Response to the independent Privacy Impact Assessment of MADIP

April 2018

The Multi-Agency Data Integration Project, or MADIP, is a partnership among Australian Government agencies to explore how to make better use of existing public data consistent with the Public Data Policy Statement.

On behalf of partners, the ABS commissioned an independent Privacy Impact Assessment (iPIA) of MADIP. The iPIA identifies privacy impacts of the project and outlines strategies to mitigate any residual privacy risks before the project moves into an operational phase from 1 July 2018.

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

To date, MADIP has tested the feasibility and value of combining important national datasets to create a comprehensive picture of Australia for research and statistical purposes, including to support policy analysis, decision making, and service delivery in Australia by governments at all levels.

The iPIA acknowledges there are strong measures in place to protect privacy for MADIP, including legislative safeguards, application of the separation principle, and restricting the use of data to research and statistical purposes which benefit the Australian community.

The iPIA identifies some areas for improvement and provides strategies for managing, minimising, or eliminating residual privacy risks. MADIP partners agree to the iPIA's recommendations and have commenced work to address issues raised in the iPIA.

RESPONSE TO IPIA

RECOMMENDATIONS

R1. Improve openness online about data in the MADIP.

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.

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.

R2. Improve openness about data sources.

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.

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.

R3. Minimise data sharing.

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.***

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.

R4. Review and minimise the amount of sensitive data.

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.

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.

R5. Amend ABS privacy notices to clarify scale of third party data acquisition.

To deliver best practice in openness and transparency, 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.

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.

R6. Amend other MADIP agencies' privacy notices to clarify scale and nature of third party data sharing.

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.

Agreed.

MADIP agencies other than ABS are considering updating relevant privacy notices to clarify the nature of data sharing and use is for research and statistical purposes.

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.

R7. Amend all MADIP agencies' privacy notices to describe data sharing for the MADIP as a secondary purpose.

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.

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*.

R8. 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.

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 the MADIP. The asserted legal basis / public interest in sharing and integrating sensitive information in MADIP should be clearly disclosed to the public.

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.

R9. Mandate regular independent security risk assessments for MADIP.

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.

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.

R10. Consider alternative data sharing models on an ongoing basis.

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).

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.

R11. Impose the highest possible security standards to match the risk profile of data.

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.

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.

RESPONSE TO IPIA

R12. Consider data retention and destruction requirements.

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

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.

R13. Publish detailed information on access request process (i.e. for individuals to access their personal information).

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.

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.

R14. Strengthen and enhance MADIP governance arrangements.

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

- ***A. Legal basis / Public Interest Certificates***
- ***B. Register of agreements***
- ***C. Data minimisation***
- ***D. Limits on the use of data***
- ***E. Data quality assessment***
- ***F. Minimum security requirements***
- ***G. Compliance audits***

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.