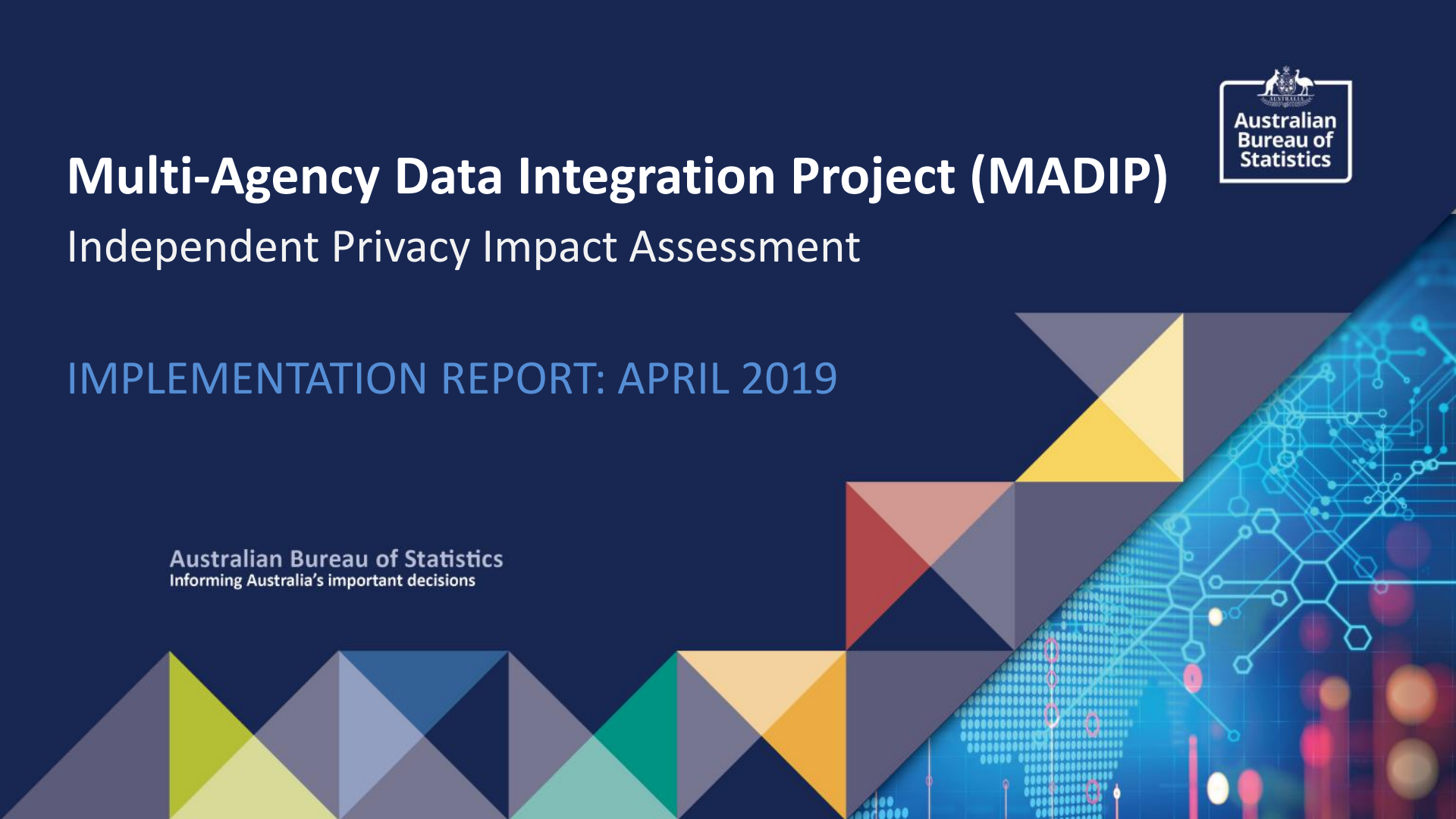
Multi-Agency Data Integration Project (MADIP)

Independent Privacy Impact Assessment

IMPLEMENTATION REPORT: APRIL 2019

Australian Bureau of Statistics
Informing Australia's important decisions



Implementation of the recommendations in the independent Privacy Impact Assessment (PIA)

April 2018 – April 2019

Overview

On behalf of partner agencies, the ABS commissioned an independent PIA of the Multi-Agency Data Integration Project (MADIP). The independent PIA identified privacy impacts of the project and outlined strategies to mitigate any residual privacy risks, to prepare for the project becoming operational on 1 July 2018.

The independent PIA was published on the ABS website on **4 April 2018**, along with the MADIP agencies' response to each of the recommendations of the report.

This **Implementation Report** presents the progress made against each of the recommendations since the publication of the independent PIA.

The MADIP agencies are committed to upholding the privacy, secrecy, and security of personal information, and to being transparent and open about the project.

Snapshot of recommendations from the MADIP independent PIA

1. Improve openness online about data in MADIP
2. Improve openness about data sources
3. Minimise data sharing
4. Review and minimise the amount of sensitive data
5. Amend ABS privacy notices to clarify scale of third party data acquisition
6. Amend other MADIP agencies' privacy notices to clarify scale and nature of third party data sharing
7. Amend all MADIP agencies' privacy notices to describe data sharing with MADIP as a secondary purpose
8. In future, data sharing governance (e.g. Public Interest Certificates) should differentiate between personal information and sensitive information. The legal basis for and public interest in data sharing should be clearly disclosed to the public.
9. Mandate regular independent security risk assessments for MADIP
10. Consider alternative data sharing models on an ongoing basis
11. Impose the highest possible security standards to match the risk profile of data
12. Consider data retention and destruction requirements
13. Publish detailed information on access request process (i.e. for individuals to access their personal information)
14. Strengthen and enhance MADIP governance arrangements

1. Improve openness online about data in MADIP

Recommendation 1

The ABS should amend the MADIP website to indicate personal information is used by MADIP for statistical and research purposes, including data integration. A list of the linkage and analytical data variables could also be provided.

MADIP agencies' response in April 2018: Agreed. ABS is in the process of reviewing and updating MADIP content on the ABS website to provide more information and increase transparency. This includes providing more detail about the kinds of data in MADIP, the legal basis for MADIP, and how the data is used by government entities and researchers.

STATUS: Complete

ACTION TAKEN: MADIP web portal updated

A suite of online information (available through the MADIP homepage) provides detail about the project, the data involved (such as types of personal information as well as data sources) and data management.

Key webpages include:

MADIP data and legislation

The MADIP data and legislation page provides information about:

- The data involved in MADIP
- The types of information shared for MADIP
- The legal basis for the project

MADIP Research Projects

The MADIP Research Projects page presents information about approved research projects that use MADIP data.

Next Steps: The MADIP agencies will continue to improve project transparency, and online information will be reviewed and updated periodically to reflect changes to the project (such as the addition of new data).

2. Improve openness about data sources

Recommendation 2

The ABS may wish to amend publicly available information and relevant Privacy Policies to be more open about the collection of data from agencies and the datasets being integrated in MADIP.

MADIP agencies' response in April 2018: Agreed. ABS is updating the ABS and Census Privacy Policies to clarify data is shared and used for research and statistical purposes through data integration projects. A MADIP Privacy Policy is being developed to outline how personal information is handled in the MADIP.

STATUS: Complete

ACTION TAKEN: ABS and Census Privacy Policies

The ABS has updated the Census Privacy Policy to clarify that personal information is used for data integration purposes. The summary and main ABS Privacy Policies are being reviewed to ensure content is up-to-date and reflective of contemporary use of personal information; updated content will be published later in 2019.

ACTION TAKEN: MADIP Privacy Policy published

A MADIP Privacy Policy has been developed to outline how personal information is handled in MADIP.

The MADIP Privacy Policy was published on the ABS website on **29 June 2018**.

Key information that can be found in the MADIP Privacy Policy includes information about:

- The authority of the MADIP agencies to share personal information.
- The personal information that is used in MADIP.
- The management of and access to personal information.
- Confidentiality.
- Security, retention, and destruction of information.
- Accessing and correcting personal information.
- How to make a privacy complaint.

Next Steps: The MADIP, ABS, and Census Privacy Policies will be reviewed periodically to ensure information is up-to-date and accurate.

3. Minimise data sharing

Recommendation 3

MADIP governance arrangements and public material should clarify that data minimisation occurs both during data sharing and data access for authorised researchers. MADIP should enhance the minimisation of personal data sharing by:

1. Only sharing data items that are reasonably necessary.
2. Excluding irrelevant data items where possible.
3. Using data categorisation (e.g. Yes / No responses or bands) rather than specific data fields where possible.

MADIP agencies' response in April 2018: Agreed. Data minimisation (including data categorisation) is a key feature of the MADIP. Data custodians (the agencies responsible for collecting data shared in MADIP) only share data necessary for use in MADIP. Access to MADIP data assets is only provided to the data necessary for an authorised purpose, such as particular statistical or research projects. These arrangements are consistent with the High Level Principles for Commonwealth Data Integration under which the project is conducted.

Where appropriate MADIP partner agencies will aim to use data categorisation (e.g. yes/no responses or bands) rather than specific data fields.

However, partner agencies recognise in many cases researchers will require broader data fields when making use of the de-identified analytical data provided under MADIP. In this context, where MADIP partner agencies provide access to broader fields of data, they are committed to sharing this data in a secure and safe way to ensure that the privacy, secrecy, and security of that data is maintained.

STATUS: Complete

ACTION TAKEN: Update of governance and online materials

Online materials now clarify what data is in MADIP, the legislative basis for data sharing, as well as the fact that data minimisation occurs during both data sharing and access. The latter point is also being clarified in governance materials used by the MADIP agencies to guide data sharing, use, and access.

MADIP data and legislation

The MADIP data and legislation page provides information about:

- The data involved in MADIP
- The types of information shared for MADIP
- The legal basis for the project

Next Steps: Data custodians will continue to minimise personal data sharing and only share data necessary for use in MADIP. Online materials and governance documentation will be reviewed periodically.

4. Review and minimise the amount of sensitive data

Recommendation 4

MADIP should implement a review of all sensitive data fields to assess whether it is reasonably necessary to acquire sensitive data. Unnecessary data fields should be removed from future data acquisition and deleted/quarantined from existing MADIP data holdings.

MADIP agencies' response in April 2018: Agreed. ABS manages all data acquired by MADIP consistent with the processes required when handling personal information. When providing public access to this data, ABS is legally obliged to ensure no individual is reasonably identifiable from the data remaining after the de-identification process. Public access is only given to the data necessary for each authorised project.

Consultation with users confirms all data included in MADIP is important for a range of research and statistical purposes.

STATUS: Complete

ACTION TAKEN: Review of sensitive data

The ABS has conducted a review of sensitive data in MADIP. To implement this review, MADIP agencies will:

- Minimise data sharing so that only data that are necessary for the purposes of the project are shared and used in MADIP.
- Use categorised or derived indicators for sensitive data items where this is feasible and unless sensitive data items in their original form are required for statistical or analytical purposes.
- Revise MADIP project proposals to require justification for requesting sensitive data items (including level of detail requested), and data custodian sign-off to approve access to these along with the general approval for the project.
- Review the retention of sensitive information where there is no compelling business case for retention, or by agreement between ABS and the relevant data custodian.

The ABS will continue to ensure data are stored and accessed in secure environments which have been audited to ensure appropriate levels of security. The Separation Principle and Five Safes Framework are used to manage the risks associated with providing information (sensitive or otherwise) to authorised users of MADIP data.

Next Steps: The outcomes of the review of sensitive information in MADIP will be implemented through the MADIP Operating Model. The ABS and relevant data custodians will review the need to retain information (including sensitive information) in MADIP every year, or more frequently as appropriate.

5. Amend ABS privacy notices to clarify scale of third party data acquisition

Recommendation 5

To deliver best practice in openness and transparency, the ABS may wish to review and amend privacy notices to clarify the scale of third party data acquisition, the use of automated and bulk third party data acquisition and the expanded list of third parties that are involved.

MADIP agencies' response in April 2018: Agreed. ABS is reviewing its privacy notices (such as online and on data collection forms) to clarify that information may be shared and used for research and statistical purposes consistent with legislation including the *Census and Statistics Act 1905*.

Detail on the scale of data shared is out of scope of these privacy notices and is provided in other information publicly available about MADIP.

MADIP operates in accordance with the High Level Principles for Commonwealth Data Integration, including minimising the data that is shared.

Data sharing for MADIP is not an automated process and does not involve entire datasets: agencies agree to share data pursuant to a specific request(s), and provide a subset of population-based data items which are reasonably necessary for MADIP. This approach has been undertaken as part of MADIP partner agencies' commitment to ensure privacy considerations are reflected in the continued development of the project, ensuring a 'privacy by design' approach.

STATUS: Complete

ACTION TAKEN: Review of privacy notices

The ABS is reviewing and subsequently updating its privacy notices to clarify that information may be used for research and statistical purposes, such as data integration, consistent with legislation including the *Census and Statistics Act 1905 (Cth)*.

Updates to privacy notices for ABS household surveys are being rolled out. The Survey of Disability Aging and Carers 2018/19 was the first out in the field to include the updated privacy notice with reference to data integration.

The privacy notice wording for the 2021 Census is being developed and will include references that Census information may be used for research and statistical purposes, including data integration.

Online materials for MADIP provide information about the scale of data shared to supplement the information provided in privacy notices.

Next Steps: The ABS will continue to review its privacy notices to ensure they clarify how data may be shared and used, such as through data integration.

6. Amend other MADIP agencies' privacy notices to clarify scale and nature of third party data sharing

Recommendation 6

To deliver best practice in openness and transparency, MADIP Partner agencies may wish to review and amend privacy notices to clarify the scale and detail of disclosure to the ABS for MADIP and the use of automated and bulk data sharing.

MADIP agencies' response in April 2018: Agreed. Detail on the scale of data shared is out of scope of these privacy notices and is provided in other information publicly available about MADIP. MADIP agencies note data sharing for MADIP is not an automated process and does not involve entire datasets: agencies agree to share data pursuant to a specific request(s), and provide a subset of population-based data items which are reasonably necessary for MADIP.

STATUS: Finalising

ACTION TAKEN:

- The Department of Education and Training has updated its departmental privacy statement to include that personal information is disclosed to the ABS for MADIP.
- The Department of Human Services departmental short form privacy notice recognises that personal information may be used for research purposes. A revision to the Privacy Policy is in progress to explicitly recognise data sharing with the ABS, including for MADIP.
- The Department of Social Services has specified in its Privacy Policy that it collects data for a variety of different purposes including policy development, research, and evaluation.
- The Australian Taxation Office and the Department of Health are reviewing their privacy notices and are actively considering the implementation of amendments.

Next Steps: MADIP agencies will finalise the review and necessary amendments to privacy notices to ensure best practice in openness and transparency. MADIP agencies will continue to review privacy notices to ensure information is current and relevant as the project evolves.

7. Amend all MADIP agencies' privacy notices to describe data sharing for MADIP as a secondary purpose

Recommendation 7

To deliver best practice in openness and transparency, MADIP Partner agencies may wish to consider amending privacy notices at the point of collection, as well as other public information, to indicate that data may be shared and used for statistical and research purposes, including data integration.

MADIP agencies' response in April 2018: Agreed. MADIP agencies are considering updating relevant privacy notices to clarify that information may be shared and used for research and statistical purposes. These updates (covered in our response to Recommendations 5 and 6) are relevant for the sharing and use of data in MADIP for both primary and secondary purposes in accordance with the *Privacy Act 1988*.

STATUS: Finalising

ACTION TAKEN:

Four MADIP agencies have reviewed and/or amended their privacy notices to describe data sharing for MADIP as a secondary purpose of collection. Two MADIP agencies are actively considering this recommendation.

- The Department of Education and Training has updated its departmental privacy statement to include that personal information is disclosed to the ABS for MADIP.
- The Department of Human Services departmental short form privacy notice recognises that personal information may be used for research purposes. A revision to the Privacy Policy is in progress to explicitly recognise data sharing with the ABS, including for MADIP.
- The Department of Social Services has specified in its Privacy Policy that it collects data for a variety of different purposes including policy development, research and evaluation.
- The Australian Taxation Office and the Department of Health are reviewing their privacy notices and are actively considering the implementation of amendments.
- See Recommendation 5 for action taken by the ABS.

Next Steps: MADIP agencies will finalise the review and necessary amendments to privacy notices to ensure best practice in openness and transparency. MADIP agencies will continue to review privacy notices to ensure information is current and relevant as the project evolves.

8. In future, data sharing governance should differentiate between personal information and sensitive information

Recommendation 8

To deliver best practice in data management, MADIP Partner agencies may wish to consider differentiating between general personal information and sensitive information in future Public Interest Certificates issued for MADIP. The asserted legal basis / public interest in sharing and integrating sensitive information in MADIP should be clearly disclosed to the public.

MADIP agencies' response in April 2018: Agreed. ABS is currently updating publicly available information to clearly outline the legal basis for MADIP. A number of MADIP partner agencies already clearly list personal information and sensitive personal information variables in their Public Interest Certificates (PICs).

However, partner agencies agree where they have capacity to do so, they will strengthen approaches to differentiating between personal information and sensitive information in PIC arrangements.

STATUS: Finalising

ACTION TAKEN:

Data sharing agreements:

- The Department of Education and Training explicitly identified authorising legislation and personal and sensitive information being shared to the ABS for MADIP in recent data sharing agreements and are committed to keep providing this information in the future.
- The ABS has updated its data sharing agreements for MADIP to require that data custodians identify personal and sensitive data items and note the legal basis for sharing data to the ABS.

Public Interest Certificates:

- The Department of Social Services lists all analytical data items provided to the ABS for MADIP on the ABS website and lists the data items approved to be provided for each project in Public Interest Certificates. The Department also states the legislation under which the data is provided and the reason for providing access to the data.
- This recommendation is under active consideration by the Department of Health.

Publicly available information:

- The MADIP Data and Legislation webpage has been updated to outline the legal basis for MADIP.

Next Steps: MADIP agencies will periodically review and discuss differentiation between personal information and sensitive information as data management best practice evolves.

9. Mandate regular independent security risk assessments for MADIP

Recommendation 9

The ABS should commission regular independent security risk assessments for MADIP. The reviews should establish minimum security standards for all data sharing and require further independent security risk assessments for any new data exchanges.

MADIP agencies' response in April 2018: Agreed. ABS has strong data security measures in place to safeguard MADIP data.

ABS has commissioned an independent Information Security Registered Assessors' Program (IRAP) review of MADIP. Pending the outcomes of this assessment, ABS will consider recommendations to improve the security of information in MADIP, including regular independent assessments.

STATUS: Complete

ACTION TAKEN:

In June 2018, an assessor accredited by the Australian Signals Directorate (ASD) evaluated the data linkage environment used for MADIP as part of an Information Security Registered Assessors Program (IRAP). The ABS Data Linkage Centre was certified as being compliant with the Government's Information Security Manual (ISM).

The ABS is updating the MADIP Operating Model so that it includes the requirement to commission periodic independent and internal security risk assessments.

Next Steps: The ABS will commission periodic internal and independent security risk assessments of its data linkage environment.

10. Consider alternative data sharing models on an ongoing basis

Recommendation 10

MADIP should consider alternative data sharing models on an ongoing basis. The current data centralisation model should be the subject of constant evaluation against alternatives such as a federated model. These evaluations should assess the comparative security risk profile of each model (amongst other factors).

MADIP agencies' response in April 2018: Agreed. MADIP operates under a centralised data sharing model in which data is shared for the project and stored securely by an Accredited Integrating Authority, the ABS, for linkage and creation of analytical datasets necessary for statistical and research purposes. Within ABS, this is not a pure centralised model, as datasets are stored separately, and personal information is also stored separately from analytical information to reflect best practice in security and available technology.

One alternative data sharing model is a federated system where subsets of data are extracted by data custodians and linked by an Accredited Integrating Authority like the ABS in a secure web-based environment e.g. via cloud technology. As advised by experts, this data sharing model is not feasible in the current technical environment. MADIP agencies will consider whether other data sharing models (including federated models) are appropriate, present lower security risks, and are viable as MADIP evolves.

STATUS: Complete

ACTION TAKEN:

The ABS has developed a secure privacy-preserving linkage infrastructure for MADIP. The analytical information of the individual datasets in MADIP (e.g. Census, Medicare Benefits Schedule) are stored separately from each other. They are only assembled into products and extracts as required. Personal information, such as name and address, is stored separately from analytical information at all times in line with the Separation Principle.

As MADIP evolves, the ABS and MADIP agencies will consider whether other data sharing models (including federated models) are appropriate, present lower security risks, and are viable.

The ABS is updating the MADIP Operating Model to state that periodic assessments of the MADIP data model and potential viable alternatives will occur.

Next Steps: The MADIP agencies are developing a strategy to take the project forward which will consider future possible data models.

11. Impose the highest possible security standards to match the risk profile of data

Recommendation 11

MADIP should impose security standards consistent with the Australian Government Information Security Manual and the Protective Security Framework on data sharing arrangements, to reflect the sensitivity and scale of the data being exchanged.

MADIP agencies' response in April 2018: Agreed. MADIP agencies are committed to keeping data secure, and will continue to manage data in accordance with legislative requirements and Australian Government standards including the Information Security Manual and Protective Security Policy Framework.

STATUS: Complete

ACTION TAKEN:

MADIP agencies are committed to keeping data secure, and will continue to manage data in accordance with legislative requirements and Australian Government standards including the Information Security Manual and Protective Security Policy Framework.

In June 2018, an assessor accredited by the Australian Signals Directorate (ASD) evaluated the data linkage environment used for MADIP as part of an Information Security Registered Assessors Program (IRAP). The ABS Data Linkage Centre was certified as being compliant with the Government's Information Security Manual (ISM).

Next Steps: The ABS will commission periodic internal and independent security risk assessments of its data linkage environment.

12. Consider data retention and destruction requirements

Recommendation 12

MADIP should continue to review its approach to data retention and destruction.

MADIP agencies' response in April 2018: Agreed. The need to retain data for MADIP is considered annually by the Accredited Integrating Authority, the ABS, in consultation with the other MADIP agencies. A retention and destruction policy is being developed for MADIP which clarifies this current practice.

STATUS: Complete

ACTION TAKEN:

The ABS has conducted a review of data retention and destruction in MADIP. An updated data retention and destruction policy will be implemented through the MADIP Operating Model.

This policy notes the following:

- The accredited Integrating Authority and data custodians will review the need to retain information in MADIP every year, or more frequently as appropriate.
- Information will be destroyed when there is no compelling business case for retention, or by agreement between the relevant data custodian and the accredited Integrating Authority.

Next Steps: The ABS and data custodians will continue to review data retention and destruction policies as MADIP evolves.

13. Publish detailed information on access request process (i.e. for individuals to access their personal information)

Recommendation 13

The MADIP Agreement, the MADIP website and relevant privacy policies should provide detail on the MADIP Access request process. Note: these access requests do not relate to the process of accessing analytical information for research, as this information is de-identified.

MADIP agencies' response in April 2018: Agreed. MADIP agencies provide information about how people can access their personal information through their privacy policies. ABS is updating its website and MADIP governance materials to explain how individuals can apply to access their personal information in MADIP.

STATUS: Complete

ACTION TAKEN:

The MADIP agencies already have well established, publicly available procedures for individuals to apply for access to their personal information held by each agency:

- Australian Bureau of Statistics
- Australian Taxation Office
- Department of Education and Training
- Department of Health
- Department of Human Services
- Department of Social Services

The MADIP Privacy Policy, general online materials (e.g. the MADIP FAQs), and governance resources have been updated to provide information on how individuals can apply to access or correct their personal information.

Next Steps: The MADIP agencies will periodically review governance documentation and published materials to ensure information is up-to-date and accurate.

14. Strengthen and enhance MADIP governance arrangements

Recommendation 14

The ABS and MADIP Partner agencies need to continually review, strengthen, and enhance the MADIP governance framework, including:

- Legal basis/Public Interest Certificates
- Register of agreements
- Data minimisation
- Limits on the use of data
- Data quality assessment
- Minimum security requirements
- Compliance audits

MADIP agencies' response in April 2018: Agreed. The MADIP Agreement and other governance materials (such as data sharing agreements) already provide a strong foundation for the project, and outline the legal basis for data sharing and use, permissible uses of data, and data security requirements.

MADIP agencies will consider updating governance materials to provide more specific detail, and to address other recommendations from the iPIA to improve transparency.

STATUS: Complete

ACTION TAKEN:

The ABS, in collaboration with MADIP partner agencies, is revising governance arrangements for the project including the development of a strategy to take the project forward as the data asset and the environment it operates in evolve.

Governance resources and communications materials are being updated in accordance with this and other recommendations (e.g. to more clearly set out principles of data management such as data minimisation, and to establish timeframes for review of the data model). Content is being clarified to specify the authorised uses of MADIP data, the legal basis for data sharing, data quality, and data security.

Next Steps: The MADIP agencies will review project and data governance, including governance documentation, on an annual basis.


Australian
Bureau of
Statistics