

# Department of Health – PIA – Routine data matching

## Executive Summary

This Privacy Impact Assessment (**PIA**) has been commissioned by the Department of Health (**Department**) to serve as a baseline assessment of routine and ongoing data matching programs relating to Medicare compliance by health providers (**routine data matching programs**).

It is intended to be a foundational document and covers a range of compliance activities undertaken by the Benefits Integrity and Digital Health Division (**BIDHD**). BIDHD intends that, having addressed the foundational questions in this PIA, only data matching activities which do not follow the standard processes outlined in this PIA will require a supplemental PIA.

## Overview of this PIA

This PIA comprises four parts, summarised in the table below.

Part	Description
<b>Part 1</b>	Explains the routine data matching programs undertaken by BIDHD and examines overarching questions relating to data matching activities generally.
<b>Part 2</b>	<p>Examines the flows of personal and sensitive information in relation to 4 pilot data matching programs (<b>data matching pilots</b>):</p> <ul style="list-style-type: none"><li>• eHealth Practice Incentives program (<b>ePIP</b>)</li><li>• Psychotropics program</li><li>• Medicare Benefits Schedule (<b>MBS</b>) and Pharmaceutical Benefits Scheme (<b>PBS</b>) Claims program</li><li>• Home Affairs Passenger Movement Records program.</li></ul> <p>These programs are examined in their own right and as examples of the typical governance processes for Medicare compliance data matching activities undertaken by the Department in respect of health providers.</p>
<b>Part 3</b>	<p>Part 3 addresses the compliance of the data matching pilots with:</p> <ul style="list-style-type: none"><li>• Pt VIIIA of the <i>National Health Act 1953</i> (<b>NH Act</b>), which authorises data-matching</li><li>• the Australian Privacy Principles (<b>APPs</b>) in Sch 1 to the <i>Privacy Act 1988</i> (<b>Privacy Act</b>)</li><li>• the <i>National Health (Data-matching) Principles 2020</i> (<b>DM Principles</b>) made under s 132F(1) of the NH Act, and</li><li>• the <i>National Health (Privacy) Rules 2021</i> (<b>Privacy Rules</b>) made under s 135AA of the NH Act.</li></ul> <p>Where we have identified privacy risks or gaps in meeting the legislative requirements, we have made recommendations to address or mitigate these risks.</p>
<b>Part 4</b>	Examines the Department's systems for reviewing and approving new data matching programs to determine whether they are likely to ensure compliance with these requirements in future and sets out a risk matrix which identifies key privacy risks for new data matching activities to determine whether a supplementary PIA is required in relation to new activities.

---

## Purpose of this PIA

APP 1.2 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, such as the data matching pilots: see s 12(1) of the *Australian Government Agencies Privacy Code (Privacy Code)*.

This PIA is a key part of the activities undertaken by the Department to identify possible privacy impacts from its routine data matching activities, implement solutions to minimise any privacy risks and ensure compliance with legislative requirements.

---

## Summary of findings

In **Part 3** of this PIA, we have identified a number of potential privacy impacts specific to the data matching pilots including:

- collection of detailed health information about patients and providers
- indirect collection of matched data about patient and providers (other than from the patients and providers)
- the collection of large amounts of personal information about patients and providers, including about providers who may not be suspected of wrongdoing
- risks associated with data quality, unauthorised access and data security due to the volume and sensitivity of the data to be matched.

We consider these impacts can be mitigated if the recommendations in this report are adopted, including through:



- updating guidance to the public about the data matching programs, including through the data matching notice and the public register
- updating governance documents to require technical standards reports to contain more detailed information and to minimise the data fields and data subjects in the matching process
- carefully reviewing the quality of matched datasets to ensure that data matching input and data matching output is accurate, complete and up to date
- increasing guidance about the destruction of data and what constitutes the 'results' of data matching
- carefully reviewing the contractual arrangements with contracted service providers
- ensuring that information technology systems are secure and regularly audited.






Ultimately, while data matching will impact on the privacy of individuals, it delivers considerable benefits to the community in assisting with the prevention and identification of, and taking compliance action in relation to, incorrect claiming, inappropriate practice and fraud by health providers. If appropriate steps are taken to implement the measures recommended in this PIA, we consider the privacy impacts associated with data matching activities can be minimised.





---





## Recommendations





Recommendations relating to compliance risks and measures for improving privacy practices are set out in detail in **Part 3** of the PIA and summarised below.



Icons	Recommendations
	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

#	Type	Recommendation	Department's Response
1		<p><b>Consider publication of PIA</b></p> <p>The Department consider whether this PIA, or an edited or summary version, should be published on its website or otherwise made available on request.</p>	<p><b>Accepted.</b> The Department will publish an executive summary of this PIA on its website.</p>
2		<p><b>Update the Department privacy policy</b></p> <p>The Department review and update its privacy policy to insert a reference to the Data matching for Medicare Compliance Purposes (<b>DM Notice</b>) and the public register which contain further detail about the Department's personal information handling practices.</p>	<p><b>Accepted.</b> The Department will review and update Health's Privacy Policy to include a reference to the DM Notice and the public register.</p>
3		<p><b>Update the DM Notice</b></p> <p>The Department update the DM Notice to include a reference to the kinds of Medicare compliance actions that may be taken as a result of data matching. It could do so by linking to the Department's <a href="#">How we ensure Medicare compliance</a> web page.</p>	<p><b>Accepted.</b> The Department will update the DM Notice to include the actions that may be taken as a result of authorised information-matching.</p>
4		<p><b>Consider the privacy evaluation when completed by Data Governance and Engineering Section (DG&amp;ES)</b></p> <p>The Department consider the recommendations of the DG&amp;ES privacy evaluation report when determining the content and frequency of any future evaluations.</p>	<p><b>Accepted.</b> A privacy evaluation report will consist of this PIA and a Post-implementation Review of the data matching pilots. It will serve as the first privacy evaluation by the Department for data matching for Medicare compliance purposes and will establish the frequency of subsequent reviews.</p>
5		<p><b>Update the public register</b></p> <p>The Department review and update the data matching public register to include more detail about the kinds of information used in data matching activities, the datasets from which the information was taken and the source agency for each kind of information. We have proposed wording for the 4 pilot programs in this PIA.</p>	<p><b>Accepted.</b> The Department will update the Public Register and the Public Register templates as per the suggested wording in this PIA.</p>

#	Type	Recommendation	Department's Response
6		<p><b>Update the Data Matching Governance Directives (Directives)</b></p> <p>The Department update sections 1.4 and 2.4 of the Directives to require the Technical Standard Reports (<b>TSRs</b>) and records of the data matching program to include information about decisions:</p> <ul style="list-style-type: none"> <li>• that the matching is reasonably necessary for a permitted purpose</li> <li>• the data fields that are necessary for that purpose and how they can be minimised</li> <li>• the data subjects that are necessary for the matching and how they can be minimised</li> <li>• as to how the use of personal information can be minimised.</li> </ul>	<p><b>Accepted.</b> The Department will update the Directives sections 1.4 and 2.4 and the relevant templates as required. Specifically, the TSRs will be updated to include a signature box to indicate confirmation by the Data Analyst and relevant Director that:</p> <ul style="list-style-type: none"> <li>• the matching is reasonably necessary for the indicated permitted purpose(s)</li> <li>• the data fields are necessary for that purpose (including details of how they have been minimised)</li> <li>• the data subjects are necessary for the matching (including details of how they have been minimised)</li> <li>• the personal information has been minimised to the extent possible for the data matching activity (and how this was done).</li> </ul>
7		<p><b>Update the Final Approval template</b></p> <p>The Department update the Final Approval template to require the delegate of the Chief Executive Medicare (<b>CEM</b>) to:</p> <ul style="list-style-type: none"> <li>• be satisfied of the matters in s 20(1) of the <i>National Health (Data-Matching) Principles 2020 (DM Principles)</i></li> <li>• note the matters in the TSR that relate to s 20(2) of the DM Principles.</li> </ul>	<p><b>Accepted.</b> The Department will update the Final Approval template to specifically refer to s 20(1) and s 20(2) for consideration by the delegate of the CEM.</p>
8		<p><b>Review data fields, subjects and the use of personal information as the data matching pilots progress</b></p> <p>The Department regularly review and update the technical standards to determine the necessity of including all data fields, data subjects and personal information in future iterations of the program.</p> <p>In particular, the Department consider whether fewer data fields can be included, the number of match subjects can be reduced or whether less personal information can be used.</p> <p>Where fields are excluded, the Department should consider its obligations under Pt 5 of the DM Principles and ensure any changes are accurately recorded in the technical standards.</p>	<p><b>Accepted.</b> The Department will include in the Divisional policy and data governance framework that regular reviews are required. This will include:</p> <ol style="list-style-type: none"> <li>1. A review of the TSR post-match to ensure that any changes to the data matching process post-approval is documented</li> <li>2. A regular review of the TSR for ongoing data matching programs to ensure that any changes to the data matching process post-approval is documented</li> <li>3. Developing robust Quality Assurance and minimisation procedures</li> <li>4. Updating the TSR template to include destruction plans.</li> </ol>
9		<p><b>Update DM Notice to provide notice of collection</b></p> <p>The Department update the DM Notice to inform consumers and providers of the collection of data matching input and output, and to make the minor amendments proposed in Table 28.</p>	<p><b>Accepted.</b> The Department will update the DM Notice to inform consumers and providers of the collection of data matching input and output, and to make the minor amendments proposed.</p>

#	Type	Recommendation	Department's Response
10		<p><b>The Department consider means of notifying affected classes of individuals of the collection</b></p> <p>Where a data matching program involves the collection of data about an identified class of persons, such as the ePIP program, the Department consider the reasonableness of any means of notifying the affected class of persons of the collection, for example in enrolment documents for the program.</p>	<p><b>Accepted.</b> The Department will investigate adding in a notice of data matching in the Practice Incentive Programs Guidelines. All other projects will be reviewed on a case-by-case basis to identify if there is a reasonable method of notifying a class of individuals.</p>
11		<p><b>Notification of data matching at time of original collection</b></p> <p>The Department:</p> <ul style="list-style-type: none"> <li>include within notices relating to the collection of original data information about the disclosure of personal information to the CEM for a data matching purpose and a link to the DM Notice</li> <li>liaise with source agencies about the collection of original data and encourage the inclusion of information about disclosure for data matching activities in the relevant collection notice or the agency privacy policy.</li> </ul>	<p><b>Accepted.</b> The Department will liaise with source agencies about the collection of original data and encourage the inclusion of information about disclosure for data matching activities in the relevant collection notice or the agency privacy policy.</p>
12		<p><b>Update Directive 1.7 to require agreement about data specifications</b></p> <p>The Department update Directive 1.7 to require Letters of Agreement (<b>LoAs</b>) to facilitate agreement about the specifications or format of shared data to minimise data quality issues. This can be done by reference to the Home Affairs program LoA, which includes a schedule of data specifications.</p>	<p><b>Accepted.</b> The Department will update Directive 1.7 and the LoA template with a requirement that a schedule of data specifications (as per the Home Affairs LoA) is included in data sharing agreements to ensure data quality.</p>
13		<p><b>The Department update the TSRs to include all measures taken to ensure the quality of data</b></p> <p>The Department should update the TSRs for each document to make clear what reasonable steps it has taken to ensure that data matching input and data matching output are accurate, up-to-date and complete.</p>	<p><b>Accepted. The Department will:</b></p> <ol style="list-style-type: none"> <li>Undertake regular reviews of the TSRs to ensure that any changes to the data matching process post-approval is documented (as per Recommendation 8)</li> <li>Ensure any filtering of records is included in the TSRs</li> <li>Develop closure reports/checklists for TSRs.</li> </ol>

#	Type	Recommendation	Department's Response
14		<p><b>Recommendation 14 – Consider further steps in relation to data quality of MBS and PBS Claims data matching output</b></p> <p>There are significant APP 10.1 risks in relation to the MBS and PBS Claims program due to inherent limitations in the data matching input, which may have the effect that data matching output is incomplete or misleading. While many of these risks are addressed by the Department prior to operational treatment, we recommend the Department carefully consider the data quality of data matching output in the post implementation review to determine whether further steps could be taken to ensure that the targeted MBS and PBS services are sufficiently tailored to ensure the matched data is accurate, up-to-date and complete.</p>	<p><b>Accepted.</b> The Department is committed to continuous improvement and will initiate data quality measures for data matching output. This will include data governance processes for an escalation procedure for notifying Services Australia about any data quality issues.</p>
15		<p><b>Improve the clarity of the TSRs</b></p> <p>The Department ensure that TSRs for data matching programs include clear information demonstrating the process by which the data is matched, the reason for inclusion of each data field, which information is used as a match key, and what the final result of the data matching activity will be.</p>	<p><b>Accepted.</b> The Department will update the technical standards templates and work to ensure there is adequate detail regarding the process by which the data is matched, the reason for inclusion of each data field, which information is used as a match key, and what the final result of the data matching activity will be.</p>
16		<p><b>Review and audit access to protected information layers</b></p> <p>The Department regularly:</p> <ul style="list-style-type: none"> <li>• review access permissions and remove access permissions to staff without a need-to-know</li> <li>• audit access to the raw data layer and the consumable data layer to ensure its data access restrictions are effective.</li> </ul>	<p><b>Accepted.</b> Access permissions and monitoring policies and procedures have been included in Divisional Data Governance Policies.</p>
17		<p><b>Appropriate contractual measures for any 3rd party provider</b></p> <p>Appropriate contractual measures be imposed when engaging any third party provider, including to limit the use of matched data to the nominated permitted purpose for which the original data was matched and the destruction of matched data when no longer needed. Consideration should also be given to technological solutions to limit the use of self-service tools to the nominated permitted purposes.</p>	<p><b>Accepted.</b> The Department will impose appropriate contractual measures for any third-party provider.</p>

#	Type	Recommendation	Department's Response
18		<p><b>Update TSRs to provide a definite timeline for destruction of data</b></p> <p>The TSRs should be updated to:</p> <ul style="list-style-type: none"> <li>• address the destruction of data matching input (other than live feeds and original data) and data matching output</li> <li>• include a concrete timeframe for destruction of all data which is based on the Department's assessment of when data is no longer needed for any permitted purpose.</li> </ul>	<p><b>Accepted.</b> The Department will develop a destruction plan based on each of the compliance operational treatment types. The TSR template will also be updated to include destruction requirements.</p>
19		<p><b>Update Directive to provide guidance on the definition of results of data matching</b></p> <p>The Department update Directive 2.5 to provide additional guidance on the definition of 'results of matching' and the kinds of documents that must be destroyed when no longer needed for any s 132A purpose.</p>	<p><b>Accepted.</b> The Department will update the Directives with a definition of 'Results of matching'. A Destruction Plan will be developed based on each of the compliance operational treatment types with a specific timeframe or 'trigger' to identify when the data is no longer required for the purpose of the match.</p>