations in **Appendices 1 and 2** are adopted, including by:

- obtaining appropriate consents
- requiring regular review of links by specialists and authorised representatives
- implementing layered privacy notices
- limiting CROMPS data used by the Department.

If the recommendations in the primary and supplementary PIA are adopted in full, we consider the Department will comply with the APPs and implement appropriate solutions to minimise or eradicate potential privacy impacts of the MCF Portal.

Part 1 – Information Flows

1. This part of the PIA summary briefly summarises the flow of information (collection, use and disclosure) within the MCF Portal.
2. In the primary PIA, AGS described in detail the relevant steps for handling personal information as part of the MCF program. Details of the previous manual process, and how this matches up with the online process, is summarised in **Table 1** below. **Image 2** depicts how the specialist registration process will operate.

Step	Manual process	Online portal process
1a	Invite specialist to join MCF program	Invitation for MCF program
1b	Receive initial indication of interest from specialist	
2	Send out proforma consent form to specialist	Specialist registers for the MCF portal: • Verify identity using myGovID • Verify practitioner status and speciality using CROMPS and AHPRA data • Create user profile Authorised representative registers for the MCF Portal
3	Obtain consent from specialists to (1) extract data and (2) communicate with the Department re publication	
4	Extract CROMPS or AHPRA Data	
5	Prepare pre-populated form for specialist to complete / send to specialist for review	Specialist or authorised representative enters specialist's details
6	Receive completed form from specialist	
7	Transfer information to staging environment	
8	Specialist review of information in staging environment / confirm or correct information / obtain consent to publish	Specialist approves data for publication
9	Publish specialist information via the MCF website	Approved data published on MCF website
10	Withdrawal of consent	Withdrawal of consent

Table 2: MCF program personal information flow

3. The following levels of read/write access will apply to each users in the Portal:

User	Level of access
Contact Centre	Full read/write access
Specialists	Able to input information (notified of authorised representative changes).
Authorised representative	Those with full access can input information, edit any aspect of profile without requiring approval from specialist if permitted (specialist notified). Those with partial access can input information on behalf of specialist or authorised representative, specialists must approve any changes.

Table 2: Level of user access and permissions

Step 1 – Invitation for MCF program

4. As part of the pilot phase of the Project, the specialist will receive an email invitation to participate in the MCF program. The email will include a link to the registration page for the MCF Portal.

Step 2 – Registration for MCF Portal

5. Two types of external users can register for the MCF Portal: (1) specialists and (2) authorised representatives.

Specialist registration

6. The specialist will visit the MCF Portal by either selecting the email link (pilot phase only) or visiting the MCF Portal website directly (**Image 1**).
7. At the outset, they will be asked to nominate their areas of speciality. If their specialty is not yet available, users will be able to register their interest and will be notified via email when their specialty becomes available.
8. If the specialist's area of speciality is eligible to participate, they will proceed to the registration phase. In order to register, a specialist will need to authenticate their identity via a three step process and provide additional information and consents.

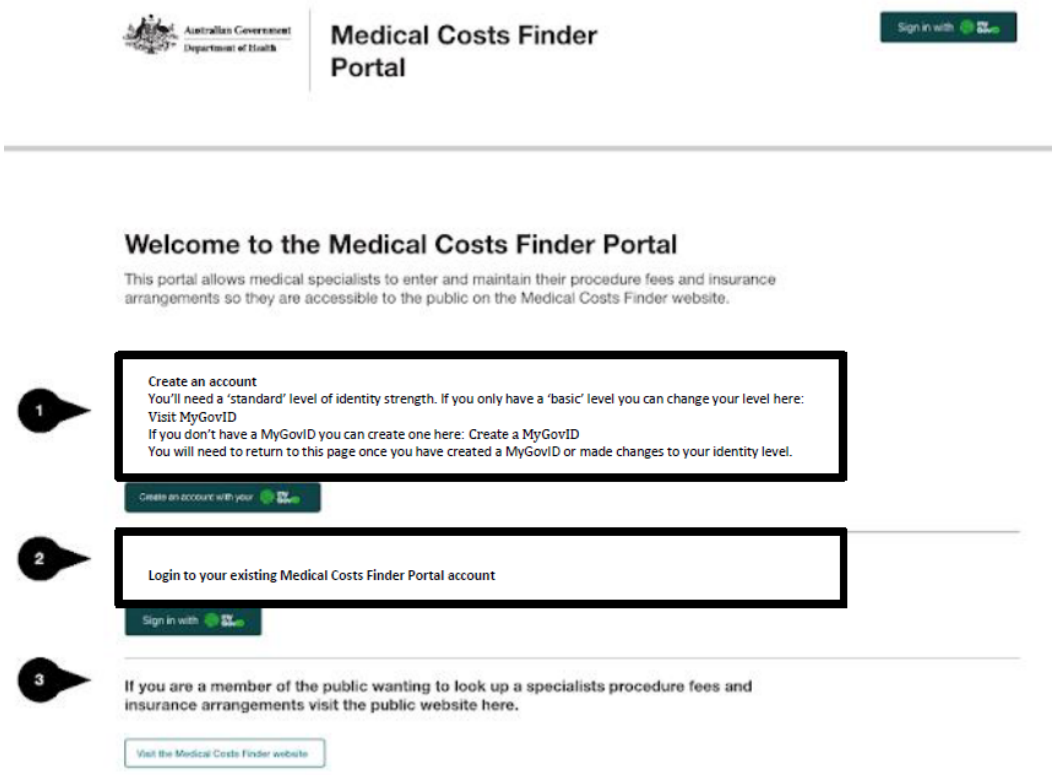

Image 1: MCF Portal Homepage

(1) Proof of identity

9. A specialist will need to prove their identity by setting up or using an existing myGovID. The myGovID will need to be set up to a standard identity strength by verifying two Australian identity documents.
10. After successfully verifying their identity, the specialist will be asked to consent to the Digital Identity Exchange sharing their given names, surname, common name (if applicable) and date of birth (**DOB**) with the MCF Portal. This information will be used to auto populate these fields in the MCF user profile. This information cannot be changed by a specialist.

(2) Verification of medical practitioner status and specialisation

11. To facilitate the verification of their status as a medical practitioner and specialisation, the specialist will be asked to provide additional information including their full name, AHPRA registration number and Medicare provider number.

12. This information will be used to ensure the name they provided to the Portal is consistent with the information in their verified digital identity (myGovID). The specialist will then select from a list of applicable specialties.

13. The specialist must also consent to the terms and conditions of the MCF and consent to the use of personal information about the specialist from the Centralised Register of Medical Practitioners (**CROMPS**) acquired under the *Health Insurance Act 1973* (**HI Act**).

14. Checks will then be undertaken to verify:

14.1. **Practitioner status:** the specialist's name in their verified digital identity, AHPRA number and MBS provider number will be checked against the same fields in CROMPS information (full name, AHPRA number, MBS provider number).

14.2. **Specialisation:** the specialist's nominated speciality will be verified against their speciality code in CROMPS.

(3) Entering profile information

15. If a user account is created, the specialist will then need to enter some basic profile information:

    15.1. Personal details (title, qualifications) that will appear on the MCF website

    15.2. Practice details (name, address) that will appear on the MCF website. Each practice location must be added by the specialist.

    15.3. Contact details (phone number, email) that will be used for administrative purposes only and will not be published on the MCF website.

16. From the profile page, a specialist can nominate an authorised person.

Authorised representative registration

17. The specialist may authorise another person to enter details on their behalf (**authorised representative**) by providing their email address. An authorised representative can act for more than one specialist and for more than one location per specialist.

18. When registering, the authorised representative will need to consent to the Department collecting, using and disclosing their personal information to administer the MCF Portal.

19. If the nominated authorised representative is not an MCF Portal user, they will need to have a myGovID at the 'standard' level, or need to create one. They will be asked to enter the registration code from their invitation email and consent to the MCF terms and conditions.

20. MCF Portal users can also make a request to a specialist to be linked as their authorised representative. This process follows the same steps at [17]-[18].

21. Specialists will be able to manage their authorised representatives in the MCF Portal. They will be able to add an authorised representative, manage the permissions for existing authorised representatives or remove a representative.

Step 5 – Enter specialist details

22. Post-registration, the specialist or authorised representative can enter details about the specialist into the MCF Portal, e.g. to add locations or add/change fee and insurance information.

23. Each procedure and location must state the fee, any applicable gap arrangements with the insurance provider listed and the quantum of the gap arrangement (or 'no gap' arrangement).

Step 8 – Specialist approves data for publication

24. A specialist can opt to publish relevant profile information to the MCF website. If the specialists chooses to do this, they must review their profile information for publication, confirm this information is correct and provide express consent to publish the profile information on the MCF website.

25. Where information is added/changed by a linked authorised representative, the specialist will receive an email:

    25.1. notifying of the changes if the authorised representative can publish information on the specialists behalf

    25.2. requesting the specialist login and approve publication where an authorised representative can only submit information for review.

Step 9 – Approved data published on MCF website

26. If the specialist approves publication, the profile information is extracted from the MCF Portal database and transferred to the data warehouse/data lake for access by the MCF website using an Application Programing Interface (**API**).

27. Once transferred, the information will be published and publicly searchable on the MCF website by users by location (geographic region), speciality group or procedure.

Step 10 – Withdrawal of consent / authorisation

28. MCF Portal users will be able to withdraw their consent using the Portal. The specialist can do this by cancelling their registration and withdrawing their consent to participate in the MCF program.

29. There is also a process by which administrators can deactivate or suspend a specialist. This will generally occur when a medical professional has been suspended or retires.

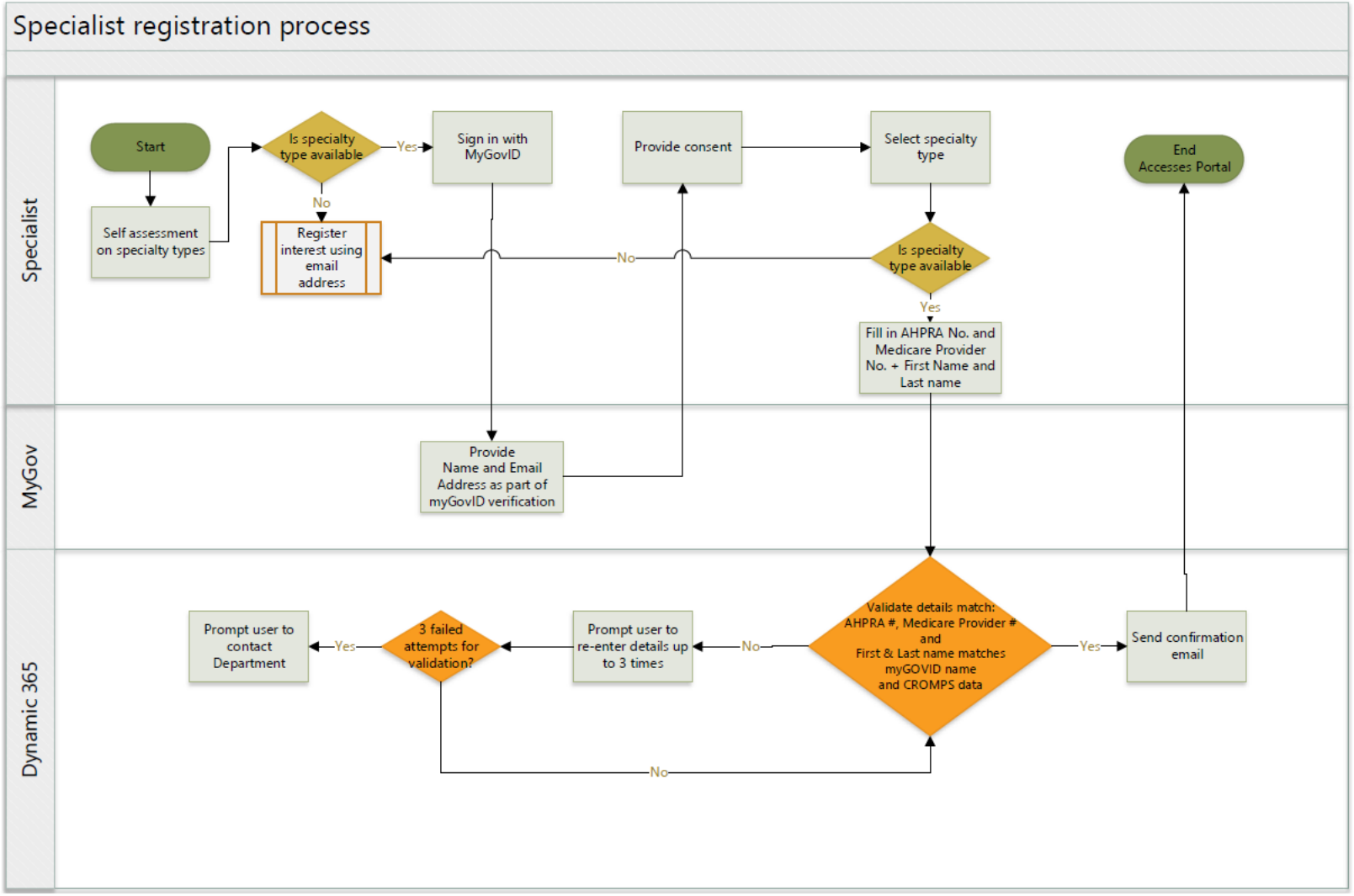

Image 2: MCF program personal information flow

Part 2 – Review of MCF benefits, impacts and protections

30. Throughout the development of the MCF Portal, the Department has implemented a privacy by design approach.

31. This summary is about a second and supplementary PIA which reflects how the Department have pro-actively sought to address privacy risks at each stage of the OOPT Project. Throughout the preparation of both PIAs, the Department has sought to mitigate privacy risks by adopting changes to the system build to reflect a privacy enhancing design.

32. The MCF Portal emphasises user choice and control consistent with best practice and the objects of the *Privacy Act 1988.* The specialist must consent to all stages of the process but can also determine what degree of control they retain over the information. The specialist can opt out of the Portal at any time. The specialist can engage people to assist with the management of their fee information on the Portal and can determine what level of assistance they require.

Benefits of the Project

33. Intrinsic to the Privacy Act is the balance that is sought to be achieved between the interests of the individuals and those of the entities the legislation regulates. This is reflected in the objects of the Privacy Act which recognise that the protection of the privacy of individuals is to be balanced with the interests of entities in carrying out their functions or activities: see s 2A(b).

34. The Department publishes the MCF website as part of its broader education and awareness function. Information about individual specialists will provide the public with greater transparency around the costs of medical specialist providers and enable users to:

    34.1. obtain fee information in advance of consultations or appointments to make informed decisions about the cost of treatment

    34.2. compare the fees of specialists, including a specialist's fees at different locations, to select arrangements most suitable for their circumstances.

Impacts of the Project

35. Privacy has been a key consideration within the build of the MCF Portal as a project involving new methods of handling personal information.

Potential impacts

36. Although the adoption of an online portal process for the collection of information is generally privacy enhancing, the handling of personal information by the MCF Portal may impact on the privacy of individuals for a number of reasons. These include:

    36.1. any collection and use of unnecessary or irrelevant data may unreasonably intrude on the privacy of individuals and increase their exposure to other privacy risks

    36.2. an individual's ability to control who can see or use their personal information is fundamental to an individual's privacy. Any collection of personal information from third parties without the individual's knowledge or consent will cause an individual to have less control over how their personal information is handled

    36.3. additionally, out-of-date consents or data quality issues will risk the publication of inaccurate information about specialists on the MCF website

    36.4. due to the nature and volume of personal information handled by the Department, this may expose individuals to harm if unauthorised access, use or disclosure were to occur.

Potential harms

37. Some of these impacts have the potential to harm individuals, including the risk of emotional, financial or reputational harm to individuals if:

    37.1. inaccurate or incorrect information is published about a specialist on the public MCF portal as a result of a system error, incorrect authorisations or a malicious actor exploiting out-of-date authorisations

    37.2. personal information is made available to the public, or a section of the public, as a result of unauthorised access, use or disclosure.

38. While we view the prospect of the impacts at paragraphs 36.1 to 36.4 to be low, the realisation of any of these events could have a significant impact on the privacy of an individual. For example, a failure in the operation of identity verification or consent rules might permit a malicious actor to publish incorrect and untrue information about a specialist on the MCF website.

39. As this risk of these privacy impacts is not negligible, taking into account the potential nature and severity of any harm, the MCF Project should be treated as a 'high risk' project. [1] Importantly, the risks associated with these activities can be minimised by implementing the recommendations made in this PIA.

Protections within the Project

40. There are number of protections within the MCF Portal that ensure the security of personal information and mitigate against other privacy risks. Recommendations from the primary PIA that are relevant to the MCF Portal, as well as all recommendations from the supplementary PIA are set out in **Appendices 1 and 2** and referred to in the paragraphs below.

Minimisation of personal information

41. Over the course of the OOPT Project, the Department has significantly reduced the volume of personal information to be handled about specialists. Only limited, relevant personal information will be collected directly from specialists about fees and practice locations (**Recommendation 21**). CROMPS information used to verify the eligibility of specialists will be limited to eligible speciality groups (**Recommendation 26**).

Obtaining ongoing and relevant consents

42. As detailed in **Part 1**, obtaining ongoing consents from specialists and authorised representatives for the collection, use and disclosure of their personal information is integral to the MCF Portal. **Recommendations 9** and **20** outlines the consents to be obtained at **Step 2**, **Step 5 and Step 8** from specialists and authorised representatives.

43. To ensure informed consent, a link to a detailed collection notice is provided at the point of collection as part of the linking process in **Step 2**, entering details in **Step 5** and approving publication in **Step 8**: **Recommendations 22, 23.**

44. If a specialist or authorised representative withdraws consent, user access to their personal information via the MCF Portal will be removed. Where a specialist withdraws consent, their information will be removed from the MCF website and from the data warehouse which populates the MCF website: **Recommendation 29**.

[1] A 'high risk' project involves new or changed ways of handling personal information that is likely to have a significant impact on the privacy of individuals: see s 12(1) of the Privacy Code.

Verification of identity

45. Requiring users to authenticate for the MCF Portal using a digital identity verified to the standard level provides the Department with a high level of assurance as to the identity of each user. Matching a specialist's digital identity with information in CROMPS provides assurance that the Department is dealing with a specialist that is eligible to publish information on the MCF website.

Quality of personal information

46. The MCF Portal has extensive safeguards to ensure the information collected, used and disclosed by the Department is accurate, up to date and complete. These include the requirement for users to verify their identity, only submit complete forms (**Recommendation 10**) and declare information is accurate at the time of collection.
47. All information (with the exception of information associated with their digital identity) can be amended via the MCF Portal and information published on the MCF website will be regularly reviewed and updated: **Recommendation 14**.

Audit logs

48. The MCF Portal will produce audit logs of specialist profile access and specialist record additions, updates, and deletions as well as technical events such as exceptions and errors. These audit logs will be subject to regular reviews to protect against unauthorised use or disclosure: **Recommendation 15**.

Access security and training

49. Levels of permission to access the MCF Portal will be cascaded and appropriate permissions will depend on the staff member's role in the Department.
50. To mitigate against unauthorised access, the Department has committed to implementing a regular prompt from specialist and authorised representatives to frequently review their ongoing association: **Recommendations 12, 27**.
51. The Department has a data breach response plan, implemented across the agency, and brought to the attention of staff as part of annual training. In addition to this IT Security maintain an incident response plan which encompasses data loss. Similarly Protective Security maintain an Incident response policy which deals with information loss.
52. Finally, the Department has committed to adopting a number of recommendations to further strengthen these protections.

Appendix 1 – Primary PIA Recommendations

The following table summarises ongoing recommendations from the primary PIA that are **met** by the MCF portal or are **yet to be implemented**.

#	Primary PIA Recommendation	Department Response	Supplementary PIA Status
4	The Department develop a simple and straightforward process for withdrawing consent, with details available on the IFD website provided to medical specialists in Step 5 and the Project's long form collection notice.	The Department will adopt this recommendation and devise simple and straightforward processes appropriate to the manual and/or web-based environment for a specialist to withdraw their consent at any time and make this advice available to medical specialists.	A simple and straightforward process for withdrawing consent has been incorporated into the online portal process.
9	The Department seek express consent for overseas disclosure of information to be published via the IFD website on its website at Step 8.	The Department will adopt this recommendation and consent to be obtained at Step 8 will include overseas disclosure as information will be published on a publically accessible website.	The consent wording prepared in response to **Recommendation 20** requires express consent for overseas disclosure at Step 2 and Step 8.
10	The Department develop a process for handling incomplete responses at Step 1b, Step 3, Step 5 or Step 8.	The Department will adopt this recommendation and develop procedures to manage instances where (i) the Department needs to liaise with Specialists or Authorised Persons for incomplete information sets and (ii) to ensure only complete and approved information is progressed to publication.	The MCF Portal only permits complete responses to be submitted.
12	The Department invite medical specialists to update their contact details in Step 3 and Step 5 to ensure information used is up-to-date.	The Department will adopt this recommendation and invite medical specialists to review and update their contact details in Step 3 and Step 5 to ensure they are current.	The MCF Portal permits specialists and authorised representatives to update their contact details at any time.
14	The Department develop and implement processes: • For specialists to regularly review and update the information published on the IFD website • To review personal information used and disclosed as part of the IFD Project to ensure it remains relevant to the transparency purpose.	The Department will adopt this recommendation and develop and implement processes for specialists or their Authorised Person to review and update information for publication and the Department review personal information disclosed as part of the IFD website to ensure it remains relevant to the transparency purpose.	This process has yet to be implemented. **Recommendation 25** additionally suggests that any linking by an authorised representative also be regularly confirmed to prevent unauthorised collection and publication of specialist information. The MCF Portal will reflect this recommendation, which will involve a reminders function that will go out to users every 6 months.
15	The Department implement audit processes to review OOPT related audit logs and access review rights on a quarterly basis.	The Department will adopt the recommendation to undertake review of audit logs and access review rights on a quarterly basis.	This will be implemented in relation to the MCF Portal.

Appendix 2 – Supplementary PIA Recommendations

Additional recommendations made in the supplementary PIA are set out below. For each recommendation, we have indicated the nature of the risk.

	**Compliance risk:** implementation of this recommendation is required to comply with the requirements of the Privacy Act
	**Privacy protection:** implementation of this recommendation will minimise privacy risk and improve privacy protections

Recommendation 18 – Consider publication of PIA	
	The Department consider publishing a summary PIA on its website.
Response:	The Department agrees with this recommendation.

Recommendation 19 – Minimisation collection of name of specialist	
	The Department only collect the name of a specialist at the time it collects the specialist's AHPRA number where the specialist has indicated that their name on their AHPRA registration is different to their identity documents.
Response:	The Department notes this recommendation, however the Department intends to collect the name of the specialist as part of the registration process. There will be a note to indicate that the name being registered should be the name used on the specialist's AHPRA registration.

Recommendation 20 – Consent to collect personal information	
	The Department update Step 2 to require a specialist or authorised representative to confirm as part of the linking process that: • the other person consents to be nominated and to provide their email address to the Department • to require both the party requesting and accepting the link to consent to the collection of their personal information from the other person to manage their relationship, or in the case of specialists, to update their details in the MCF Portal. The Department update Step 5 to require an authorised representative to confirm that the specialist consents to the collection and publication of their details.
Response:	The Department will adopt this recommendation and include the above consents at Step 2 and 5.

Recommendation 21 – Character limit on free text fields	
	The Department consider setting a character limit on free text fields to minimise the risk of receiving unsolicited personal information.
Response:	The Department will adopt this recommendation.

Recommendation 22 – More prominent collection notice prior to registration	
	The Department include a more prominent privacy notice at Step 2 prior to a user registering for the MCF Portal, linked to the long form privacy notice.
Response:	The Department will adopt this recommendation and provide a more prominent privacy notice at Step 2.

Recommendation 23 – More prominent links to privacy notice	
	The Department consider including more prominent links to the privacy notice as part of the linking process in Step 2, entering details in Step 5 and approving publication in Step 8.
Response:	The Department will adopt this recommendation and provide more prominent privacy links at Steps 2, 5 and 8.

Recommendation 24 – Recommend specialists use same identity documents	
	The Department include a ‘tip’ at the registration page (Image 5) that specialists use the same identity documents submitted as part of their AHPRA registration.
Response:	The Department notes this recommendation, but will not implement.

Recommendation 25 – Develop process to verify identity after matching fail	
	The Department develop a process to resolve any difference in a specialists name in their digital identity and CROMPS information, including the destruction of any change of name documentation after verification is complete.
Response:	The Department will adopt this recommendation and develop a process whereby any identity documents submitted by specialists are destroyed. It should be noted the Department does not anticipate these kinds of documents will be required from specialists.

Recommendation 26 – Review processes for handling CROMPS data	
	The Department consider if the CROMPS data extract can be limited only to specialists eligible to participate in the MCF Portal.
Response:	The Department will adopt this recommendation, noting however that while the CROMPS data extract will be limited to the eligible speciality groups, it will include all specialists in those groups and not just those specialists who opt to participate.

Recommendation 27 – Minimise potential for misuse of inactive accounts	
	The Department implement a regular requirement to confirm the ongoing association between a specialist and an authorised representative, as well as measures to prevent publication of edits made by an authorised representative until the relationship is confirmed. The MCF Portal Terms and conditions require users to take steps to unlink a specialist or authorised representative as soon as possible after the end of the relationship.
Response:	The Department agrees with this recommendation and will implement a reminders system for specialists to regularly review authorised persons' permissions in the MCF Portal.

Recommendation 28 – Appropriate contractual measures for any 3rd party provider	
	Appropriate contractual measures be imposed when engaging any third party provider.
Response:	The Department agrees with this recommendation.

Recommendation 29 – Remove specialist data from Portal upon consent withdrawal	
	The Department delete specialist data from the MCF data warehouse upon withdrawal of consent but retain that information in the MCF Portal database in accordance with their usual archiving processes and the *Archives Act 1983.*
Response:	The Department will adopt this recommendation.