galexia

Australian Bureau of Statistics (ABS)

Independent Privacy Impact Assessment (PIA) on the National Health Survey (NHS) Linkage Project

30 July 2018 (GC514)

Contact: Galexia
Level 11, 175 Pitt Street, Sydney NSW 2000
ABN: 72 087 459 989
Ph: +61 2 9660 1111
www.galexia.com
Email: manage@galexia.com

Document Control

Client

This document has been written for the Australian Bureau of Statistics (ABS).

Document Purpose

This document is an Independent Privacy Impact Assessment (PIA) examining the privacy considerations around the National Health Survey (NHS) Linkage Project.

Document Identification

Document title	ABS NHS Linkage Independent Privacy Impact Assessment (PIA)
Document filename	gc514_ABS_NHS_linkage_PIA_2018_v5_20180730_FINAL.pdf

Client Details

Australian Bureau of Statistics (ABS) <www.abs.gov.au>
ABS House
Ground Floor
45 Benjamin Way
Belconnen ACT 2617

Consultant Details

Consultant Contact **Galexia** <www.galexia.com>
Level 11, 175 Pitt Street, Sydney NSW 2000
Phone: +612 9660 1111
Email: manage@galexia.com

Peter van Dijk (Managing Director)
Mobile: +61 419 351 374 (Peter van Dijk)

Document Authors Galexia (Chris Connolly and Peter van Dijk were the principal consultants)

Reference	GC514
Project Email	absnhs@galexia.com

Copyright

Contents

1. Executive Summary

Galexia has been commissioned by the Australian Bureau of Statistics (ABS) to prepare an Independent Privacy Impact Assessment (PIA) examining the privacy considerations around the National Health Survey (NHS) Linkage Project.

The purpose of this PIA is to assist in identifying and managing privacy issues that are raised by the proposed integration of data between the 2014-15 NHS[1] and MADIP (Multi-Agency Data Integration Project[2]).

This PIA has found that the NHS Linkage Project is largely compliant with the Australian Privacy Principles (APPs) and has made a small number of recommendations to further strengthen existing privacy safeguards and governance arrangements.

1.1. Approach and Scope

The PIA process is being conducted in accordance with *PIA Guidelines* issued by the Office of the Australian Information Commissioner (OAIC). The ABS has agreed to publish the PIA as part of their ongoing consultation with stakeholders and the community.

The key proposals in the NHS Linkage Project are to:

1. Link the 2014-15 NHS data with a range of other data held in MADIP to facilitate research and statistical analysis; and
2. Create an effective governance framework for the proposed data linking.

Information contained in this PIA is based on:

- Meetings with ABS, including senior management, technical staff, legislation and policy staff and the data linkage centre team;
- Meetings with external stakeholders, notably the Office of the Australian Information Commissioner (OAIC), several health research organisations and one consumer advocacy stakeholder (further details included in Appendix 1 – Stakeholder Consultation);
- Documentation related to the proposal;
- General research and literature review on privacy and data integration issues; and
- Review of relevant privacy legislation and guidelines.

Galexia's advice in this PIA concentrates on the following areas:

- **Privacy legislation compliance**
  The PIA assesses the proposed sharing of data (for research and statistical purposes) against the Australian Privacy Principles (APPs) in the Commonwealth *Privacy Act*;
- **Practical measures to address privacy**
  The PIA identifies several practical measures that can be taken to manage privacy issues; and
- **Governance**
  The PIA considers key privacy governance steps that could be implemented to ensure the ongoing protection of privacy once the data integration arrangements are operational.

[1] <www.abs.gov.au/ausstats/abs@.nsf/PrimaryMainFeatures/4363.0>.

[2] <www.abs.gov.au/madip>.

1.2. Australian Privacy Principle (APP) Compliance Summary

The PIA assesses the National Health Survey (NHS) Linkage Project against the APPs in the *Privacy Act*.

The following table summarises the main findings, with links to further information and detailed discussion in the body of the report:

Australian Privacy Principle (APP)	Compliance Status	Galexia Commentary	Galexia Recommendation
APP 1 – Openness and Transparency	**Compliant**	The proposed linking of the 2014-15 NHS data set with MADIP is a new procedure. APP 1 requires the ABS to be open and transparent about the use and disclosure of data. There are no specific references to data linking, data integration or MADIP in the ABS Privacy Policy. However, detailed information on data integration is provided in the MADIP Privacy Policy and the ABS' data integration web-pages. The ABS online resources regarding the NHS will also be updated once the NHS Linkage Project proceeds. **Note:** There is a further discussion of potential governance arrangements to assist in privacy compliance in Section 3 of this PIA (below).	
APP 2 – Anonymity and Pseudonymity	**Compliant**	The ABS provides limited anonymity to general web site visitors. Respondents in the NHS survey understand that they are participating in a survey, and have the option of not providing their names if they prefer. All of the other data collected and linked by the ABS for the NHS Linkage Project is covered by exceptions to the anonymity principle.	

APP 3 – Collection of solicited personal information	**In progress**	APP 3 requires agencies to only collect data that is 'reasonably necessary'. The necessity of data collection needs to be assessed for each proposed collection by the ABS. In 2018 the OAIC advised that 'collection' includes the creation of new data sets via data linking projects – and this may apply to some aspects of the linking of NHS to MADIP. Data minimisation requirements will be incorporated at both the point of linking the data and the point of providing research access to the linked data. However, the ABS should be permitted some flexibility in order to allow exploratory testing / evaluation of data integration without data minimisation (e.g. trials or pilots in order to ensure the best possible linking quality). The other requirements of APP 3 can be met by reliance on the exceptions that apply where data collection is authorised by a specific law. While there is no dedicated specific legislation for the NHS or MADIP, the linkage of data with MADIP is authorised by ABS legislation (and further legislation specific to other MADIP Partner Agencies).	**Recommendation 1: Minimisation of data collection** The NHS Data Linkage Project should require the minimisation of personal data collection at both the initial data linking stage and the research access stage. Data minimisation should include: 1. Only linking and sharing data fields that are necessary 2. Excluding irrelevant data subjects where possible 3. Using data verification rather than detailed data collection where possible. The data minimisation requirements should not apply to trials or pilots designed to evaluate data linking quality.
APP 4 – Dealing with unsolicited personal information	**Compliant**	The ABS is already fully compliant with APP 4. The NHS Data Linkage Project is unlikely to have an impact on APP 4 compliance.	

APP 5 – Notification	**In progress**	The ABS uses a mix of correspondence and forms to provide notice of privacy issues to NHS participants. These forms are compliant with many of the requirements of APP 5. However, the NHS notices were provided to respondents between July 2014 and June 2015 – prior to the decision to link NHS data to MADIP. The privacy notices[3] do inform consumers that their data will be used for research and statistical purposes – so the linking with MADIP is not a complete 'repurposing' of their data. However, the notices are silent on the general concept of data integration. The notices were accurate 'at or around the time of collection' so the notices comply with APP 5. However, the absence of any mention of data integration does cause some concerns regarding appropriate privacy practice and the best way to ensure that participants remain confident in the use of their NHS data. Overall, the notices are sufficient for linking the 2014-15 NHS, subject to general strengthening of other privacy protections (especially APP 1 and APP 3). However, improvements should be made to future privacy notices for the NHS.	**Recommendation 2: Amend privacy notices to clarify the role of data integration** NHS privacy notices should be reviewed and amended to clarify the role of data integration.
APP 6 – Use or Disclosure	**Compliant**	The APP 6 provisions that allow the use and disclosure of data where this type of use is 'authorised by a law' are sufficient to achieve compliance for linking NHS and MADIP data.	
APP 7 – Direct Marketing	**Compliant**	Direct marketing is not applicable in this PIA.	
APP 8 – Cross Border Disclosure	**Compliant**	Cross border data transfers are not relevant to the NHS Data Linkage Project. They have not been considered in detail in this PIA.	
APP 9 – Government Related Identifiers	**Compliant**	APP 9 does not apply to Agencies unless they are undertaking prescribed commercial activities. APP 9 is not applicable in this PIA.	
APP 10 – Quality of Personal Information	**In progress**	The NHS Data Linkage Project may have an impact on linked data quality. The ABS may need to undertake trials and pilot data linkages to assess the accuracy of data linking. The ABS is already planning an initial trial.	**Recommendation 3: Assess data quality benefits and risks** The NHS Data Linkage Project should be subject to an initial evaluation / assessment regarding the potential data quality benefits and risks.

[3] Note: In this PIA we refer to the ABS survey respondent communications as 'privacy notices'. The ABS does not use the term 'privacy notice', but it is a generic term that is used in PIAs to cover any section in communications that informs users about their privacy rights.

APP 11 – Security	**Compliant**	The data being exchanged in the NHS Data Linkage Project includes sensitive data. The scale of the data involved is also significant. It will be important for security settings to match the potential harm of any breaches. The ABS data linkage environment has recently been upgraded and has been independently reviewed and assessed as providing an appropriate level of security.	
APP 12 – Access	**Compliant**	The ABS has access policies and procedures in place that are fully compliant with APP 12. The NHS Linkage Project does not have a significant impact on Access requests under APP 12.	
APP 13 – Correction	**Compliant**	The ABS has correction policies and procedures in place that are fully compliant with APP 13. The NHS Linkage Project does not have a significant impact on correction requests under APP 13.	
Governance		The NHS Linkage Project needs to comply with a variety of requirements contained in: – Privacy legislation (the APPs) – ABS legislation – The MADIP Operating Model It is also important to continually address issues that may arise from public expectations or perception issues that are associated with such a large, high profile, high risk project. NHS Linkage Governance will fall under MADIP Governance arrangements.	**Recommendation 4: Strengthen and enhance NHS Linkage Project Governance arrangements** The ABS need to continually review, strengthen and enhance the NHS Linkage Project governance framework, including: **A.** Data minimisation **B.** Minimum security requirements and assessments **C.** Compliance audits

1.3. Suggested Future Work Plan

A suggested future work plan for the ABS, based on the recommendations in this PIA, is set out in the following table. The ABS can allocate the appropriate person to take responsibility for each action item, and can establish procedures for verifying that the issues have been addressed.

Priority Legend	High	Medium	Low

APP	Recommendation	Action Required	Agency responsible	Priority
APP 3 – Collection of solicited personal information	**Recommendation 1:** Minimisation of data collection	Clarify that data minimisation occurs in the data linkage as well as research access stages.	ABS	Medium
APP 5 – Notification	**Recommendation 2:** Amend privacy notices to clarify the role of data integration	NHS privacy notices to be reviewed and amended to clarify the role of data integration.	ABS	Medium
APP 10 – Quality of Personal Information	**Recommendation 3:** Assess data quality benefits and risks	Initial evaluation / assessment to be undertaken on the accuracy of the proposed data linking.	ABS	Medium
Governance	**Recommendation 4.** Strengthen and enhance NHS Linkage Governance arrangements	Ongoing review to strengthen and upgrade some governance arrangements.	ABS	Low

2. Scope and Methodology

Galexia has been commissioned by the Australian Bureau of Statistics (ABS) to prepare an Independent Privacy Impact Assessment (PIA) examining the privacy considerations around the National Health Survey (NHS) Linkage Project.

The purpose of this PIA is to assist in identifying and managing privacy issues that are raised by the proposed integration of data between the 2014-15 NHS and MADIP (Multi-Agency Data Integration Project[4]). While NHS is a point in time (in this case collection took place between July 2014 and June 2015), MADIP data is longitudinal.

The key proposals are to:

1. Link the 2014-15 NHS data with a range of other data held in MADIP to facilitate research and statistical analysis; and
2. Ensure an effective governance framework for the proposed data integration (noting that NHS Linkage Governance will fall under MADIP Governance arrangements).

This PIA does not:

- Cover the data activities of ABS as a whole;
- Cover other individuals whose personal information may be collected and handled in the context of the project (e.g. personal information about researchers who apply for data access); or
- Consider State or Territory privacy laws, or compliance by researchers with applicable privacy laws or secrecy provisions.

2.1. Scope

The scope of the overall PIA is limited to the following items:

In Scope	Out of Scope
• Assessment of the project (i.e. linking the 2014-15 NHS to MADIP) against the Australian Privacy Principles.	• All other ABS surveys • Biomedical collections • Social licence or building community trust
• Review of a small number of key documents	• Review of the entire suite of ABS documentation
• Limited stakeholder consultation consisting of selected internal and external stakeholders	• Extensive public consultation, open invitation consultation, detailed assessment of public attitudes etc.
• Very high level identification and review of legal documentation	• Detailed legal advice
• Brief consideration of security issues relevant to privacy compliance	• Detailed security assessment

[4] <www.abs.gov.au/websitedbs/D3310114.nsf/home/Statistical+Data+Integration+-+MADIP>.

2.2. PIA Guidelines

The Independent PIA is being conducted in accordance with the PIA Guidelines issued by the Office of the Australian Information Commissioner (OAIC).[5]

2.3. Privacy legislation

The Independent PIA is being written in the light of current Commonwealth privacy legislation – the *Privacy Act* 1988. The Act sets out the Australian Privacy Principles (APPs),[6] which regulate the collection, use and disclosure of personal information by Commonwealth Agencies and private sector organisations.

The Australian Government Agencies Privacy Code (the Code) is also relevant. The Code was registered on 27 October 2017 and commenced on 1 July 2018. <www.oaic.gov.au/privacy-law/australian-government-agencies-privacy-code/>.

[5] <www.oaic.gov.au/privacy/privacy-resources/privacy-guides/privacy-impact-assessment-guide>.

[6] The 13 APPs are in Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, which amends the *Privacy Act 1988*. They came into force on 12 March 2014.

3. NHS Linkage Project Overview

3.1. ABS overview

The Australian Bureau of Statistics (ABS) is Australia's national statistical agency, providing statistics on a wide range of economic, social, population and environmental matters of importance to Australia.

The ABS is subject to significant confidentiality provisions contained in various legislation. The most relevant include:

- *Australian Bureau of Statistics Act 1975* (Cth);
- *Census and Statistics Act 1905* (Cth); and
- *Privacy Act 1988* (Cth) and *Australian Privacy Principles* (the APPs)

The *Australian Bureau of Statistics Act 1975* (Cth) gives the ABS the authority to integrate data from a range of sources and to support the maximum usage of these data by official bodies for statistical and research purposes. Additionally, the *Census and Statistics Act 1905* (Cth) applies to data brought into the ABS for the purposes of integration with other data via MADIP.

3.2. The National Health Survey (NHS)

The National Health Survey (NHS) is an important and high profile part of the landscape for health research in Australia.[7] The key features are:

1. The survey is conducted every three years, with a new cohort of participants each time;
2. The survey is conducted by the ABS with funding support from the Department of Health. The ABS is the data custodian for the NHS data;
3. The survey includes around 19,000 people in nearly 15,000 private dwellings. Within each selected dwelling, one adult (18+) and one child (0-17 years) are randomly selected for inclusion in the survey. Non-private dwellings such as hotels, motels, hospitals, nursing homes and short-stay caravan parks are excluded from the survey;
4. The NHS is conducted from a sample of private dwellings in both urban and rural areas across Australia. Very remote areas of Australia and discrete Aboriginal and Torres Strait Islander communities are excluded;
5. The survey is conducted in person by a trained ABS interviewer generally in participants' homes;
6. The survey includes questions on long-term health conditions, health risk factors (eg smoking, BMI, diet, exercise and alcohol consumption), and demographic and socioeconomic characteristics. Voluntary measurements of height, weight, and waist circumference are also taken of respondents aged 2+, as well as voluntary blood pressure measurements for respondents aged 18+;
7. Participation in the survey is mandatory (under ABS legislation) but participation in the measured data is voluntary. Around 61% of children and 73% of adults voluntarily provide the measured data;
8. The focus of the questions is on health and health services, but some general demographic and lifestyle information is also collected; and
9. Name and address details are collected and retained while a business requirement exists, and participants have the option of not providing their names if they prefer.

[7] Australian Bureau of Statistics (ABS), *National Health Survey: First Results, 2014-15*, <www.abs.gov.au/ausstats/abs@.nsf/mf/4364.0.55.001>.

The National Health Survey (NHS) is one of a number of surveys in this field. It is important to distinguish it from the Australian Health Survey (AHS), which is **not** the subject of this Privacy Impact Assessment (PIA). No collection of biomedical samples was undertaken in respect of the 2014-15 NHS.

3.3. MADIP

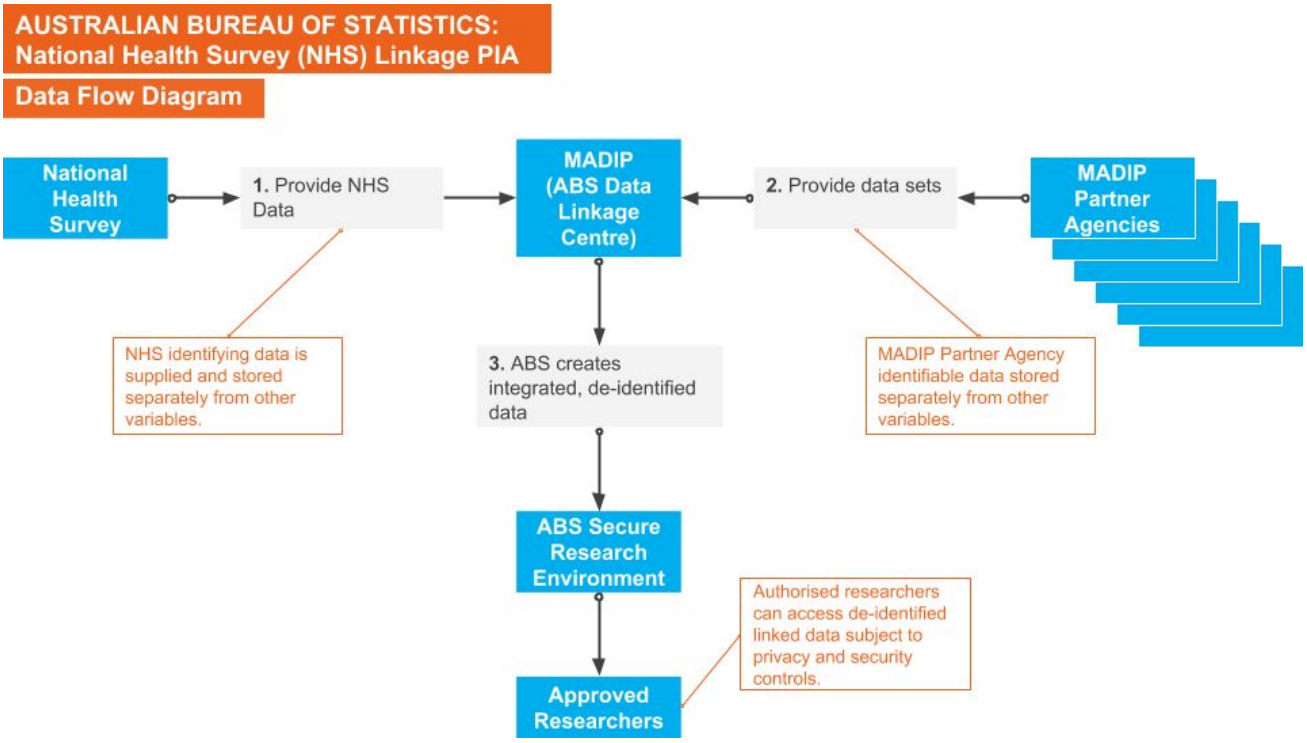
The Multi-Agency Data Integration Project (MADIP) is a cross-portfolio government partnership to demonstrate how the Australian Government can make better use of existing public data for policy analysis, research, and statistical purposes.

The current MADIP Partner Agencies are:

- Australian Bureau of Statistics (ABS)
- Australian Taxation Office (ATO)
- Department of Education and Training (DET)
- Department of Health
- Department of Human Services (DHS)
- Department of Social Services (DSS)

The MADIP combines longitudinal data on healthcare, education, government payments and personal income tax with demographic information. The MADIP was in an evaluation phase from June 2015-18 and as of 1 July 2018 the MADIP is fully operational under the Data Integration Partnership for Australia (DIPA).[8]

3.4. NHS Linkage Project Information Flow



[8] More information on MADIP is available on the MADIP online resource page at: <www.abs.gov.au/websitedbs/D3310114.nsf/home/Statistical+Data+Integration+-+MADIP>

3.5. Potential benefits

Some of the potential benefits of general data linkage are set out in MADIP Case Studies and Project Evaluations that are continually being conducted and published by the ABS. Examples are published at <www.abs.gov.au/websitedbs/D3310114.nsf/home/Statistical+Data+Integration+-+MADIP+Case+Studies>.

MADIP consultations identified that Health Outcomes data from sources like the National Health Survey would be useful.

In relation to the NHS Linkage Project stakeholders consulted during this PIA had very high expectations regarding the potential benefits of linking the NHS data with other data sets via MADIP. Some of the common themes that emerged during discussions with stakeholders (including the ABS, the Department of Health, research stakeholders and consumer stakeholders) were:

- The NHS itself is very highly regarded in terms of quality and relevance. The large sample size and the inclusiveness of the survey mean that the NHS is regarded as a premium source of data;
- Linking the NHS data to other health data, especially MBS and PBS data, would 'fill an enormous gap' in the current ability of researchers and policy makers to understand key issues in the sector, such as linking health outcomes to health services received. This gap was perceived as a 'giant black hole', and stakeholders could not think of an alternative way to obtain this data;
- The inclusion of measured data in the NHS, and the ability to link that measured data with other health data (e.g. MBS and PBS) was considered to be a major boost to the accuracy of data available in the health research sector. Some stakeholders expressed concerns about the quality of self-reported data. Around 70-80% of NHS participants agree to the inclusion of measured data, and this participation rate was considered 'excellent' in the research community;
- Stakeholders expressed their frustration at the difficulty in obtaining useful data on health issues amongst vulnerable groups, such as particular ethnic groups and / or people from lower socio-economic demographic groups. While it was widely recognised that health outcomes were sometimes poor for vulnerable groups, developing appropriate policy responses (or evaluating current policies) was hampered by a lack of data. Linking the NHS (which is highly inclusive) with other data sets via MADIP was expected to deliver a more accurate and detailed picture of health issues amongst these groups. For example, it was expected that researchers would be very interested in comparing health outcomes amongst vulnerable segments of the population, using categories that are only available via linking with MADIP. Again, stakeholders believed that there were likely to be very few effective or affordable alternatives to gaining access to this data; and
- Stakeholders were also interested in the potential for long term use of the data that could be linked in the NHS Linkage Project. Researchers were likely to be interested in studies where cohorts of NHS participants (with the rich data available about their health conditions) were studied over time (both forwards and backwards) by analysing the other data sets (e.g. MBS, PBS, welfare data, education data etc.). Even though the NHS is itself a snapshot in time of a particular cohort, integrating the NHS data with other data sets delivers a valuable insight into determinants and outcomes over time, without the need for expensive and cumbersome longitudinal studies.

3.6. Privacy Strengths and Weaknesses

The proposal to link NHS data to MADIP data raises a mix of privacy strengths and weaknesses. These are set out briefly here, and many of these issues are discussed in further detail in the relevant APP sections below:

Strengths

- There is no **new** collection of personal information from individuals. The NHS Data Linkage Project is proposing to integrate personal information that individuals have already provided through the survey with data they have already provided to other Agencies;
- The Accredited Integrating Authority (the ABS) is subject to a legislative prohibition on releasing any data in a manner that is likely to enable the identification of a particular person (the *Census and Statistics Act 1905* (Cth));
- The 'separation principle' will apply to the NHS Data Linkage Project. This principle ensures personal data (such as name and address) is stored separately to other content data, establishes significant practical barriers to the potential recombination of personal data with other content data, and restricts access according to function or role;
- Data can only be accessed by authorised users in a secure and monitored environment;
- The linking of NHS data to MADIP will be bound by the *High Level Principles for Data Integration Involving Commonwealth Data for Statistical and Research Purposes* (the High Level Principles)[9], including a requirement that data is only used for policy analysis, research, and statistical purposes (not for monitoring or compliance);
- Penalties and sanctions, including imprisonment and hefty fines, are in place for any unauthorised access to the data or inappropriate use of the data;
- The ABS has strong IT systems and security in place, including processes for detecting misuse of information by ABS staff and users of statistical information;
- The objectives and likely outcomes of the NHS Data Linkage Project are in the public interest and are likely to deliver significant community benefit; and
- There is strong community support for the use of data in the health research sector. For example, a 2018 study found that 57.6% of respondents (Australians 18+) agreed with the statement 'I would be comfortable with the government using my data for health and medical research'.[10]

Weaknesses

- The NHS Linkage Project will collect, consolidate and integrate a substantial amount of information that should be categorised under the *Privacy Ac*t as sensitive information; and
- The NHS Linkage Project data is retained for as long as a 'business requirement exists', and this is likely to result in the data being stored for lengthy periods.

[9] The High Level Principles are available at: <www.nss.gov.au>.

[10] Consumers Health Forum of Australia and NPS MedicineWise, *Engaging consumers in their health data journey*. Canberra, May 2018 <chf.org.au/sites/default/files/engaging-consumers-health-data-report.pdf>.

4. Is the data 'personal information'?

4.1. The Law

A starting point for our discussion of privacy compliance is whether or not the data that is proposed to be linked is personal information.

The Commonwealth *Privacy Act 1988* states:

> *Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable.*
> <www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#personal-information>

4.2. OAIC Guidelines

In May 2017 the OAIC provided guidance on personal information:

> *What Is Personal Information?,* Office of the Australian Information Commissioner (OAIC), 5 May 2017 <www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information>.

4.3. NHS Linkage Project – Overview

The proposed data integration arrangements incorporate a mix of personal information and non-personal information.

The core data fields collected in the National Health Survey are personal information, as they are linked with an identifiable individual. However, once the data is shared and integrated via MADIP it changes character.

To align with ABS data management practices, the ABS manages all data acquired by MADIP with processes appropriate for 'personal information'. The analytical information has the name and address removed and is subsequently not 'personal information' for the purposes of the *Privacy Act* – providing it is not 'reasonably re-identifiable'. When providing access to researchers, the ABS ensures that no individual is reasonably identifiable from the data remaining after the de-identification process.

4.4. 'Personal information' finding

The Privacy Commissioner advises that:

> where it is unclear whether an individual is 'reasonably identifiable', an organisation should err on the side of caution and treat the information as personal information[11]

Nearly all of the data initially collected in the NHS and provided to MADIP can be linked to an individual.

However, directly identifiable linkage data is only used to bring the various datasets together. The de-identified analytic data is kept separate from the personal linkage data. Once the data is acquired by MADIP, the analytical data is managed by the ABS in such a way as to minimise the likelihood of spontaneous identification of individuals. This includes a rigorous application of 'functional separation' and other systems and security protocols, as described in the section in APP 11 below.

An additional question is whether or not some of the data falls into the category of sensitive information. This has serious implications for APP 3 and APP 6 (discussed below).

Sensitive information[12] means:

[11] Office of the Australian Information Commissioner (OAIC), Guide to securing personal information, 2015, <www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>.

[12] Section 6 of the Privacy Act 1988 <www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s6.html>.

(a) information or an opinion about an individual's:

(i) racial or ethnic origin; or
(ii) political opinions; or
(iii) membership of a political association; or
(iv) religious beliefs or affiliations; or
(v) philosophical beliefs; or
(vi) membership of a professional or trade association; or
(vii) membership of a trade union; or
(viii) sexual orientation or practices; or
(ix) criminal record;
that is also personal information; or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information; or

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates.

Sensitive information, in the form of 'health information about an individual' is collected in the National Health Survey.

Other types of sensitive information are shared by MADIP Partner Agencies and the ABS with MADIP, and this data will potentially be linked with the NHS data. The main data fields that are likely to be managed as sensitive information in MADIP are health, racial, ethnic and religious data.

All of these categories of sensitive data were of interest to the research stakeholders that were consulted during the development of this PIA. Integrating health data with other sensitive data is a powerful and valuable tool in identifying and understanding health determinants and outcomes for vulnerable groups.

As they are considered sensitive, these variables are handled with the processes required by law and best practice to manage sensitive information. The ABS is currently reviewing how sensitive data is handled in MADIP. In addition, the MADIP data item list identifies each data item as being a linkage variable and / or an analytical variable, personal information or sensitive information, When the NHS is linked to MADIP this will be the case for NHS variables too – so relevant NHS data items in MADIP will be identified as 'sensitive' as defined by the *Privacy Act*. Data item lists for MADIP products are published online.

This issue is discussed in further detail in the sections on APP 3 and APP 6 (below).

5. APP 1. Open and transparent management of personal information

5.1. The Law

APP 1 — open and transparent management of personal information

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

> *(a) will ensure that the entity complies with the APPs / registered code; and*
>
> *(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the APPs / registered code.*

1.3 An APP entity must have a clearly expressed and up to date policy (the APP privacy policy) about the management of personal information by the entity.

1.4 (minimum contents of the privacy policy)

1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

> *(a) free of charge; and*
>
> *(b) in such form as is appropriate.*

More information: <www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-1-app-1-open-and-transparent-management-of-personal-information>.

5.2. NHS Linkage Project – Overview

The main ABS Privacy Policy[13] applies to all surveys including the NHS. ABS privacy policy resources can be accessed from a common location at <www.abs.gov.au/websitedbs/D3310114.nsf/Home/Privacy>.

The main ABS Privacy Policy states:

> *As part of its statistical collections, the ABS collects data from individuals, households and businesses, as well as from administrative sources.*

The main ABS Privacy Policy provides some useful information. However, it is complemented by a more specific MADIP Privacy Policy (published in June 2018).[14] The new MADIP Privacy Policy includes comprehensive information on privacy and data integration – this information is highly relevant to the NHS Linkage Project.

Further information on the NHS, data integration and MADIP is available on the ABS website.

The information available regarding the NHS is useful and comprehensive, but at this stage it obviously does not mention data linking or data integration, or any link to MADIP.

Separately, the ABS website provides a detailed overview of MADIP and links to key resources, including the MADIP FAQs, MADIP Case Studies and the High Level Principles for Data Integration Involving Commonwealth Data for Statistical and Research Purposes <www.abs.gov.au/madip>.

[13] The *ABS Privacy Policy* was released on 29 February 2008 and last updated on 9 May 2017 is available at <www.abs.gov.au/websitedbs/D3310114.nsf/Home/Privacy+Policy>

[14] The MADIP Privacy Policy was released on 29 June 2018 and is available at: <www.abs.gov.au/websitedbs/D3310114.nsf/home/MADIP+Privacy+Policy>.

The published response by the ABS and MADIP Partner Agencies to the MADIP PIA[15] describes ABS's amendment of the MADIP website to provide 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.

If the NHS Linkage Project proceeds, relevant information regarding the NHS will be added to the MADIP online resources. Once implemented, this expansion of public information regarding NHS and MADIP will enhance compliance with APP 1.

A similar enhancement is now required for the ABS web pages that describe the NHS. Useful additions would include:

1. NHS data integration agreement with MADIP;[16]
2. NHS data item list and category description;
3. List of sensitive information in NHS that may be shared with MADIP; and
4. Register of research projects (or link to the MADIP register).

The following checklist provides a useful summary of the key issues regarding openness and transparency:

APP 1. Openness and transparency	Action / Status	Galexia Commentary
A. Does the entity provide a public privacy policy?	**Compliant**	ABS maintains a generic Privacy Policy and a specific MADIP Privacy Policy.
B. Does the Policy include: (a) the kinds of personal information that the entity collects and holds;	**Compliant**	This information is included at a very high level in the main ABS Privacy Policy, and further details are provided in the MADIP Privacy Policy.
C. Does the Policy include: (b) how the entity collects and holds personal information;	**Compliant**	This information is included at a very high level in the main ABS Privacy Policy, and further details are provided in the MADIP Privacy Policy.
D. Does the Policy include: (c) the purposes for which the entity collects, holds, uses and discloses personal information;	**Compliant**	The proposed linking of the 2014-15 NHS data set with MADIP is a new procedure. APP 1 requires the ABS to be open and transparent about the use and disclosure of data. There are no specific references to data linking, data integration or MADIP in the main ABS Privacy Policy. However, detailed information on data integration is provided in the MADIP Privacy Policy and the ABS data integration web-pages. The ABS online resources regarding the NHS will also be updated once the NHS Linkage Project proceeds.
E. Does the Policy include: (d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;	**Compliant**	This information is included in the main ABS Privacy Policy, and further details are provided in the MADIP Privacy Policy.

[15] The MADIP PIA and ABS response were published on 18 April 2018 and are available at <http://www.abs.gov.au/websitedbs/D3310114.nsf/home/ABS+Privacy+Impact+Assessments>

[16] The exact nature of this agreement is difficult to determine at this stage. As ABS is both the data custodian and the data integrator, there may not be a formal agreement or MOU. However, a document of some type, describing the overall rules and governance arrangements for linking NHS data via MADIP could be available (e.g. the proposal to the MADIP Board) or specifically created.

F. Does the Policy include: (e) how an individual may complain about a breach of the APPs / registered code, and how the entity will deal with such a complaint;	**Compliant**	This information is included in the main ABS Privacy Policy, and further details are provided in the MADIP Privacy Policy.
G. Does the Policy include: (f) whether the entity is likely to disclose personal information to overseas recipients;	**Compliant**	This information is included in the main ABS Privacy Policy and the MADIP Privacy Policy. It is not a major issue in the NHS Linkage Project.
H. Does the Policy include: (g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located.	**Compliant**	This information is included in the main ABS Privacy Policy and the MADIP Privacy Policy. It is not a major issue in the NHS Linkage Project.

5.3. APP 1. Finding

It is important for the ABS to be open about linking NHS data with other data sets via MADIP.

Some limited information is provided in the ABS Privacy Policy, and further details are provided in the MADIP Privacy Policy. Some additional information is provided on the NHS and MADIP web pages.

Some enhancements now need to be made for the NHS Linkage Project, so that these resources include specific references to the NHS. This will occur once the NHS Linkage Project has proceeded to the linkage trial stage.

6. APP 2. Anonymity and Pseudonymity

6.1. The Law

APP 2 — anonymity and pseudonymity

2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

2.2 Subclause 2.1 does not apply if, in relation to that matter:

> *(a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or*
>
> *(b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.*

More information:
<www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-2-app-2-anonymity-and-pseudonymity>.

6.2. NHS Linkage Project – Overview

Some limited anonymity is provided in relation to general browsing of the ABS website and accessing information resources.

For the NHS Linkage Project the anonymity principle is not particularly relevant.

APP 2. Anonymity	Action / Status	Galexia Commentary
A. Where lawful and practicable, are individuals given the option of: – Not identifying themselves, or – Identifying themselves with a pseudonym?	**Compliant**	The ABS provides limited anonymity to general web site visitors. Respondents in the NHS survey understand that they are participating in a survey,, and have the option of not providing their names if they prefer. All of the other data collected and linked by the ABS for the NHS Linkage Project is covered by exceptions to the anonymity principle.

6.3. APP 2. Finding

While not limiting or downplaying the requirement for entities to provide anonymous and pseudonymous options to consumers in appropriate transactions and services on a case-by-case basis, APP 2 is not relevant to the day to day operation of the NHS and MADIP. APP 2 is not the subject of detailed consideration in this PIA.

7. APP 3. Collection of solicited personal information

7.1. The Law

APP 3 — collection of solicited personal information

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:

(i) if the entity is an agency — the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(ii) if the entity is an organisation — the information is reasonably necessary for one or more of the entity's functions or activities; or

(b) subclause 3.4 applies in relation to the information.

3.4 This subclause applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(b) a permitted general situation exists in relation to the collection of the information by the APP entity [none are relevant to MADIP]; or…

[Galexia Note: some further exceptions for health bodies, enforcement bodies and non-profit organisations – not relevant here]

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency:

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Some additional exceptions known as permitted general situations also apply – these can be found in Section 16A of the Act.

7.2. OAIC Guidelines

The *PIA Guidelines* issued by the OAIC contain a set of hints and risks under the category of personal information to be collected.

The Privacy Risks they have identified include:

- Collecting unnecessary or irrelevant personal information, or intrusive collection; and
- Bulk collection of personal information, some of which is unnecessary or irrelevant.

In addition to these risks, the collection of personal information should generally be kept to a minimum and personal information should normally be collected from the data subject.

The *PIA Guidelines* also contain a set of hints and risks under the category of method of collection.

The Privacy Risks they have identified include:

- Individuals unaware of the collection or its purpose; and
- Covert collection is generally highly privacy invasive, and should only occur under prescribed circumstances.

More information:
<www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-3-app-3-collection-of-solicited-personal-information>.

7.3. NHS Linkage Project – Overview

APP 3 contains several 'absolute' requirements (such as 3.1 and 3.5) and several conditional requirements that contain exceptions.

In terms of the absolute requirements, the NHS Linkage Project must therefore only acquire information that is reasonably necessary (APP 3.1) and only acquire information by lawful and fair means (APP 3.5). These requirements apply to both the initial collection in the National Health Survey (not the focus of this PIA) and the subsequent linking of NHS data with other data via MADIP.

The reason that the 'collection' principle applies to data linking is that the Office of the Australian Information Commissioner (OAIC) advise that 'collection' includes the creation of new data sets via data linking projects.

The OAIC define Collection (for data analytics) as:

> The concept of 'collects' applies broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means. This includes collection by 'creation' which may occur when information is created with reference to, or generated from, other information the entity holds.[17]

This definition of 'collection by creation' may apply to some aspects of the linking of NHS data to other data sets via MADIP. For example, the sharing of name and address data for linking purposes across multiple data sets is possibly an example of collection by creation. However, this identifying data is not used for any other purposes and is not shared with researchers, so the integration of de-identified data is not likely to be a new collection.

In terms of the conditional requirements, the NHS Linkage Project is able to rely on the exceptions that are available for acquiring personal information where data integration is authorised by a law (APP 3.4).

Sharing NHS data with MADIP is allowed based on ABS legislation and the exceptions in APP 3, complemented by further exceptions in the legislation that governs MADIP Partner Agencies. The overall result is that the sharing of personal information and sensitive information in MADIP is legal, in that it complies with the relevant exceptions in the *Privacy Act*, the ABS legislation and the MADIP Partner Agency legislation.

[17] Office of the Australian Information Commissioner (OAIC), *Guide to Data Analytics and the Australian Privacy Principles* (March 2018) <www.oaic.gov.au/agencies-and-organisations/guides/guide-to-data-analytics-and-the-australian-privacy-principles>.

The following table summarises some of the key issues regarding sharing of personal data from the perspective of the NHS Linkage Project:

APP 3. Collection of solicited information	Action / Status	Galexia Commentary
A. Is collected information reasonably necessary for, or directly related to, one or more of the entity's functions or activities?	**In Progress** **Further measures possible**	In 2018 the OAIC advised that 'collection' includes the creation of new data sets via data linking projects – and this may apply to some aspects of the linking of NHS to MADIP. For example, the sharing of name and address data for linking purposes across multiple data sets is possibly a new collection. However, this identifying data is not used for any other purposes and is not shared with researchers, so the integration of de-identified data is not likely to be a new collection. Data can be collected under APP 3 by relying on the exceptions that apply where data collection is authorised by a specific law. Data collected in the NHS is authorised by the ABS legislation. While there is no dedicated specific legislation for MADIP, the sharing of data with MADIP is authorised by ABS legislation and legislation specific to the other MADIP Partner Agencies. Even though the collection is authorised, it is important to ensure that there is a link between the sharing / linking of data fields and the objectives of the NHS Linkage Project, in order to comply with APP 3.1 (data minimisation). Once data is shared with MADIP, the ABS has a strong data minimisation culture in place, including implementation of the High Level Principles for Commonwealth Data Integration. Data minimisation requirements will be incorporated at both the point of linking the data and the point of providing research access to the linked data. However, there is room for further strengthening of the data minimisation approach. For example, it may be possible to meet the objectives of the NHS Linkage Project without sharing every single detail provided by NHS participants. The intention of this approach is not to restrict valid research activity – it is to ensure that all data items and the level of detail are / continue to be appropriate. Data verification may be useful for data minimisation. 'Data verification' means that the system verifies something as true, rather than collecting the full data. For example, if a researcher just wants to know whether a data subject is an adult or a child, the system only needs to provide a yes/no response on the data field: 'adult'. There is no need to provide the exact date of birth or even the age. Similarly, if a researcher just needs to know whether someone is born overseas, then the system doesn't need to provide the exact country of birth, it can just verify by providing a yes/no response to the query: 'born in Australia'. Data verification is used widely in Australia, particularly in the implementation of the Document Verification Service (DVS)[18] and the Face Verification Service (FVS)[19]. Finally the ABS should be permitted some flexibility in order to allow exploratory testing / evaluation of data integration without data minimisation (e.g. trials or pilots in order to ensure the best possible linking quality).

[18] Refer to <www.homeaffairs.gov.au/about/crime/identity-security/document-verification-service> and <www.dvs.gov.au>.

[19] Refer to <www.homeaffairs.gov.au/about/crime/identity-security/face-matching-services>.

		Recommendation 1: Minimisation of data collection The NHS Data Linkage Project should require the minimisation of personal data collection at both the initial data linking stage and the research access stage. Data minimisation should include: **1.** Only linking and sharing data fields that are necessary **2.** Excluding irrelevant data subjects where possible **3.** Using data verification rather than detailed data collection where possible. The data minimisation requirements should not apply to trials or pilots designed to evaluate data linking quality.
B. Is NO sensitive information about an individual collected (unless a relevant exception applies)?	**Compliant**	Sensitive data is collected in the NHS survey, in the form of health information about an individual. Significant sensitive data has also been acquired under MADIP from other sources, including health data, religious affiliation, sexuality and ethnicity. The sharing of sensitive data with MADIP can be achieved by reliance on the exception in APP 3.4 (a), which allows sensitive data to be acquired where this is authorised by a specific law. This exception clearly applies to the NHS Linkage Project.
C. Is personal information collected only by lawful and fair means?	**Compliant**	ABS has taken steps to ensure that all data being collected in the NHS is collected by lawful and fair means.
D. Is personal information about an individual collected only from the individual (unless a relevant exception applies)?	**Compliant**	NHS data is collected directly from the data subject in most cases. Exceptions are where an adult participant may submit some data relating to a child in the household. This collection is reasonable in the circumstances and is permitted under APP 3.6. MADIP is a data integration, combining data from multiple sources. The acquisition of data from multiple sources is compliant with APP 3 due to the broad exceptions in APP 3.6.

7.4. APP 3. Finding

APP 3 contains several ‘absolute’ requirements (such as 3.1 and 3.5) and several conditional requirements that contain exceptions.

In terms of the absolute requirements, the NHS Linkage Project must only acquire information that is reasonably necessary (APP 3.1) and only acquire information by lawful and fair means. This PIA includes a recommendation to ensure that the ABS is taking steps to minimise the data that is linked and shared in the NHS Linkage Project, in order to meet the requirement in APP 3.1.

In terms of the conditional requirements, the NHS Linkage Project is able to rely on the exceptions that are available for acquiring personal information where data collection and data integration are authorised by a law.

8. APP 4. Dealing with unsolicited personal information

8.1. The Law

APP 4 requires entities who receive unsolicited personal information to determine whether or not they could have collected the information under APP 3. If they determine that they could *not* have collected the personal information; the information must be destroyed.

More information:
<www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-4-app-4-dealing-with-unsolicited-personal-information>.

8.2. NHS Linkage Project – Overview

APP 4 requires agencies and organisations to assess unsolicited information as it arrives, and destroy it if it is information that they could not have collected themselves.

Although the ABS is bound by the rules on unsolicited personal information, this APP is not particularly relevant to the NHS Linkage Project.

APP 4. Dealing with unsolicited information	Action / Status	Galexia Commentary
A. Are there circumstances in which the ABS may receive unsolicited personal information?	**Compliant**	The NHS Linkage Project is very unlikely to receive unsolicited personal information.
B. Does the ABS have a policy in place for managing unsolicited personal information in accordance with the *Privacy Act*?	**Compliant**	This requirement is not relevant to The NHS Linkage Project.

8.3. APP 4. Finding

The NHS Linkage Project is unlikely to have an impact on APP 4 compliance.

9. APP 5. Notification of the collection of personal information

9.1. The Law

APP 5 — notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

> *(a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or*
>
> *(b) to otherwise ensure that the individual is aware of any such matters.*

5.2 The matters for the purposes of subclause 5.1 are as follows:

> [Galexia Note: itemised list follows]

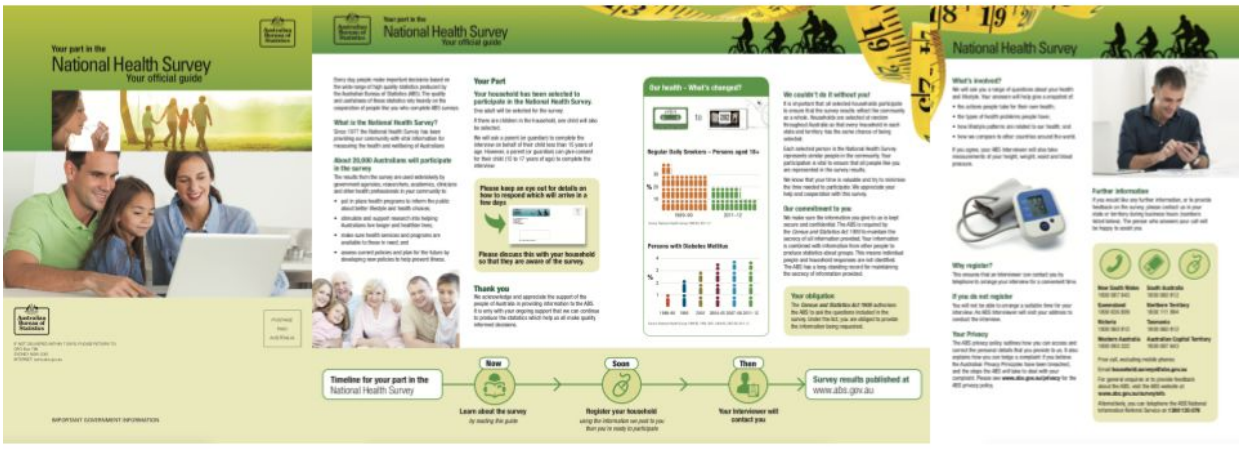
More information:
<www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information>.

9.2. NHS Linkage Project – Overview

Note: In this section we refer to the ABS survey respondent communications as privacy notices (e.g. in the recommendations). The ABS does not use the term 'privacy notice' but it is a generic term that is used in PIAs to cover any section in communications that informs users about their privacy rights.

APP 5 contains a series of important requirements regarding the notice that is provided to data subjects.

The National Health Survey was conducted from July 2014 to June 2015 and the key notice provided to participants was a double sided brochure sent to all participating households, and described as 'Your Official Guide'.



The Guide is, generally, an excellent example of how to give users an effective privacy notice. It is written in plain language, and it strikes a good balance between providing key data without being too lengthy.

Privacy issues are discussed at several points in the Guide. The key statement regarding the use of NHS data is:

> *The results from the survey are used extensively by government agencies, researchers, academics, clinicians and other health professionals in your community to:*
>
> - *put in place health programs to inform the public about better lifestyle and health choices;*
> - *stimulate and support research into helping Australians live longer and healthier lives;*
> - *make sure health services and programs are available to those in need; and*
> - *assess current policies and plan for the future by developing new policies to help prevent illness.*

This is complemented by a section explaining the key privacy protections that are in place, under the heading 'Our Commitment To You':

> *We make sure the information you give to us is kept secure and confidential. The ABS is required by the Census and Statistics Act 1905 to maintain the secrecy of all information provided. Your information is combined with information from other people to produce statistics about groups. This means individual people and household responses are not identified. The ABS has a long-standing record for maintaining the secrecy of information provided.*

Also, a link to further information is provided under the heading 'Your Privacy':

> *The ABS privacy policy outlines how you can access and correct the personal details that you provide to us. It also explains how you can lodge a complaint if you believe the Australian Privacy Principles have been breached, and the steps the ABS will take to deal with your complaint. Please see www.abs.gov.au/privacy for the ABS privacy policy.*

If a participant in the National Health Survey followed the link to the ABS Privacy Policy between July 2014 and June 2015 they would receive some additional information. Although the Policy does not mention data linking or data integration, it does contain some relevant and useful information. For example, the ABS Privacy Policy (2014) included the following statements:

- *We may collect personal information about you directly from you as well as indirectly from third parties.*
- *We only use or disclose your personal information for the purposes for which it was given to us, i.e. purposes which are related to our functions as described under the ABS Act and the Census and Statistics Act.*
- *We do not usually disclose your personal information .... The ABS will never release any information of a personal or domestic nature that has been collected under the Census and Statistics Act.*
- *For statistical purposes, your personal information may be handled in relation to statistical collection activities or statistical coordination and dissemination activities.*

Taken together, the NHS notice and the ABS Privacy Policy 2014-15 make it clear to participants that their information will be collected and used for research and statistical purposes, and that some disclosure and dissemination of data will occur, including sharing data with other agencies and researchers. However, the notice and Privacy Policy are both silent on the general concept of data integration.

This 'silence' does not necessarily amount to a breach of the APP 5 requirements. This is because:

- APP 5 requires the notice to be accurate at or about the time of collection, and the NHS notice was accurate in 2014-15;
- The NHS notice makes it clear that NHS data will be used for research and statistical purposes, and the NHS Linkage Project is still working within that broad category of 'use'; and
- The NHS notice and ABS Privacy Policy indicate that some disclosure of data will take place, and although the NHS Linkage Project involves a significant disclosure of NHS data, the disclosure of actual identifiable personal information is very limited (that data is only disclosed within the ABS for the very limited and specific purpose of data integration, and is subject to a range of strict controls).

The compliance of ABS with APP 5 can be assessed using the following checklist:

APP 5. Notification	Action / Status	Galexia Commentary
A. Does the entity provide notice of its identity and contact details?	**Compliant**	The NHS notice correctly identifies the ABS and includes relevant contact details.
B. Does the entity provide notice of third party collection? (if relevant)	**Compliant**	The NHS notice explains the need for some limited collection of data relating to third parties (e.g. the provision of data on children in the household).
C. Does the entity provide notice of the fact that the collection is required or authorized? (if relevant)	**Compliant**	The NHS notice includes extensive information regarding the collection of data that is authorised by law, with details of relevant legislation. The notice is very clear on the issue of mandatory data collection and a separate letter to participants explains the ABS mandatory collection powers in further detail.
D. Does the entity provide notice of the purpose of collection?	**Compliant**	The NHS notice includes information regarding the original purpose of collection of data.
E. Does the entity provide notice of the main consequences (if any) for the individual if all or some of the personal information is not collected?	**Compliant**	The NHS notice include extensive information regarding the consequences of not providing data. The notice is very clear on the issue of mandatory data collection. The notice states: 'Your obligation: The Census and Statistics Act 1905 authorises the ABS to ask the questions included in the survey. Under the Act, you are obliged to provide the information being requested.' A separate follow-up letter to selected participants explains the ABS mandatory collection powers in further detail. This letter is only provided where necessary (e.g. where there is a compliance issue).
F. Does the entity provide notice of any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected?	**In Progress**	The ABS uses a mix of correspondence and forms to provide notice of privacy issues to NHS participants. However, the NHS notices were provided to respondents between July 2014 and June 2015 – prior to the decision to link NHS data to MADIP. The privacy notices do inform consumers that their data will be used for research and statistical purposes – so the linking with MADIP is not a complete 'repurposing' of their data. However, the notices are silent on the general concept of data integration. The notices were accurate 'at or around the time of collection' so the notices comply with APP 5. However, the absence of any mention of data integration does cause some concerns regarding appropriate privacy practice and the best way to ensure that participants remain confident in the use of their NHS data. Overall, the notices are sufficient for linking the 2014-15 NHS, subject to general strengthening of other privacy protections (especially APP 1 and APP 3). However, improvements should be made to future privacy notices for NHS. **Recommendation 2: Amend privacy notices to clarify the role of data integration** NHS privacy notices should be reviewed and amended to clarify the role of data integration.

G. Does the entity provide notice that the privacy policy contains information about how the individual may access their personal information and seek the correction of such information?	**Compliant**	The NHS notice includes a brief notice regarding the availability of access to data and points participants towards the ABS Privacy Policy for further details.
H. Does the entity provide notice that the privacy policy contains information about how the individual may complain?	**Compliant**	The NHS notice includes a brief notice regarding the availability of corrections and points participants towards the ABS Privacy Policy for further details.
I. Does the entity provide notice of whether the entity is likely to disclose the personal information to overseas recipients (and if so, where)?	**Compliant**	The NHS notice is silent on this issue, and this is an accurate reflection of the relevance / likelihood of overseas transfer of NHS data.

9.3. APP 5. Finding

Generally, the ABS is compliant with many of the requirements of APP 5. The NHS notice is an excellent example of how to give users an effective privacy notice. It is written in plain language, and it strikes a good balance between providing key data without being too lengthy.

However, the notice is silent on the general concept of data integration.

This PIA has concluded that this 'silence' does not amount to a breach of the APP 5 requirements. This is because:

- APP 5 requires the notice to be accurate at or about the time of collection, and the NHS notice was accurate in 2014-15;
- The NHS notice makes it clear that NHS data will be used for research and statistical purposes, and the NHS Linkage Project is still working within that broad category of 'use';
- APP 5 is not triggered by a new collection (e.g. at the point of data integration with MADIP) as the integrated dataset is de-identified; and
- The NHS notice indicates that some disclosure of data will take place, and although the NHS Linkage Project involves a significant disclosure of NHS data, the disclosure of actual identifiable personal information is very limited.

Overall, the notices are sufficient for linking the 2014-15 NHS to other data sets via MADIP, subject to general strengthening of other privacy protections (especially APP 1 and APP 3).

Improvements should be made to future privacy notices for the NHS.

10. APP 6. Use or disclosure of personal information

10.1. The Law

APP 6 — use or disclosure of personal information

Use or disclosure

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:

> *(a) the individual has consented to the use or disclosure of the information; or*
>
> *(b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.*

6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:

> *(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:*
>
> > *(i) if the information is sensitive information — directly related to the primary purpose; or*
> >
> > *(ii) if the information is not sensitive information — related to the primary purpose; or*
>
> *(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or*
>
> *...*
>
> *(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.*

10.2. OAIC Guidelines

The *PIA Guidelines* issued by the Office of the Australian Information Commissioner contain a set of hints and risks under the category of purpose, use and disclosure.

The Privacy hints they have identified include:

- No surprises! Use personal information in ways that are expected by the individual
- No surprises! Tell the individual about disclosures

The Privacy Risks they have identified include:

- Using personal information for unexpected secondary purposes
- Unnecessary or unexpected data linkage
- Unexpected disclosures can lead to privacy complaints

More information:
<www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-6-app-6-use-or-disclosure-of-personal-information>.

10.3. NHS Linkage Project – Overview

APP 6 concerns the use and disclosure of personal information. The legal authority for the use and disclosure of the NHS data comes from ABS legislation.

The *Australian Bureau of Statistics Act 1975* (Cth) gives the ABS the authority to integrate data from a range of sources and to support the maximum usage of these data by official bodies for statistical and research purposes. Additionally, the *Census and Statistics Act 1905* (Cth) applies to data brought into the ABS for the purposes of integration with other data (e.g. data integrated via MADIP).

For NHS data, the ABS is usually prohibited from disclosing any data that identifies an individual. However, in the NHS Linkage Project the personal information is only shared with MADIP in order to integrate the data and make de-identified data available to researchers. The data is collected directly by the ABS under the *Census and Statistics Act 1905* (Cth), and the ABS is also the Accredited Integrating Authority for MADIP, so the personal information always remains within the ABS environment, and no prohibited disclosure occurs.

Significant sanctions apply for the unauthorised disclosure of both NHS and MADIP data.

The following table summarises the key compliance tasks relevant to APP 6:

APP 6. Use or Disclosure	Action / Status	Galexia Commentary
A. Has the entity clearly defined the primary purpose of collection and identified any secondary purposes?	**Compliant**	The NHS privacy notices describe the primary purpose and secondary purposes. As a primary function of ABS is research and the provision of statistics, it is easy for ABS to comply with APP 6 in relation to its own contribution of data to MADIP, including the contribution of data from the NHS.
B. Will the entity only disclose personal information for a secondary purpose with consent (or a relevant exception)? **[Non sensitive information]**	**Compliant**	No secondary use of personal information is envisaged in the NHS Linkage Project. The data is only used (including following integration with other data via MADIP) for the primary purpose of research and statistical analysis.
B. Will the entity only disclose personal information for a secondary purpose with consent (or a relevant exception)? **[Sensitive information]**	**Compliant**	No secondary use of sensitive information is envisaged in the NHS Linkage Project. The data is only used (including following integration with other data via MADIP) for the primary purpose of research and statistical analysis.
C. Is any biometric information only disclosed for a secondary purpose in accordance with Clause 6.3 and the relevant OAIC Guidelines?	**Compliant**	No biometric data is shared in the NHS Linkage Project.
D. Is a written note made of any disclosures that are made relying on the law enforcement exception?	**Compliant**	The NHS Linkage Project disclosures do not rely on the law enforcement exception.

10.4. APP 6. Finding

In order to comply with APP 6, the NHS Linkage Project can rely on the exception in APP 6.2 (b) – that the disclosure is authorised by a law. The NHS Linkage Project is fully compliant with APP 6.

11. APP 7. Direct marketing

11.1. The Law

APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies.

More information:
<www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-7-app-7-direct-marketing>.

11.2. NHS Linkage Project – Overview

Direct marketing is not relevant to the NHS Linkage Project.

11.3. APP 7. Finding

Direct marketing is not relevant to the NHS Linkage Project.

12. APP 8. Cross-border disclosure of personal information

12.1. The Law

APP 8 states that before an organisation discloses personal information to an overseas recipient, they must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information. The organisation that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient. Several exceptions apply.

APP 8 — Cross-border disclosure of personal information

*8.1 Before an APP entity discloses personal information about an individual to a person (the **overseas recipient**):*

> *(a) who is not in Australia or an external Territory; and*
>
> *(b) who is not the entity or the individual;*

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

> *(a) the entity reasonably believes that:*
>
> > *(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and*
> >
> > *(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or*
>
> *(b) both of the following apply:*

(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;

(ii) after being so informed, the individual consents to the disclosure; or

(c) [Galexia note: several additional exceptions apply, but it is difficult to see how these will be relevant to the NHS Linkage Project]

More information:
<www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information>.

12.2. NHS Linkage Project – Overview

Cross border data transfers are not particularly relevant to the NHS Linkage Project.

12.3. APP 8. Finding

Cross border data transfers are not particularly relevant to the NHS Linkage Project. They have not been considered in detail in this PIA.

13. APP 9. Adoption, use or disclosure of government related identifiers

13.1. The Law

APP 9 states that an organisation must not adopt a government related identifier of an individual as its *own* identifier. In addition, an organisation must not use or disclose a government related identifier of an individual unless the use or disclosure is reasonably necessary for the organisation to verify the identity of the individual. Some other exceptions apply.

More information:
<www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-9-app-9-adoption-use-or-disclosure-of-government-related-identifiers>.

13.2. NHS Linkage Project – Overview

APP 9 contains two key requirements:

- **The first is that organisations must not adopt a government identifier as their own identifier.** This is designed to prevent the development of de facto national identifiers. For example, organisations cannot use the Tax File Number (issued by the Commonwealth government) as their own identifier.
- **The second requirement of APP 9 is that government related identifiers should not be disclosed except in specific situations where the disclosure is reasonably necessary to verify identity.**

APP 9 does not generally apply to agencies apart from some prescribed commercial activities undertaken by agencies. The ABS does not undertake such activities as part of their business as usual practices.

The ABS may incidentally use a government related identifier as part of its identity linking and identity verification process, however these are never disclosed by the ABS to any external parties.

13.3. APP 9. Finding

APP 9 does not apply to agencies such as the ABS.

14. APP 10. Quality of personal information

14.1. The Law

APP 10 — quality of personal information

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.

10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

14.2. OAIC Guidelines

The *PIA Guidelines* issued by the Office of the Australian Information Commissioner contain a set of hints and risks under the category of data quality.

The Privacy Risks they have identified include:

- Retaining personal information unnecessarily
- Making decisions based on poor quality data

More information:
<www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-10-app-10-quality-of-personal-information>.

14.3. NHS Linkage Project – Overview

The ABS is conscious of the importance of accurate data and accurate data linking processes. In the NHS Linkage Project, research outputs and analysis will be relied on by a range of third parties, including policy makers and planners.

Stakeholders consulted during the development of this PIA expressed a high level of confidence in the accuracy of the NHS data. It is clearly viewed as a premium data source compared to other available data.

However, making links between diverse data sets is a difficult process, and some incorrect links are likely to emerge. The ABS are conscious of the need to make accurate links once the NHS data is integrated with other data sets via MADIP.

The following table summarises compliance with APP 10, but it is very important to note that the data quality issues need to be assessed on a case by case basis for each linkage.

APP 10. Data Quality	Action / Status	Galexia Commentary
A. Has the entity taken such steps (if any) as are reasonable in the circumstances to ensure that the personal information collected is accurate, up-to-date and complete?	**Compliant**	The ABS has extensive systems in place for ensuring that its own data is accurate. These systems are not the subject of detailed consideration in this PIA.

B. Has the entity taken such steps (if any) as are reasonable in the circumstances to ensure that the personal information **that the entity uses or discloses** is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant?	**In progress**	The NHS Data Linkage Project may have an impact on linked data quality. The ABS may need to undertake trials and pilot data linkages to assess the accuracy of data linking. The ABS is already planning an initial trial. There is also a continual assessment of data linking processes in MADIP to assess the accuracy of data that can be provided by Partner Agencies. **Recommendation 3: Assess data quality benefits and risks** The NHS Data Linkage Project should be subject to an initial evaluation / assessment regarding the potential data quality benefits and risks.

14.4. APP 10. Finding

The ABS has extensive systems in place for ensuring that its own data is accurate, and the NHS data is regarded as high quality. However, making links between diverse data sets is a difficult process, and some incorrect links are likely to emerge;

The NHS Data Linkage Project may have an impact on linked data quality and this will have to be assessed on a case by case basis. The ABS may need to undertake trials and pilot data linkages to assess the accuracy of data linking. The ABS is already planning an initial trial.

15. APP 11. Security of personal information

15.1. The Law

APP 11 requires entities to take such steps as are reasonable in the circumstances to protect personal information from misuse, interference and loss; and from unauthorised access, modification or disclosure.

Also, if the organisation no longer needs the information for any purpose for which the information may be used or disclosed, they must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

15.2. OAIC Guidelines

APP 11 has a wide scope for interpretation, as it includes multiple tests for what is 'reasonable in the circumstances'. Some additional guidance is available from the Office of the Australian Information Commissioner (OAIC) in the form of guidelines:

- *Guide to securing personal information*, OAIC, 2015 <www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>

More information: <www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information>.

15.3. NHS Linkage Project – Overview

The security risk profile of the data involved in the NHS Linkage Project is high, as it includes the linking and sharing of personal information and sensitive information that would have an impact on individuals, the ABS and MADIP Partner Agencies if it was made public.

In addition, the data retention and data destruction requirements of APP 11 are difficult to apply where data is intended to be retained indefinitely, as is the case in the NHS Linkage Project.

The following table provides a high level summary of potential compliance with APP 11 regarding the NHS Linkage Project.

APP 11. Security	Action / Status	Galexia Commentary
A. Has the entity taken such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss?	**Compliant**	The NHS Linkage Project has a high security risk profile, and it is vital that key aspects of the Project – especially the transfer of data to MADIP and its subsequent processing and storage – are subject to regular, independent security risk assessments. The ABS data linkage environment has recently been upgraded and has been independently reviewed and assessed as providing an appropriate level of security.
B. Has the entity taken such steps as are reasonable in the circumstances to protect the information from unauthorised access, modification or disclosure?	**Compliant**	The ABS has processes in place to guard against unauthorised access while the data is held by the ABS. ABS legislation includes severe penalties for unauthorised access.
C. Does the level of security in the application match the potential harm caused by breaches of privacy?	**Compliant**	The data being exchanged in the NHS Linkage Project includes sensitive personal information that is initially provided in the NHS or already exists in other data sets that are integrated via MADIP. The scale of the data involved is also significant. It is important for security settings to match the potential harm of any breaches. The ABS applies high security standards to both the NHS and MADIP.

D. Will detailed access trails be retained and scrutinised for security breaches?	**Compliant**	The ABS already applies detailed access logging requirements to researchers accessing data via the ABS secure research environment. These processes will apply to the NHS Linkage project.
E. Will a data retention policy / destruction schedule be developed which requires retention of personal information only for the period required for use?	**Compliant**	The ABS has a formal data retention policy in place for all data. The intention in the NHS Linkage Project is that data will be retained as long as there is a business need to do so, and regular review points for the continued retention of information ensure it is not retained any longer than the period required for use. In practice, data can be retained indefinitely, and data sets integrated via MADIP are designed to be 'enduring' data sets. Research stakeholders consulted during the development of this PIA were very interested in the long-term retention of NHS data that could be linked to other data sets via MADIP. This approach is anticipated to provide considerable public benefits. The long-term retention of data raises the security risk profile of the NHS Linkage Project, but it does not breach APP 11.
F. Is personal information de-identified as soon as possible?	**Compliant**	The ABS has a sophisticated approach to the de-identification of data. 1. Names and addresses are separated from other information in most source datasets (including the NHS) prior to supply to MADIP (and are supplied separately). 2. Identifiable information is de-identified in the linkage process (e.g. through encoding), prior to analytical datasets being assembled for use by researchers. 3. Analytical data provided to researchers do not contain directly identifiable information, and outputs are checked for confidentiality prior to release.

15.4. APP 11. Finding

The data being exchanged in the NHS Linkage Project has a high security risk profile, and APP 11 requires reasonable steps to be taken to protect the data from unauthorised access.

Currently there are strong security measures in place at ABS that are relevant to the NHS Linkage Project. These include:

- Storage of all data in the 'NextGen Infrastructure Environment',
- Implementation of functional separation of linkage data from other data variables, and restricting access according to function or role,[20]
- Implementation of the 5 Safes Framework,[21] and
- Restricting access to NHS data that is integrated with other data sets via MADIP to monitored access at the ABS DataLab.[22]

The ABS data linkage environment has recently been upgraded and has been independently reviewed and assessed as providing an appropriate level of security. The findings of this review apply to the NHS Linkage Project.

[20] More information on the Separation Principle is contained in *A Guide for Data Integration Projects Involving Commonwealth Data for Statistical and Research Purposes* (Australian Government National Statistical Service), available at <statistical-data-integration.govspace.gov.au/topics/applying-the-separation-principal>.

[21] More information on the Five Safes Framework is contained in *Managing the Risk of Disclosure: The Five Safes Framework* (Australian Bureau of Statistics, Confidentiality Series 116.0, August 2017) available at: <www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/1160.0Main%20Features4Aug%202017?opendocument&tabname=Summary&prodno=1160.0&issue=Aug%202017&num=&view=>.

[22] For a general overview of relevant protections in place at the Australian Bureau of Statistics, refer to: *The Confidentiality Series* (ABS 116.0, August 2017), available at: <www.abs.gov.au/ausstats/abs@.nsf/mf/1160.0>.

APP 11 also requires the ABS to establish appropriate rules for the destruction and de-identification of data. The NHS data will be retained for a lengthy period, as there are likely to be significant benefits from integrating the NHS data with other data sets via MADIP over time. This approach raises the security risk profile of the NHS Linkage Project, but is not itself a breach of APP 11.

16. APP 12. Access to personal information

16.1. The Law

APP 12 — access to personal information

Access

12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exceptions to access…

More information:
<www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information>.

16.2. NHS Linkage Project – Overview

ABS has a **general exemption** to access requests to data that it holds. The *Privacy Act* allows an agency to refuse access where they are authorised under Freedom of Information (FOI) legislation to refuse access. The *Freedom of Information Act 1982* (Cth) (Schedule 2, Part II, Division 2) exempts the ABS from providing access to documents containing information collected under the *Census and Statistics Act 1905* (Cth).

The following table summarises the key requirements of APP 12:

APP 12. Access	Action / Status	Galexia Commentary
A. Can the individual ascertain whether the entity has records that contain personal information, the nature of that information and the steps that the individual should take to access their record?	**Compliant**	ABS has general access policies and procedures in place. ABS also has the ability to refuse access requests under its general exemption to APP 12.
B. If an agency holds personal information about an individual, does the agency, on request by the individual, give the individual access to the information? (unless relevant exceptions apply)	**Compliant**	ABS has general access policies and procedures in place. ABS also has the ability to refuse access requests under its general exemption to APP 12.

16.3. APP 12. Finding

APP 12 requires the ABS to provide clear information to consumers on how they can access their data. The extent of access to NHS Linkage Project data may be limited by exemptions that are available to the ABS under privacy and FOI legislation.

17. APP 13. Correction of personal information

17.1. The Law

APP 13 — correction of personal information

Correction

13.1 If:

> *(a) an APP entity holds personal information about an individual; and*
>
> *(b) either:*
>
> > *(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or*
> >
> > *(ii) the individual requests the entity to correct the information;*
>
> *the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.*

Notification of correction to third parties

13.2 If:

> *(a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and*
>
> *(b) the individual requests the entity to notify the other APP entity of the correction;*

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

...

Dealing with requests

13.5 If a request is made under subclause 13.1 or 13.4, the APP entity:

> *(a) must respond to the request:*
>
> > *(i) if the entity is an agency — within 30 days after the request is made; or*
> >
> > *(ii) if the entity is an organisation — within a reasonable period after the request is made; and*
>
> *(b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).*

17.2. OAIC Guidelines

The *PIA Guidelines* issued by the Office of the Australian Information Commissioner contain a set of hints and risks under the category of correction of personal information.

- Getting access to personal information should be clear and straightforward.
- Inaccurate information can cause problems for everyone!

More information:
<www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-13-app-13-correction-of-personal-information>.

17.3. NHS Linkage Project – Overview

The ABS already has policies and procedures in place for complaints and the correction of inaccurate data. The following table sets out the key steps required in order to comply with APP 13:

APP 13. Correction	Action / Status	Galexia Commentary
A. UPON REQUEST Does the entity take such steps (if any) as are reasonable in the circumstances to correct that information?	**Compliant**	ABS has correction policies and procedures in place that are fully compliant with APP 13. These provisions will apply to the NHS Linkage project.
B. UPON LEARNING OF INACCURACIES Does the entity take such steps (if any) as are reasonable in the circumstances to correct that information? (where the inaccuracy relates to a purpose for which the information is held)	**Compliant**	ABS has correction policies and procedures in place that are fully compliant with APP 13. These provisions will apply to the NHS Linkage project.
C. UPON REQUEST ONLY Will corrections and annotations be disseminated to third parties to whom personal information has previously been disclosed?	**Compliant**	ABS has correction policies and procedures in place that are fully compliant with APP 13. These provisions will apply to the NHS Linkage project.

17.4. APP 13. Finding

The ABS is compliant with the complaints and corrections requirements of APP 13.

18. Governance

In the NHS Linkage Project, the ABS has compliance requirements in addition to the APPs, and therefore may require a broader governance framework.

Additional compliance requirements come from:

- Legislation, especially secrecy and confidentiality provisions in ABS legislation;
- Conditions imposed on the use of data supplied by NHS (potentially to be set out in the application to the MADIP Board or in a written agreement);
- Audit findings and recommendations (in time, these will become more important); and
- Best practice guidance (e.g. developed by the Department of Prime Minister and Cabinet).

The following table summarises (briefly) the potential Governance requirements for the NHS Linkage Project. Note that this table only addresses issues most relevant to privacy.

NHS Linkage Governance will fall under MADIP Governance arrangements.

Governance Issue	ABS Requirements	Galexia Note
A. Data minimisation	The ABS should minimise the data that it links. This should include as a minimum three tests: 1. Only collecting data fields that are necessary 2. Excluding irrelevant data subjects where possible 3. Using data verification rather than data collection where possible	It is possible that this can be introduced as a simple protocol for each research proposal. This is already established practice for MADIP. This requirement comes from APP 3.
B. Minimum security requirements and independent security risk assessments	The ABS should establish minimum security requirements for all data integration and conduct regular independent security risk assessments	This is already established practice for MADIP. The most recent security assessment has established that appropriate security safeguards are in place for the linking of NHS data via MADIP.
C. Compliance audits	ABS should establish an internal compliance audit regime. The audits should examine: 1. compliance with the APPs; 2. compliance with conditions imposed by other agencies; 3. compliance with other secrecy and confidentiality requirements; and 4. compliance with minimum security standards. We note that the OAIC already has an audit function (Part IV of the *Privacy Act*) that will enable it to oversee the data linking activities.	This is already established practice for MADIP. These audits will cover the linking of NHS data via MADIP.

Recommendation 4. Strengthen and enhance NHS Linkage Governance arrangements
The ABS need to continually review, strengthen and enhance the NHS Linkage Project governance framework, including:

A. Data minimisation
B. Minimum security requirements and assessments
C. Compliance audits

19. Appendix 1 – Acronyms

Acronym	Term
ABS	Australian Bureau of Statistics <www.abs.gov.au>
AHS	Australian Health Survey (different from National Health Survey)
APP	Australian Privacy Principle
APS	Australian Public Service <www.apsc.gov.au>
BMI	Body Mass Index
DIPA	Data Integration Partnership for Australia <www.pmc.gov.au/public-data/data-integration-partnership-australia>
DoH	Department of Health
FOI	Freedom of Information
IRAP	InfoSec Registered Assessors Program <www.asd.gov.au/infosec/irap.htm>
MADIP	Multi-Agency Data Integration Project <www.abs.gov.au/madip>
MBS	Medicare Benefits Schedule <www.mbsonline.gov.au>
MOU	Memorandum of Understanding
NHS	National Health Survey (different from Australia Health Survey)
NHS 2014-15	The National Health Survey that was conducted in the 2014-2015 financial year <www.abs.gov.au/ausstats/abs@.nsf/PrimaryMainFeatures/4363.0>
OAIC	Office of the Australian Information Commissioner <www.oaic.gov.au>
PBS	Pharmaceutical Benefits Scheme <www.pbs.gov.au>
PIA	Privacy Impact Assessment

20. Appendix 2 – Stakeholder Consultation

During the development of this PIA, Galexia met with the following organisations:

- Australian Bureau of Statistics (ABS)
- Australian Institute of Health and Welfare (AIHW)
- Australian National University (ANU) Research Services Division
- Consumers Health Forum of Australia
- Department of Health
- Office of the Australian Information Commissioner (OAIC)

Additional stakeholder consultations regarding ABS data linkage activities such as MADIP have been conducted by the ABS as separate activities.