Australian Government

Department of Health

Health Legislation Amendment (Data-matching) Bill 2019

Response to Privacy Impact Assessment for Fraud detection and compliance activities

The Department of Health (Health) is proposing changes through the Health Legislation Amendment (Data-matching) Bill 2019 (the Bill) to establish a new scheme of data matching for specified Medicare compliance purposes.

The Chief Executive Medicare is responsible for protecting the integrity of the Commonwealth's health payment systems.

To examine the privacy risks associated with the Bill and Health's application of the legislation, a Privacy Impact Assessment (PIA) has been completed by independent, external assessors. This PIA will assist Health to systematically identify and manage privacy issues raised by the introduction of the legislative package.

This document outlines Health's response to recommendations presented in the PIA for data matching for fraud detection and compliance activities.

RECOMMENDATIONS

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.

Departmental response:

Agreed.
Health will work with Services Australia (formerly the Department of Human Services) to ensure Privacy Policies are updated to accurately reflect the scope of data collection and ensure that this information is readily accessible to the public.

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 likely external agencies involved in data sharing / matching. As some initial data collection occurs via the DHS, this recommendation extends to the DHS Privacy Policy.

Departmental response:

Agreed.
Health will work with Services Australia to ensure Privacy Policies are updated to accurately reflect the scope of data sharing and data matching activities, including a list of partner agencies.

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 portal 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.

Departmental response:

Agreed.
The Chief Executive Medicare will maintain a public register to report on all data matching activities.

In addition, Health will comply with *the Guidelines on Data Matching in Australian Government Administration (*the Guidelines*)* which are issued by the Office of the Information Commissioner (OAIC). Health will publish proposed data matching activities through publication of all data matching protocols and a public notice in the Commonwealth Government Gazette.

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.

Departmental response:

Agreed.
Health will work with partner agencies to ensure transparency and awareness that data is collected and used for Medicare compliance purposes, and to ensure that relevant information is available in partner agencies' privacy policies and online resources.

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.

Departmental response:

Agreed.
The legislation will require the Chief Executive Medicare to establish and maintain systems and processes, which will require the use of information is limited to what is reasonably necessary for the purpose of data matching for permitted purposes.

In line with the Guidelines, Health will prepare a program protocol and technical standards report, which will detail the reasons for matching specific data fields, that will be submitted to and available for review by the OAIC.

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.

Departmental response:

Agreed.
Health will work with Services Australia to update privacy notices where relevant to accurately describe third party data collection practices.

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.

Departmental response:

Agreed.
Health will work with Services Australia to ensure privacy notices are updated to accurately describe the proposed data matching arrangements.

Recommendation 8 – Assess data quality benefits and risks

The Data Matching Proposal should include a requirement for routine data sharing in controlled data-matching to be assessed regarding the potential data quality benefits and risks.

Departmental response:

Agreed.
The Bill will require the Chief Executive Medicare to establish and maintain systems and processes for ensuring that information that is matched is accurate, up-to-date and complete. As part of these systems and process, an assessment of data quality benefits and risks will be included.

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.

Departmental response:

Agreed in principle.
Health already has strong security measures in place to safeguard data received and retained by the Department, and manages data in accordance with legislative requirements and Australian Government standards, including the Information Security Manual and Protective Security Policy Framework. Other Commonwealth entities are also bound by these standards.

Health will establish a security compliance framework that covers all participants undertaking data matching. The technical standards that will be developed in compliance with the Guidelines will also detail the security arrangements that will be agreed between agencies.

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.

Departmental response:

Agreed.
The Bill will require the Chief Executive Medicare to establish and maintain systems and processes governing when and how information that is matched for Medicare compliance purposes and the results of the matching is to be destroyed.

Recommendation 11 – Sharing corrections

The Department of Health should share all relevant data corrections with third parties involved in data matching.

Departmental response:

Agreed.
Health will update its agreements with third parties to include an obligation for the relevant third party to be responsible for correcting the original dataset.

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 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.

Departmental response:

Agreed.
Health will establish privacy governance arrangements that will be reviewed, strengthened and enhanced in consultation with the OAIC.