



IMPLEMENTATION REPORT

MADIP Privacy Impact Assessment Update

November 2020



OVERVIEW

In 2019 the Australian Bureau of Statistics (ABS) conducted an update to the Multi-Agency Data Integration Project (MADIP) Privacy Impact Assessment (PIA) on behalf of the MADIP Board. The [MADIP PIA Update](#) was published in November 2019 accompanied by an [assurance report](#) from external privacy advisors Maddocks who were engaged to provide independent review, advice, and assurance for the PIA process and report. At the same time, a [Response to 2019 MADIP PIA Update](#) from the MADIP Board was also published, outlining the Board's response to each of the recommendations and suggestions presented in the PIA.

This Implementation Report presents the progress since the publication of the MADIP PIA Update towards each of the recommendations for compliance with the [Australian Privacy Principles \(APPs\)](#) and suggestions to enhance privacy best practice for MADIP.

During the COVID-19 pandemic in 2020 the ABS has responded rapidly to data needs across government including through exploring new data sources, increased data integration activity and supporting high priority projects through access and analysis services. The MADIP partner agencies have also responded to new and changing demands throughout the pandemic. A focus on responding to demand for additional and more timely information about the impacts of COVID-19 on Australia has delayed the implementation of some findings from the MADIP PIA Update.

The five compliance recommendations in the MADIP PIA Update have largely been addressed or work is underway to address them. The ABS continues to take steps to ensure privacy is protected and data is kept safe and secure while responses to the best practice suggestions are determined and implemented.

1. SUMMARY OF RECOMMENDATIONS AND SUGGESTIONS

The 2019 MADIP PIA Update identified five areas of improvement to ensure MADIP data practices comply with the APPs. The compliance recommendations are summarised along with the relative APPs in Table 1 below.

A further twelve suggestions were put forward for consideration to enhance privacy best practice for MADIP. The best practice suggestions and relative APPs are summarised in Table 2.

Table 1: Summary of compliance recommendations

APP5 - Notification of the collection of personal information

Recommendation 1 The ABS should continue to update its APP 5 collection notices, used when the ABS is collecting personal information as a data custodian, to make it clearer to individuals that their personal information may be used for data integration.

Recommendation 2 In relation to collection of personal information by the ABS as the accredited Integrating Authority for MADIP, the ABS should:

- Advocate with entities responsible for collection notices to enhance transparency about their disclosure of personal information to the ABS for MADIP by taking reasonable steps to update notices or otherwise make individuals aware of data use.
- Continue to increase transparency about the collection and use of data, including personal information, for MADIP in online materials.

APP6 - Use or disclosure of personal information

Recommendation 3 MADIP data sharing documentation should be updated to provide information that confirms the APP 6 authority for sharing data to the ABS for MADIP.

APP11 - Security of personal information

Recommendation 4 The ABS should commit to undertaking a 2 yearly IRAP assessment of the MADIP operating environment as part of a regular program of audits of information security in MADIP.

Recommendation 5 The ABS should finalise and implement the MADIP Data Retention and Destruction policy.

Table 2: Summary of best practice suggestions

APP1 - Open and transparent management of personal information

- Suggestion 1** The ABS should update online materials to include more information on:
- Non-enduring linkages that have occurred.
 - Some summary information about the datasets that have been linked to MADIP.
 - MADIP's governance framework, including a description of the decision and assessment process (including risk assessments) or new linkages and research projects using MADIP.
- Suggestion 2** The ABS should continue to obtain advice from a range of sources (including data custodians, whole of-government building trust initiatives, and stakeholders such as those consulted for this PIA Update) to develop content for online materials for MADIP.

APP3 - Collection of solicited personal information

- Suggestion 3** The ABS should update online materials to outline the data minimisation approach, including treatment of sensitive data, for MADIP.

APP4 - Dealing with unsolicited personal information

- Suggestion 4** Before data are disclosed to the ABS for MADIP, the ABS should:
- Provide information and assistance to data custodians to aid them in checking data for unsolicited personal information; and
 - Work with data custodians to decide what reasonable steps, if any, will be taken to reduce the risk of unsolicited information being disclosed to the ABS for MADIP.
- Suggestion 5** MADIP data sharing documentation should be updated to highlight the issue of unsolicited information and to note the ABS will work with data custodians to take reasonable steps to reduce the risk of sharing unsolicited personal information with the ABS for MADIP.
- Suggestion 6** The ABS should update online materials to provide more information about the management of unsolicited personal information in MADIP.

APP5 - Notification of the collection of personal information

- Suggestion 7** Data custodian agency delegates should confirm that, for their disclosure of data to the ABS for MADIP, APP 5 notification requirements have been met and the APP 6 authority for disclosure (and use by the ABS for MADIP) is identified; data custodian delegates may wish to consult with their agency Privacy Officers or otherwise authorised officers for advice on these matters.
- Suggestion 8** MADIP data sharing documentation should be updated to provide information that confirms how APP 5 notification requirements are met for collection of data by the ABS for MADIP.

APP6 - Use or disclosure of personal information

- Suggestion 9** The ABS should update and maintain online materials that communicate to the public about the data shared in MADIP.

APP11 - Security of personal information

- Suggestion 10** The ABS should enhance information in online materials about the data security protections in place for MADIP.

Additional suggestions

- Suggestion 11** The MADIP Board should establish and document threshold triggers for future updates of the MADIP PIA.
- Suggestion 12** The MADIP Board should consider leveraging government consultation mechanisms to obtain broad-based advice on privacy issues and ethics issues relevant to MADIP.
-

2. RESPONSE TO COMPLIANCE RECOMMENDATIONS

Outcomes to address three of the five compliance recommendations have been delivered, with action to progress the other two currently underway. In discussing the recommendations below, we have noted:

- the MADIP Board's acknowledgement and commitment to the recommendations (published as the [MADIP Board's response](#)) following PIA publication in November 2019;
- actions taken in the past 12 months to achieve recommendation outcomes; and
- actions underway to progress recommendation outcomes.

Recommendation 1

The ABS should continue to update its APP 5 collection notices, used when the ABS is collecting personal information as a data custodian, to make it clearer to individuals that their personal information may be used for data integration.

MADIP Board response in November 2019

Agreed - The ABS is committed to transparency about its collection and use of information for MADIP, including through collection notices. The ABS will continue to test collection notice enhancements to ensure updates to wording are improving transparency as intended.

Action – Complete

The ABS routinely adjusts wording in collection notices as public understanding of topics evolves. In the case of data integration, the current approach to informing survey respondents is a high-level statement in initial approach materials, supported by supplementary materials that provide more detailed information about data integration for respondents.

To achieve transparency about data collection and use, the ABS has a broad program of work to optimise household survey approach materials. Data integration content improvements have been progressed as part of this program, and through qualitative research the ABS has deepened its understanding of survey respondents' interpretation of data integration.

The ABS has developed a succinct point-of-collection statement based on the learnings from this research. The statement below is an example of how data integration is raised in initial approach materials.

To create insights about Australia, and to keep the survey as short as possible, we will link your information with data from other sources. For more information, please visit our Survey Information Page at ([link to the survey](#), for example <https://www.abs.gov.au/NHS>)

Given the nature of MADIP and data integration it is difficult to provide condense a great level of detail, such as about data sources and linkage information, into a statement such as the one above. To address this, a general data integration statement can be found with survey information under the header "Will the information I provide be combined with other data?" (see the [National Health Survey](#) example above), and comprehensive data integration content is on the [data integration](#) pages. More detailed data integration resources for survey participants are under development and will be available on forthcoming survey information pages.

Next Steps

As part of continuous improvement, the ABS is developing an information page on data integration for interviewers to provide to participants on request during survey collection.

Recommendation 2

In relation to collection of personal information by the ABS as the accredited Integrating Authority for MADIP, the ABS should:

- *Advocate with entities responsible for collection notices to enhance transparency about their disclosure of personal information to the ABS for MADIP by taking reasonable steps to update notices or otherwise make individuals aware of data use.*
- *Continue to increase transparency about the collection and use of data, including personal information, for MADIP in online materials.*

MADIP Board response in November 2019

Agreed - The MADIP Board supports the ABS taking this advocacy role, noting that the PIA recognises that the decisions to update collection notices and determine 'reasonable steps' lie with entities responsible for collection notices.

The MADIP Board recognises that for some collections there may be no reasonable steps that can be taken to update collection notices. Where notices can be updated, it may take some time to implement changes.

The MADIP Board is committed to building transparency about the data shared with the ABS for the project and supports the ABS in updating MADIP online materials.

Action – In progress

The ABS has taken steps to increase its advocacy role regarding collection notices administered by MADIP data custodians. As a matter of standard practice, the ABS requires information about collection notices to be articulated in the Data Integration Plan whenever a new linkage is proposed, prompting project leads to engage with custodians about the supporting information around data collection.

Online transparency has been addressed by enhanced data integration online materials, including information about MADIP. The [MADIP Data and Legislation](#) page includes a summary of the two types of information shared for MADIP, these being personal identifiers and analytical information, and continues to be updated with new and potential data inclusions in MADIP.

Next Steps

- To further formalise recordkeeping around collection notices, the ABS is developing more standardised data sharing approaches with MADIP data custodians, through which the ABS will ask custodian to confirm how APP 5 collection notices support data sharing for MADIP.
- Review of MADIP online content is ongoing and information will continue to be updated as required.

Recommendation 3

MADIP data sharing documentation should be updated to provide information that confirms the APP 6 authority for sharing data to the ABS for MADIP.

MADIP Board response in November 2019

Agree - The MADIP Board notes that existing data sharing documentation for MADIP outlines the legislative or other authority for disclosing data to the ABS, but acknowledges there would be value in providing a more consistent approach to documenting the authority for disclosure by data custodians to the ABS, particularly where there is no specific legislative authority. The Board also

recognises the value in publishing information about the legislative or other authority for disclosing data to the ABS for MADIP.

Action – In progress

Similar to the action taken in response to Recommendation 2, the authority for disclosing data to the ABS is required to be documented in the Data Integration Plan and a risk assessment process is undertaken whenever a new linkage is proposed. The ABS has also updated data sharing documentation requirements for MADIP to more clearly articulate data custodians' authority for disclosing data to the ABS for MADIP.

A draft data sharing agreement template has been published by the Office of the National Data Commissioner (ONDC) for use under the Data Availability and Transparency (DAT) Bill. ABS data sharing documentation has been used to inform the template's development, and the ABS will look to align MADIP documentation with the DAT Bill data sharing agreement once it has been finalised.

Next Steps

Once enacted, the DAT Bill may become a method to share data for use in MADIP. Where possible, compatibility in government approaches to data sharing by further standardising and streamlining data sharing documentation will be beneficial. The MADIP agencies will continue to monitor the progress of the DAT Bill, and consider its potential application to MADIP.

Recommendation 4

The ABS should commit to undertaking a 2 yearly IRAP assessment of the MADIP operating environment as part of a regular program of audits of information security in MADIP.

MADIP Board response in November 2019

Agreed - The ABS has strong protections in place to safeguard the security of MADIP data. The ABS commits to a 2-yearly Information Security Registered Assessors' Program (IRAP) to ensure the currency of MADIP security measures. The next IRAP review will be conducted in 2020.

Action – Complete

The ABS has delivered on its commitment to 2-yearly IRAP reviews of the Secure Data Integration Environment (SDIE) in which MADIP data integration takes place. IRAP reviews are performed by a registered assessor to assess the implementation, appropriateness and effectiveness of the SDIE's security controls. Assessments are made against security requirements documented in the Australian Government Information Security Manual (ISM) issued by the Australian Signals Directorate (ASD).

The ABS SDIE was assessed most recently in July 2020 and found to be compliant.

Next Steps

The ABS will maintain its certification for the coming two years at which point it will be subject to the next assessment.

Recommendation 5

The ABS should finalise and implement the MADIP Data Retention and Destruction policy.

MADIP Board response in November 2019

Agreed – The ABS will present this policy to the MADIP Board for their approval by early 2020.

Action – Complete

The [MADIP Privacy Policy](#) incorporates a section on Security, Retention and Destruction of Information. This section outlines the ABS approach to data retention and destruction and the broader government framework in which the ABS is operating, such as the Australian Government records management regime. It states that personal information in MADIP is destroyed or deleted when no longer required, and all information in MADIP is retained by the ABS only while there is a business need to do so.

The ABS also routinely reviews access to integrated data that has been authorised for specific project purposes. Once a project is completed or a researcher no longer requires access, the access is revoked and project data is removed from the ABS DataLab. This is consistent with requirements for releases under Section 15 of the *Census and Statistics (Information Release and Access) Determination(2018)*.

Next Steps

While the [MADIP Privacy Policy](#) as described above broadly covers data destruction and retention for MADIP, the one element outstanding to meet Recommendation 5 involves finalising the process for data custodians to request their information in MADIP be destroyed, in line with the MADIP Privacy Policy's broad approach. Options will be presented to the MADIP Board to agree to the process in early 2021.

3. RESPONSE TO BEST PRACTICE SUGGESTIONS

The MADIP PIA Update identified 12 suggestions for enhancing privacy best practice for MADIP data practices. While the suggestions are framed around the relevant Australian Privacy Principles in Table 1 of the [MADIP PIA Update](#), this report will frame progress towards implementing the suggestions according to the themes of transparency, data sharing arrangements and the broader MADIP privacy framework. Full suggestions and the APPs to which they relate are listed in Table 2 of this report – *Summary of suggestions*.

Transparency

Increased transparency by way of publicly available online materials was a common theme for the following best practice suggestions:

- S1 – Update information on one-off linkages, source data and the governance process
- S2 – Seek advice from a range of sources for MADIP web content
- S3 – Update information on data minimisation and treatment of sensitive data
- S6 – Enhance material about managing unsolicited personal information
- S9 – Update and maintain public facing materials about data shared in MADIP
- S10 – Enhance information about data security protections

ABS has introduced a new website and is undertaking a phased program of updating information relating to data integration. This included updates to enhance the main data integration webpages with new and replaced content published in October 2020. An ongoing review of MADIP online materials will see the remaining suggestions rolled out across a variety of webpages by March 2021.

Data Sharing Arrangements

The arrangements and documentation for sharing data to use in MADIP was a common theme for the following best practice suggestions relating to APP4 and APP5.

- S4 – Support data custodians to identify and manage unsolicited personal information
- S5 – Support custodians to reduce the risk of unsolicited data being disclosed to the ABS
- S7 – Confirm custodians meet APP5 notification and APP6 authority for disclosure requirements when data is disclosed
- S8 – Update documentation to clarify how APP5 notification requirements are met by the ABS for data it collects for MADIP

A review of MADIP data sharing documentation is planned in early 2021 with a view to standardising approaches and documentation, including how APP requirements are documented.

Privacy Framework

The two final suggestions do not relate to any specific APPs and were provided as additional considerations for the broader privacy framework under which MADIP operates. These are:

- S11 – Establish threshold triggers for future MADIP PIA updates
- S12 – Leverage government consultation mechanisms for broad advice on MADIP privacy issues and ethics

The ABS is currently developing a standard template for Privacy Threshold Assessments relating to ABS data integration activity. This purpose of the template is to increase consistency in the approach to Threshold Assessments and streamline processes across the ABS. A standard Privacy Threshold Assessment template would also be applied to MADIP as a mechanism to trigger future PIA updates. The development of this template will draw upon the new OAIC guidance on [conducting threshold assessments](#).

The ABS takes a privacy-by-design approach to its data integration infrastructure and management framework in order to manage privacy risks. The ABS regularly reviews the MADIP arrangements and actively engages external privacy expertise to assist in navigating data integration scenarios outside of the current MADIP arrangements.

4. NEXT STEPS

The ABS protects the privacy of data providers and is committed to keeping information safe and secure. MADIP has expanded since its inception and continues to evolve as new data is integrated, and in some instances as new practices are adopted. The standard practice of conducting Privacy Threshold Assessments for all data integration projects, with a particular focus on new types of data and changed data handling practices and where necessary conducting or updating PIAs ensures privacy impacts are identified and managed appropriately.

As a recent example, the ABS conducted a PIA about the integration of jobs related data with MADIP to inform analysis of key employment data. A [summary of the PIA](#) was published in September 2020.

The ABS will continue to monitor changes in MADIP and consider conducting a further update to the MADIP PIA towards the end of 2021.