KING&WOOD MALLESONS

galexia

Australian Government

Department of Health

Privacy Impact Assessment (PIA) for the Data Matching Proposal

PIA: Fraud detection and compliance activities

12 September 2019

[FINAL]

Document Control

Client

This document has been written for the Department of Health.

Document Purpose

This document is a Privacy Impact Assessment (PIA) for the proposed sharing / matching of some health data with key partners (the *Data Matching Proposal*) for fraud detection and compliance related activities.

Document Identification

Document title	Health Data Matching PIA – Fraud Detection and Compliance Activities
Document filename	gc525_health_data_matching_compliance_PIA_20190912_FINAL.pdf

Client Details

Department of Health
Australian Government
Sirius Building, Furzer Street, Woden Town Centre, ACT
<www.health.gov.au>

Consultant Details

KWM Contact	**Patrick Gunning** | Partner profile King & Wood Mallesons Level 61, Governor Phillip Tower, 1 Farrer Place, Sydney NSW 2000 p: +61 2 9296 2170 m: +61 418 297 018 e: patrick.gunning@au.kwm.com
Galexia Contact	**Peter van Dijk** (Managing Director) Galexia <www.galexia.com> Level 11, 175 Pitt St, Sydney NSW 2000, Australia p: +612 9660 1111 m: +61 419 351 374 e: manage@galexia.com
Reference	GC525 (Compliance PIA)
Project Email	kwm-health@galexia.com

1. Executive Summary

1.1. Approach and Scope

KWM and Galexia have completed this Privacy Impact Assessment (*PIA*) for the proposed sharing and matching of particular health and non-health data between key partners for compliance checking purposes (the *Data Matching Proposal*).

This PIA has been developed in consideration of a proposed package of legislative reform to facilitate data sharing and data matching in relation to health data. The package is likely to include the proposed *Health Legislation Amendment (Data-matching) Bill 2019*[1] supplemented by additional governance arrangements and individual data sharing agreements. Any later changes to the bill or legislative package may require revisions to this privacy advice

'*Compliance checking purposes*' broadly includes:

- Identifying whether a person may have, under a Medicare program, claimed or been paid a benefit that exceeds the amount of the benefit that was payable to the person;
- Recovering overpayments of benefits under a Medicare program;
- Monitoring services, benefits, programs or facilities that are provided for under a Medicare program
- Educating healthcare providers about requirements relating to Medicare programs
- Detecting or investigating contraventions of a law of the Commonwealth relating to a Medicare program; and
- Detecting or investigating inappropriate practice.

This PIA has been conducted in accordance with *PIA Guidelines* issued by the Office of the Australian Information Commissioner (OAIC).[2]

The purpose of this PIA is to assist in identifying and managing privacy issues that are raised by the proposed matching and sharing of data between the Department of Health and other agencies and third parties. The key proposals are:

1. To engage in a range of data sharing and data matching activities for compliance checking purposes (e.g. to help detect incorrect claiming, fraud and inappropriate practice);

2. To replace some existing manual and transaction based data sharing with routine data sharing arrangements from limited and specified sources within a controlled, closed environment between government agencies; and

3. To create an effective governance framework for the proposed data sharing and data matching.

This PIA considers compliance with privacy legislation, compliance with other legislation (including proposed amendments), user acceptance and public perception issues. The PIA makes a broad range of recommendations for mitigating privacy risks, including changes to the design, practical privacy compliance steps, further research and privacy governance arrangements.

Information contained in this PIA is based on:

- Meetings with the Department of Health, including senior management, technical staff, policy staff and the privacy compliance team;
- Meetings with data owner/custodian stakeholders (further details included in Appendix 3);
- Documentation related to the proposal;
- General research and literature review on privacy and data sharing / data matching issues; and
- Review of relevant privacy legislation and guidelines.

[1] The version reviewed for this PIA is v39 of 11 April 2019.

[2] Office of the Australian Information Commissioner, Australian Government, *Guide to undertaking privacy impact assessments* (May 2014) <www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments>.

Our advice in this PIA concentrates on the following areas:

- **Privacy legislation compliance** – This PIA assesses the proposed sharing / matching of data between the Department of Health and a range of other agencies and third parties against the Australian Privacy Principles (*APPs*) in the *Privacy Act 1988* (Refer to 1.2. Australian Privacy Principle (APP) Compliance Summary);
- **Practical measures to address privacy** – This PIA identifies several practical measures that can be taken to manage privacy issues;
- **Governance** – The PIA considers key privacy governance steps that could be implemented to ensure ongoing protection of privacy once data sharing / data matching proposals are operational (Refer to 18. Governance); and
- **Future work plan** – This PIA identifies several priority tasks to be included in the Department of Health's future work plan. (Refer to 1.3. Future Work Plan).

This PIA has been conducted over a 12+ month period and has followed an iterative process. Some earlier advice and recommendations have already been adopted and actioned by the Department of Health and this has been progressively reflected in the findings and recommendations.

1.2. Australian Privacy Principle (APP) Compliance Summary

This PIA assesses the proposed data sharing and data matching against the APPs in the Commonwealth *Privacy Act*. The scope of this PIA is limited to the use of matched data by the Department of Health, and therefore this PIA only considers privacy issues in the context of *provider* compliance. The use of matched data by the Department of Human Services is outside the scope of this PIA.

This PIA has been developed on the assumption that the proposed *Health Legislation Amendment (Data-matching) Bill (2019)* has been passed. Any later changes to the bill or legislative package may require revisions to this privacy advice.

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

Australian Privacy Principle (APP) / Privacy Component	Compliance Status	Findings Summary	Recommendation
Is the data 'personal information'?	**Not applicable**	Nearly all of the data that is proposed to be shared / matched will be linked to an individual, or can be linked to the correct individual. All data matched for compliance purposes should all be treated as personal information for the purpose of compliance with the APPs. Some of the data also falls into the category of sensitive information. This has implications for compliance with APP 3 and APP 6 (discussed below).	
APP 1 – **Openness and transparent management**	**In Progress**	The proposed data sharing and data matching arrangements for fraud detection and compliance related activities are new procedures. APP 1 requires the Department of Health to be open and transparent about these new arrangements, and to take reasonable steps to implement practices, procedures and systems to ensure compliance with the other APPs and any applicable privacy code. There may be follow on consequences for partner agencies / data sources regarding their own compliance with APP 1. The Department of Health and Department of Human Services have acknowledged the need to update their Privacy Policies and at the time of completing this PIA these changes are in progress. **Note:** There is a further discussion of potential governance arrangements to assist in privacy compliance in Section 18. Governance (below). These governance arrangements will also address openness and transparency and assist in compliance with APP 1.	**Recommendation 1. Improved openness in Privacy Policies about data sources** The Department of Health should amend the Privacy Policy to be more open about the collection of new data fields and the extensive variety of data sources. As some initial data collection occurs via the Department of Human Services (DHS), this recommendation extends to the DHS Privacy Policy. **Recommendation 2. Improved openness in Privacy Policies about data sharing / matching** The Department of Health should amend the Privacy Policy to be more open about the use of routine data sharing for controlled data-matching' activities, and to update the list of I kely external agencies involved in data sharing / matching. As some initial data collection occurs via the DHS, this recommendation extends to the DHS Privacy Policy.

			Recommendation 3. Establish an online resource to improve openness and transparency about data sharing / matching The Department of Health should establish a dedicated website or secure data transfer facility with a list of key documents, a register of data matching activities, contact details and other relevant information about its data sharing / data matching activities. **Recommendation 4. Improve openness and transparency at partner agencies / data sources regarding data sharing / data matching with the Department of Health** The Department of Health should take steps to encourage improved openness and transparency at partner agencies and data sources regarding data sharing / data matching activities. This could include provisions in the data sharing agreements and regular checks and updates. Openness and transparency at partner agencies and data sources could be improved by: **1.** Changes to relevant privacy policies, naming the Department of Health as an entity that shares / receives data; and **2.** Online information and resources, or links to the Department of Health online resource established under Recommendation 3.
APP 2 – Anonymity and Pseudonymity	**Compliant**	The Department of Health provides some limited anonymity to general web site visitors. All of the other data collected and matched by the Department of Health for compliance checking purposes is covered by exceptions to the anonymity principle.	

APP 3 – Collection of solicited personal information	**In Progress**	In the Data Matching Proposal the Department of Health will be able to match data collected from limited and specified sources. If data is collected specifically for data-matching, the necessity of this data needs to be assessed for each proposed collection. The Data Matching Proposal will need to establish baseline rules for the collection of data. Also, the categorisation of shared data as 'sensitive' data needs to be assessed for each proposed collection. The collection of sensitive data is permitted by relying on exceptions contained in APP 3.4. In some cases it may be necessary for the Department of Health to engage in data matching that helps the Department to identify and / or narrow down the potential list of individuals who are likely to be engaged in incorrect claiming, fraud and inappropriate practice. Normally the collection of sensitive data would require explicit consent. However, reliance on explicit consent is unlikely to be an appropriate solution in the context of fraud detection and compliance related activities. The Department of Health needs to find a balance between openness and the need to avoid alerting persons who may be the subject of compliance activity to specific fraud detection processes in a manner that would enable them to continue engaging in fraudulent conduct without detection. This PIA concludes that the use of the exceptions in APP 3.4 is appropriate. However, the application of APP 3.4 does not remove the requirement to minimise data collection (APP 3.1). The proposed legislative framework includes a high level data minimisation requirement. This requires some further detail (e.g. in the implementation and governance arrangements) to ensure that systems and processes include data minimisation steps.	**Recommendation 5. Minimisation of data collection** The systems and processes for proposed data sharing / data matching arrangements should require the minimisation of personal data collection by: **1.** Only collecting data fields that are necessary; **2.** Excluding irrelevant data subjects where possible; **3.** Using data verification (e.g. Yes/No responses) rather than data collection where possible.
APP 4 – Dealing with unsolicited personal information	**Compliant**	The Department of Health's legislation anticipates that a variety of sources, including information that is held or has been obtained by the Department for the purposes of a Medicare program, can be used by the agency to assist in its administrative and law enforcement processes. The Department of Health is already fully compliant with APP 4. The expansion of data sharing / matching arrangements is unlikely to have an impact on APP 4 compliance.	

APP 5 – Notification	**Compliant** (Further measures possible)	In the Data Matching Proposal defined data from limited and specified sources is proposed to be shared with other Agencies and entities. Compliance with APP 5 therefore needs to be assessed for each proposed disclosure. The Department of Health uses several forms to provide notice of privacy issues to its data subjects. Some of these forms are initially provided by the Department of Human Services (DHS). These forms are compliant with many of the requirements of APP 5. However, the Department of Human Services privacy notices do not provide notice of the scope of third party collection that is envisaged under the Data Matching Proposal. This is particularly relevant if the Chief Executive Medicare authorises Commonwealth entities to engage in data-matching on the Department's behalf for permitted purposes. Although third party collection is briefly mentioned, a consumer is unlikely to be on notice regarding the collection of third party data by the Department of Health, or the range of third parties involved. Also, the notices do not provide notice of the scope of data matching. Although disclosure to other Agencies is discussed in broad terms, a consumer is unlikely to be on notice regarding matching of data supplied by other agencies to the Department of Health, or the range of other agencies / entities involved. The finding for APP 5 is categorised as 'Compliant (Further measures possible)' because the suggested improvements to privacy notices are not a strict *Privacy Act* requirement – they do however represent best practice.	**Recommendation 6. Amend privacy notices to clarify scope of third party data collection** The Department of Health and Department of Human Services privacy notices should be reviewed and amended to clarify the scope of third party data collection, and the expanded list of third parties that are involved. **Recommendation 7. Amend privacy notices to clarify the scope of data matching** The Department of Health and Department of Human Services privacy notices should be reviewed and amended to clarify the scope of data matching and the expanded list of other agencies that are involved in the data matching proposal.
APP 6 – Use or Disclosure	**Compliant**	Subject to the passage of appropriate legal authority, this PIA has found that the APP 6 provisions that allow the use and disclosure of data where authorised by a law are sufficient to achieve compliance for the various data matching proposals.	
APP 7 – Direct Marketing	**Compliant**	Direct marketing is not relevant to this PIA.	
APP 8 – Cross Border Disclosure	**Compliant**	Cross border data transfers are not relevant to the Data Matching Proposal. 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 prescr bed commercial activities.	
APP 10 – Quality of Personal Information	**In Progress**	The Department of Health 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. The Data Matching Proposal may have an impact on data quality and this will have to be assessed on a case-by-case basis.	**Recommendation 8. Assess data quality benefits and risks** The Data Matching Proposal should include a requirement for routine data sharing for controlled data-matching to be assessed regarding the potential data quality benefits and risks.

		Some of the data matching proposals are 'exploratory'. The Department of Health will need to undertake trials and pilot data exchanges to assess the accuracy of data that can be provided by partner agencies and entities in the Data Matching Proposal. Several trials and evaluations have already been conducted.	
APP 11 – Security	**Action required**	The data being exchanged in the Data Matching Proposal 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 Department of Health has extensive security measures in place to protect the data that it receives. The IT environment that will be used for data matching is also the subject of periodic independent security risk assessments. The security measures could be improved by the use of common security standards for other agencies and third parties who receive data from the Department of Health in the Data Matching Proposal and the extension of security audits and compliance checks to cover the entire Proposal. All Australian Commonwealth entities must comply with the Australian Signals Directorate Information Security Manual (ISM). These may serve as a common standard. It will also be important to develop the capability to detect and identify data breaches (both within the Department of Health and at third parties accessing the data). Data destruction requirements are also an important part of compliance with privacy best practice. The proposed legislative framework – envisaged in the *Health Legislation Amendment (Data-matching) Bill 2019* – and additional governance arrangements will need to include clear data destruction and data retention requirements. The new data retention / destruction requirements should be applied to any sensitive personal information collected or disclosed for data matching and also the results / output of the data matching process conducted by the Department of Health.	**Recommendation 9. Establish a security compliance framework** Where data is shared with Commonwealth entities and other agencies, the Department of Health should establish a security compliance framework (consisting of mandatory security requirements backed by regular security audits, testing and reporting) that extends security measures to all participants in the Data Matching Proposal. **Recommendation 10. Expansion of data destruction requirements** The Department of Health should expand processes for data retention / destruction to cover data that is shared by / with other Commonwealth entities and third parties, ensuring that participants are complying with data destruction conditions imposed by the Department of Health and vice versa.
APP 12 – Access	**Compliant**	The Department of Health has access policies and procedures in place that are fully compliant with APP 12. The Data Matching Proposal does not have a significant impact on Access requests under APP 12.	
APP 13 – Correction	**Action required**	The Data Matching Proposal will require an expansion of complaints management and the correction of data to ensure that all third parties involved in data matching are covered.	**Recommendation 11. Sharing corrections** The Department of Health should share all relevant data corrections with third parties involved in data matching.

Section 18. Privacy Governance	**Action required**	In the Data Matching Proposal the Department of Health and partner agencies are subject to more than compliance with the APPs, so a broader governance framework is required. In this context there is a framework made up of the department's Privacy Plan, data matching plans and the governance arrangements established under the proposed legislative framework. The Department of Health will benefit from addressing all of these compliance requirements in a single framework, and has begun work on developing an appropriate framework.	**Recommendation 12. Establish privacy governance arrangements and then review, strengthen and enhance on a regular basis** The Department of Health should formally, establish core criteria for the privacy governance arrangements, including: A. Register of agreements B. Data minimisation C. Openness D. Notice E. Data quality assessment F. Minimum security requirements and independent security risk assessments G. Compliance audits H. Managing data destruction Once established, the Department should review, strengthen and enhance the privacy governance arrangements on a regular basis.

1.3. Future Work Plan

A suggested future work plan for the Department of Health, based on the recommendations in this PIA, is set out in the following table. Department of Health 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 / Privacy Component	Recommendation	Action Required	Agency responsible	Priority
APP 1 – Openness and transparent management	**Recommendation 1.** Improved openness in Privacy Policies about data sources	DoH and DHS to amend and review Privacy Policies.	DoH DHS	High
	Recommendation 2. Improved openness in Privacy Policies about data sharing / matching	DoH and DHS to amend and review Privacy Policies.	DoH DHS	High
	Recommendation 3. Establish an online resource to improve openness and transparency about data sharing / matching	DoH to establish new online resource.	DoH	Medium
	Recommendation 4. Improve openness and transparency at partner agencies / data sources regarding data sharing / data matching with the Department of Health	DoH to reach agreements with data sources on openness.	DoH	Medium
APP 3 – Collection of solicited personal information	**Recommendation 5.** Minimisation of data collection	Data minimisation requirements to be added to: • The proposed legislative framework • Additional governance arrangements; and • Agreements with data custodians.	DoH	Low
APP 5 – Notification	**Recommendation 6.** Amend privacy notices to clarify scope of third party data collection	DoH and DHS to amend and review Privacy Notices.	DoH DHS	Medium
	Recommendation 7. Amend privacy notices to clarify the scope of data matching	DoH and DHS to amend and review Privacy Notices.	DoH DHS	Medium
APP 10 – Quality of Personal Information	**Recommendation 8.** Assess data quality benefits and risks	DoH to undertake a trial / evaluation for each proposal: • Proposal 1: TGA – yet to be scheduled • Proposal 2: MBS/PBS – yet to be scheduled • Proposal 3: Insurers – yet to be scheduled • Proposal 4: Home Affairs – completed • Proposal 5: AHPRA – yet to be scheduled • Proposal 6: DVA – completed • And all future proposals.	DoH Data custodians	Low

APP 11 – Security	**Recommendation 9.** Establish a security compliance framework	DoH to establish a minimum security standard and add it to: • Additional governance arrangements; and • Agreements with data custodians.	DoH	**High**
	Recommendation 10. Expansion of data destruction requirements	DoH to establish data destruction requirements and add them to: • The proposed legislative framework • Additional governance arrangements; and • Agreements with data custodians.	DoH	**Medium**
APP 13 – Correction	**Recommendation 11.** Sharing corrections	DoH to establish a protocol for sharing relevant data corrections with data custodians.	DoH	**Low**
Section 18. Governance	**Recommendation 12.** Establish privacy governance arrangements and then review, strengthen and enhance on a regular basis	DoH to enhance / upgrade some governance arrangements	DoH	**High**