OAIC Response to Final Report

Overview

The Office of the Australian Information Commissioner (OAIC) engaged privacy consultancy Information Integrity Solutions Pty Ltd (IIS) to conduct a public consultation from March to June 2021. The consultation involved publishing a consultation paper, inviting submissions and holding two targeted roundtable discussions with key stakeholders to provide input to the review. The OAIC received 23 written submissions and the roundtables were attended by 23 stakeholder representatives from 14 different organisations.

The IIS Final Report was finalised on 27 July 2021. The Final Report made 16 recommendations (some with multiple sub-recommendations) for amending the National Health (Privacy) Rules.

OAIC response to IIS Final Report recommendations

The OAIC has sought to implement the recommendations of the Final Report to the extent possible within the scope of the Information Commissioner's powers under section 135AA of the *National Health Act 1953*, noting that the Act confines the matters which may be dealt with by the Commissioner's rules to those set out in subsection 135AA(5), whilst intending to be privacy preserving some of the recommendations were found to go beyond this scope.

We note that the IIS recommendations were also developed before the *Data Availability and Transparency Act 2022* (the DAT Act) was passed on 30 March 2022. We have since adjusted our response to the IIS recommendations to reflect the impact of the DAT Act, which may also apply to the sharing of claims information by government agencies (and overrides the application of the Rules in some instances).

In revising the Rules, the OAIC has also taken into account significant changes in context since the last substantive revision in 2008. The IIS Final Report pointed to the developments in government information handling and digital technologies which have changed foundational aspects of how the Rules apply in practice. Government initiatives to remove obstacles to information sharing and foster data integration for research and public policy have direct relevance for the Rules. The OAIC has therefore sought to update the Rules where appropriate so that they continue to be fit for purpose while ensuring that the use and disclosure of claims information remains subject to strict controls, in line with community expectations in relation to sensitive MBS and PBS claims data.

The OAIC has engaged with government agencies including Services Australia, the Department of Health and Aged Care, and the Office of the National Data Commissioner while developing the new draft Rules.

Key features of the new draft Rules

The key features of the new draft Rules are:

- Simplified structure and greater clarity, including in relation to the Rules' application to government agencies and operation of provisions relating to data separation, old information, and disclosures for medical research purposes
- Introduction of express provisions to authorise the use of claims information

- Requirements for data-sharing agreements to govern the disclosure of claims information to government agencies by Services Australia or the Department of Health and Aged Care
- Introduction of the principle of data minimisation which will apply to most authorised uses and disclosures as well as all authorised linkages of claims information
- Aligned destruction of linkage requirements for all agencies subject to the Rules, to ensure valuable public policy uses can continue and for greater consistency with other data governance frameworks
- Amendments to ensure the traceability of linkages conducted in accordance with the Rules

IIS Recommendation		OAIC Response
1 Keep the Rules technology neutral to the extent possible		**Agreed in part**
2 Clarify the application of the Rules to agencies	2.1 Revise the Rules to apply to 'primary agencies' and 'secondary agencies'	**Agreed in part**
	2.2 Define 'primary agency'	**Agreed in part**
	2.3 Define 'secondary agency'	**Agreed in part**
	2.4 Divide the Rules into parts	**Agreed in part**
	2.5 Specify the application of Parts 3 and 4	**Agreed in part**
3 Amend the Rules to clarify the application of the Data Availability and Transparency Bill (DATB)	3.1 Clarify the provisions in the Rules that are unaffected by the DATB	**Not adopted**
	3.2 Revise disclosure provisions in the Rules to clarify interaction with the DATB	**Not adopted**
	3.3 Apply data minimisation to DATB sharing requests	**Agreed in part**
	3.4 Require data sharing agreements to prohibit re-identification	**Agreed in part**
4 Prohibit secondary uses resulting in individuated intervention	4.1 Prohibit secondary use for the purpose of individuated intervention	**Not adopted**
	4.2 Prohibit disclosure for a purpose that would result in individuated intervention	**Not adopted**
	4.3 Define the meaning of individuated intervention	**Not adopted**
5 Require the use of data sharing agreements for disclosure	5.1 Require agencies to use data sharing agreements when disclosing claims information	**Agreed**

IIS Recommendation		OAIC Response
	5.2 Require the data sharing agreement to include certain mandatory items	**Agreed**
	5.3 Remove overlap with data sharing agreement requirements under the DATB	**Not adopted**
	5.4 Include the data sharing agreement requirement in Part 2 of the Rules	**Agreed in part**
6 Prohibit release of unit level claims information as open data		**Not adopted**
7 Formally impose governance and security requirements that align with Australian Privacy Principles (APPs) 1 and 11	7.1 Introduce an APP 1.2-like requirement into the Rules	**Not adopted**
	7.2 Move cl 14(3) to (proposed) Part 2 of the Rules	**Not adopted**
	7.3 Require agencies to publish information about their handling of claims information	**Not adopted**
	7.4 Introduce an APP 11.1-like requirement into the Rules	**Not adopted**
8 Clarify data separation arrangements	8.1 Explore options to modulate cl 6 to clarify relationship with linkage provisions	**Agreed**
	8.2 Extend cl 7(1), 7(2) and 7(3) to 'primary agencies'	**Agreed**
	8.3 Remove duplication between cl 6 and cl 7(1)	**Agreed**
9 Strengthen security requirements	9.1 Formally bind agencies to the Information Security Manual (ISM), Protective Security Policy Framework (PSPF) and Essential Eight	**Not adopted**
	9.2 Require primary agencies to develop, and report against, a security plan	**Not adopted**
	9.3 Require primary agencies to impose access controls	**Not adopted**
	9.4 Repeal the technical standards provision	**Not adopted**

IIS Recommendation		OAIC Response
10 Clarify disclosure requirements for primary agencies	10.1 Group disclosure requirements (applying to primary agencies) in one place	**Agreed**
	10.2 Simplify provisions enabling data sharing between primary agencies	**Agreed**
	10.3 Clarify and rationalise individual access provisions	**Agreed in part**
	10.4 Broaden the application of cl 7(9)	**Agreed in part**
	10.5 Consider whether Rules should permit disclosure with PICs to secondary agencies	**Agreed in part**
	10.6 Clarify disclosure provisions where agency is both a primary and secondary agency	**Not adopted**
11 Require publication of reports and linkage traceability	11.1 Require primary agencies to publish linkage reports	**Not adopted**
	11.2 Ensure linkage under cl 8 and 10 is traceable	**Agreed**
12 Clarify certain aspects of old information provisions	12.1 Reframe cl 10 to apply to primary agencies	**Agreed in part**
	12.2 Clarify the scope of cl 10(1)(b)	**Agreed**
	12.3 Clarify whether old information must be stored separately from new	**Agreed**
13 Clarify that medical research provisions apply to primary agencies	13.1 Clarify that cl 11 applies to primary agencies	**Agreed**
	13.2 Explore the desirability of the Rules aligning more closely with the format of s 16B(3) (in the Privacy Act)	**Not adopted**
	13.3 Provide for consultation between agencies subject to the Rules	**Agreed**
14 Do not extend cl 11 to include other forms of research (other than medical research)		**Agreed**
15 Revise signed undertaking requirements in cl 11 to account for varied data retention requirements		**Agreed**
16 Explore options to broaden the application of clauses 13 and 14	16.1 Explore options for reframing clauses 12 and 13 to cover secondary agencies	**Agreed in part**

IIS Recommendation		OAIC Response
	16.2 Explore options to enable the Rules to better interact with existing integration initiatives	**Not adopted**
	16.3 Consult with affected agencies on reframing clauses 12 and 13	**Agreed**
	16.4 Repeal the indefinite retention provision under cl 12(5)	**Agreed in part**
	16.5 Clarify de-identification standards in the Explanatory Statement	**Agreed**
	16.6 Apply the data minimisation principle to disclosure under cl 12(6)	**Agreed in part**