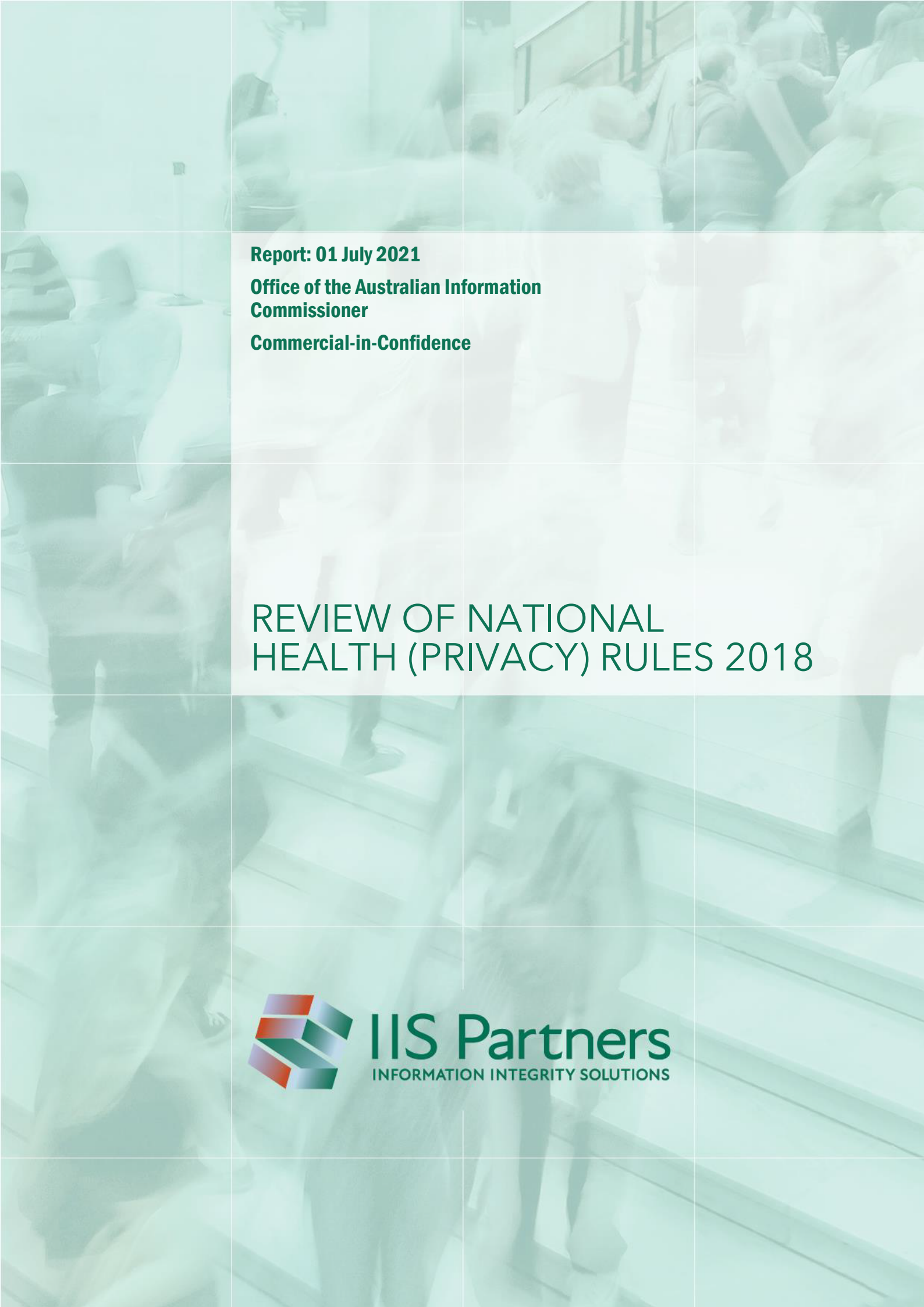


Report: 01 July 2021

Office of the Australian Information Commissioner

Commercial-in-Confidence

REVIEW OF NATIONAL HEALTH (PRIVACY) RULES 2018

IIS Partners
INFORMATION INTEGRITY SOLUTIONS

Contents

Executive summary 1

IIS's overall view 1

Recommendations 2

About this review 6

Why have a review 6

Scope of the review 7

History of the Rules 7

Consultation 8

How to read this report 9

1. Form and function of the Rules 11

1.1 Stakeholder views 11

1.1.1 Prescriptive versus principles-based 11

1.1.2 Technology specific versus technology neutral 12

1.2 Review findings 13

1.3 Recommendation 14

2. How the rules apply to agencies 15

2.1 Stakeholder views 15

2.2 Review findings 16

2.2.1 Health provider compliance functions 16

2.2.2 Simplifying the categories of agencies 17

2.2.3 Primary agencies 17

2.2.4 Secondary agencies 18

2.3 Recommendations 18

3. The Rules in context 20

3.1 Government information policy 20

3.2 Stakeholder views 21

3.2.1 Use of claims information for policy and research 21

3.2.2 Restrictions on use of claims information 22

3.2.3 Other initiatives that use claims information 23

3.2.4 Interaction with the Data Transparency and Availability Bill 24

3.3 Review findings 24

3.3.1 Interaction with the Data Transparency and Availability Bill 25

3.3.2 Use and linkage for public policy purposes 26

3.3.3 Use and disclosure for individuated interventions 26
3.3.4 Disclosure of claims information 28
3.3.5 Open release of de-identified claims information 28
3.4 Recommendations 29
4. Interaction with the APPs 34
4.1 Stakeholder views 34
4.1.1 General interaction with APPs 34
4.1.2 Interaction with APP 1 35
4.1.3 Interaction with APP 6 35
4.1.4 Interaction with APP 11 36
4.2 Review findings 36
4.2.1 'Claims information' versus 'personal information' 36
4.2.2 Formally imposing an APP 1.2-like requirement 37
4.2.3 Formally imposing transparency requirements 37
4.3 Recommendations 37
5. Data separation 39
5.1 Overview 39
5.2 Stakeholder views 39
5.3 Review findings 40
5.3.1 Data separation under cl 7 40
5.3.2 Data separation by Services Australia under cl 8 41
5.4 Recommendation 41
6. Primary agencies: Technical standards and PINs 43
6.1 Overview 43
6.2 Stakeholder views 43
6.2.1 Technical standards 43
6.2.2 Medicare PINs 45
6.3 Review findings 46
6.3.1 Technical standards and security 46
6.3.2 Assurance 47
6.3.3 Technical standards and access controls 47
6.3.4 Technical standards and data linkage 47
6.3.5 Medicare PIN 47

6.4 Recommendations 48
7. Primary agencies: Disclosure of claims information 50
7.1 Overview 50
7.2 Stakeholder views 52
7.3 Review findings 53
7.3.1 Disclosure provisions generally 53
7.3.2 Information sharing between primary agencies 53
7.3.3 Disclosure to an individual of their own information 54
7.3.4 Disclosure to an enforcement body 54
7.3.5 Disclosure of claims information to a secondary agency 54
7.3.6 Disclosure required by law or 'lawful' disclosure 55
7.3.7 Disclosure to a medical researcher 56
7.4 Recommendations 56
8. Primary agencies: Linkage, retention and reporting 58
8.1 Overview 58
8.2 Stakeholder views 59
8.3 Review findings 59
8.3.1 Linkage by primary agencies 59
8.3.2 Retention of linked claims information 60
8.3.3 Reporting of linkages 60
8.4 Recommendations 60
9. Primary agencies: Handling of old information 61
9.1 Overview 61
9.2 Stakeholder views 61
9.3 Review findings 62
9.4 Recommendations 63
10. Primary agencies: Disclosure for medical research 65
10.1 Overview 65
10.2 Stakeholder views 65
10.3 Review findings 66
10.3.1 Agencies to which the rules applies 66
10.3.2 Alignment with Privacy Act research provisions 67
10.3.3 Inefficiencies related to consent 67
10.3.4 Whether disclosure should be allowed for other forms of research 69
10.3.5 Whether retention periods should be extended 70

10.4 Recommendations 71
11. Secondary agencies: Use and disclosure 74
11.1 Overview 74
11.2 Stakeholder views 74
11.3 Review findings 75
11.3.1 Linkage including name linkage 75
11.3.2 Retention of de-identified claims information 76
11.3.3 Secondary agency disclosure of claims information 76
11.4 Recommendations 77
12. Glossary 78
Appendix A. Questions we asked 81
Appendix B. Stakeholders who made submissions 84
Appendix C. Stakeholders who attended roundtable discussion 86

Executive summary

The Office of the Australia Information Commissioner (OAIC) engaged IIS Partners (IIS) to assist with its review of the National Health (Privacy) Rules 2018 (the Rules) issued under s 135AA of the *National Health Act 1953*. The Rules regulate agency handling of Medicare Benefits Schedule (MBS) and Pharmaceutical Benefits Schedule (PBS) claims information. This report sets out IIS's findings and makes recommendations for how the Rules could be revised in light of developments since the Rules were last reviewed and issues raised by stakeholders.

IIS's overall view

Reviewing the Rules has been complex, due in part to the range of new developments in government information handling and digital technologies which have changed foundational aspects for how the Rules apply in practice. There has been a clear movement in government information policy towards enabling data re-use with several government initiatives seeking to remove obstacles to information sharing and foster data integration for research and public policy. These initiatives have direct relevance for the Rules which restrict use and disclosure of claims information – particularly data linkage.

The review has also been complex due to stakeholder division on how the Rules should look in the future. Government agencies and researchers are understandably keen to make greater use of claims information and remove barriers to that use. Civil society groups, on the other hand, were concerned to maintain protections for claims information, given its sensitivity and its coverage of most of the Australian population.

IIS's view is that claims information deserves ongoing protection over and above the protections offered in the *Privacy Act 1988*. We believe there is an ongoing role for Rules issued under s 135AA of the National Health Act. Claims information reveals health information about individuals who generally do not have a choice about when and how they interact with the health system. Use of that information – particularly secondary use – should therefore be strictly controlled.

Advances in technology have made some privacy risks and impacts more acute. In recognition of this, IIS is recommending some new protections. These include a prohibition on releasing unit-level claims information (even in de-identified form) in an open access environment, a prohibition on secondary use of claims information for individuated intervention and stronger security requirements for agencies that handle claims information. IIS also recommends strengthening governance and transparency through imposing an APP 1-like requirement on agencies requiring them to implement policies, procedures and systems to ensure compliance with the Rules. Such requirements should apply broadly to all agencies that handle claims information.

Advances in technology have also called into question some of the technology-specific directions in the Rules, such as the requirements that MBS and PBS data be stored in separate databases. The review received much stakeholder feedback on the appropriateness or otherwise of such requirements and how they impact on the efficiency of authorised data linkage and disclosure for research. Unfortunately, such requirements are dictated by s 135AA itself and therefore are out of scope for this review. IIS observes only that there may be benefit in considering the ongoing efficacy of such provisions in light of technological change in any future review of s 135AA.

More generally, IIS has made recommendations that seek to simplify what one stakeholder referred to as 'the opaque and complex matrix of responsibilities outlined in the Rules'. This includes reframing the Rules to regulate 'primary' and 'secondary' agencies, rather than its current approach of calling out the responsibilities of individual agencies. This would help to reduce the impact of machinery of government changes on the Rules. In simplifying the Rules in this way, IIS also suggests that disclosure provisions in the Rules be clarified and simplified to make clear that secondary agencies may use claims information (without personal identification components (PICs)) for public policy and research. There must also be greater clarity in how the Rules apply to existing government data integration activities.

Researchers outside of government also raised issues associated with the medical research provisions contained in the Rules. While IIS has sought to address such issues, the problem of consent 'double up' that some stakeholders complained about appears to be a problem in spite of the Rules – that is, the Rules themselves do not require any such double up of consent processes. This is an issue for further consideration outside of this review.

Taken together, the revisions IIS is proposing are significant. In our view, significant revisions are warranted by the significant changes to information policy, technology and practice that have occurred since the Rules were established and last reviewed.

Recommendations

Recommendations
1 Keep the Rules technology neutral to the extent possible
2 Clarify the application of the Rules to agencies 2.1 Revise the Rules to apply to 'primary agencies' and 'secondary agencies' 2.2 Define 'primary agency' 2.3 Define 'secondary agency' 2.4 Divide the Rules into parts 2.5 Specify the application of Parts 3 and 4.

Recommendations
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 3.2 Revise disclosure provisions in the Rules to clarify interaction with the DATB 3.3 Apply data minimisation to DATB sharing requests 3.4 Require data sharing agreements to prohibit re-identification
4 Prohibit secondary uses resulting in individuated intervention 4.1 Prohibit secondary use for the purpose of individuated intervention 4.2 Prohibit disclosure for a purpose that would result in individuated intervention 4.3 Define the meaning of individuated intervention
5 Require the use of data sharing agreements for disclosure 5.1 Require agencies to use data sharing agreements when disclosing claims information 5.2 Require the data sharing agreement to include certain mandatory items 5.3 Remove overlap with data sharing agreement requirements under the DATB 5.4 Include the data sharing agreement requirement in Part 2 of the Rules
6 Prohibit release of unit level claims information as open data
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 7.2 Move cl 15(3) to (proposed) Part 2 of the Rules 7.3 Require agencies to publish information about their handling of claims information 7.4 Introduce an APP 11.1-like requirement into the Rules
8 Clarify data separation arrangements 8.1 Explore options to modulate cl 7 to clarify relationship with linkage provisions 8.2 Extend cl 8(1), 8(2) and 8(3) to 'primary agencies' 8.3 Remove duplication between cl 7 and cl 8(1)

Recommendations
9 Strengthen security requirements 9.1 Formally bind agencies to the Information Security Manual (ISM), Protective Security Policy Framework (PSPF) and Essential Eight[1] 9.2 Require primary agencies to develop, and report against, a security plan 9.3 Require primary agencies to impose access controls 9.4 Repeal the technical standards provision
10 Clarify disclosure requirements for primary agencies 10.1 Group disclosure requirements (applying to primary agencies) in one place 10.2 Simplify provisions enabling data sharing between primary agencies 10.3 Clarify and rationalise individual access provisions 10.4 Broaden the application of cl 8(9) 10.5 Consider whether Rules should permit disclosure with PICs to secondary agencies 10.6 Clarify disclosure provisions where agency is both a primary and secondary agency
11 Require publication of reports and linkage traceability 11.1 Require primary agencies to publish linkage reports 11.2 Ensure linkage under cl 9 and 11 is traceable
12 Clarify certain aspects of old information provisions 12.1 Reframe cl 11 to apply to primary agencies 12.2 Clarify the scope of cl 11(1)(b) 12.3 Clarify whether old information must be stored separately from new
13 Clarify that medical research provisions apply to primary agencies 13.1 Clarify that cl 12 applies to primary agencies 13.2 Explore the desirability of the Rules aligning more closely with the format of s 16B(3) (in the Privacy Act) 13.3 Provide for consultation between agencies subject to the Rules
14 Do not extend cl 12 to include other forms of research (other than medical research)
15 Revise signed undertaking requirements in cl 12 to account for varied data retention requirements

[1] For a short description of the 'Essential Eight', see the Glossary.

Recommendations
16 Explore options to broaden the application of clauses 13 and 14
16.1 Explore options for reframing clauses 13 and 14 to cover secondary agencies
16.2 Explore options to enable the Rules to better interact with existing integration initiatives
16.3 Consult with affected agencies on reframing clauses 13 and 14
16.4 Repeal the indefinite retention provision under cl 13(5)
16.5 Clarify de-identification standards in the Explanatory Statement
16.6 Apply the data minimisation principle to disclosure under cl 13(6)

About this review

IIS is assisting the OAIC with its review of the National Health (Privacy) Rules 2018 (Rules) to decide whether and how they need to be updated. The Rules are a legislative instrument issued by the Information Commissioner under section 135AA of the *National Health Act 1953*. They apply to Medicare Benefits Schedule (MBS) and Pharmaceutical Benefits Schedule (PBS) claims information. People make claims under the MBS and PBS for health services in Australia. To enable this, Services Australia and the Department of Health process and store information about MBS and PBS claims.

The Rules apply to Australian Government agencies that handle MBS and PBS information with particular focus on Services Australia and the Department of Health. In brief, the Rules:

- Require that information obtained from the MBS and PBS is not stored in the same database
- Specify when claims information from the two programs may be linked
- Prohibit claims information over five years old (referred to as 'old information') from including information that could identify an individual, and
- Specify the circumstances in which old information may be re-linked with identifiers.

Why have a review

The Rules are due to repeal on 1 April 2022. This review and the associated stakeholder consultation are to enable the revision and remaking of the Rules before that date. Other factors that indicate that a review is timely include:

- Developments in information technology since 2008, which is when the contents of the Rules were last examined in depth
- The introduction of the Australian Privacy Principles (APPs) which may have changed baseline regulatory protections otherwise afforded to claims information
- The regularity and increased scale of use of information technology in the planning and provision of health services
- Public policy approaches favouring data use and re-use in research, evidence-based decision-making and the provision of government services generally
- Community attitudes and expectations regarding the handling of their personal information; in particular, certain health information.

Submissions to the review assisted the Commissioner to assess the need for revisions or amendments to the Rules.

Scope of the review

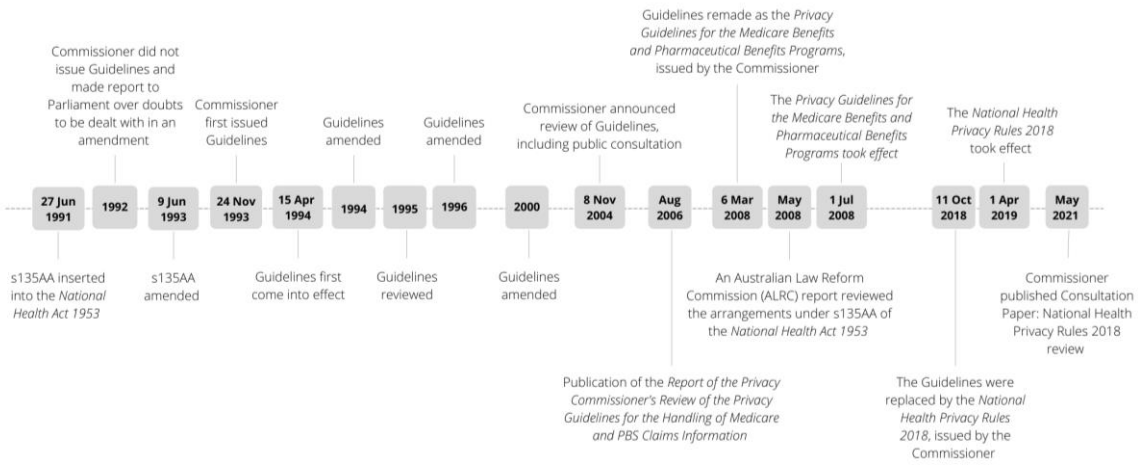
The review is a general review of all the provisions of the Rules. As with previous reviews, the objective is to ensure that the Rules, in their current form, achieve the intent of section 135AA of the National Health Act and are easy to read, understand and apply in practice. Section 135AA(5) lists matters that the Rules must cover which includes:[2]

- Storage of claims information and the circumstances in which creating copies of the information in paper or similar form is prohibited.
- Permitted uses of claims information.
- Permitted disclosures of claims information.
- Data separation requirements – including the requirement that agencies be prohibited from storing MBS and PBS information in the same database.
- Restrictions on linkage of MBS and PBS information.
- Requirements for old information including requirements that old information be stored apart from personally identifiable components and requirements for longer term storage and retrieval.

The Information Commissioner cannot revise the Rules in a way that would derogate from those requirements in the primary legislation. Therefore, where this report suggests revisions to the Rules, it does so within the boundaries of s 135AA(5). That said, where there are obvious issues or difficulties with the primary legislation, the report records those issues as 'observations' rather than recommendations for consideration in future law reform processes.

History of the Rules

Since s 135AA was inserted into the National Health Act in 1991, the Rules (previously referred to as 'Guidelines') have been made and amended many times.



[2] *National Health Act 1953,* s 135AA(5).

The original justification for the enactment of s 135AA was to act as a counterweight to government proposals in 1989 and 1990 that sought to introduce an online system for checking of pharmaceutical benefits eligibility. Introduction of such a system, which would involve sharing of sensitive identifiable information about individuals, necessitated governance by a strong privacy framework, hence the introduction of s 135AA. Ultimately, the government proposals for entitlements checking did not go ahead, however s 135AA remained in recognition of the inherently sensitive nature of MBS and PBS claims information. Parliamentary debates and the second reading speech (to the Bill that amended the National Health Act to introduce s 135AA) point to a narrow range of purposes for which it was envisaged that claims information would be used.[3] Primarily, those purposes related to reducing fraudulent claims and other forms of overpayment against the MBS and PBS schemes, with uses beyond this requiring clear and compelling justifications.[4]

The Explanatory Statement to the Rules explains that: '[t]he policy intent of the enabling provision for the Rules, section 135AA of the National Health Act, is to recognise the sensitivity of health information and restrict the linkage of claims information.' Indeed, '[s]uch linkages, may reveal detailed information on the health status and history of the majority of Australians, beyond what is necessary for the administration of the respective programs.'[5]

Consultation

The OAIC invited comment from interested individuals, agencies and organisations on all elements and aspects of the Rules, including but not limited to their effect on individuals, the operation of MBS and PBS processes, public sector operations and policy development, open data and associated research initiatives.

Questions in the Consultation paper, dated May 2021, provided a guide and were intended to elicit feedback relevant for the review. Participants were encouraged to provide data, examples, case studies, or other evidence to support the arguments presented in their submissions. The closing date for submission was Friday 4 June 2021.

In addition to the formal consultation paper process, IIS also held two roundtable sessions to elicit in-person feedback. A list of stakeholders who made submissions is included at Appendix B of this report. A list of stakeholders who attended and participated in consultation roundtable discussions, is set out at Appendix C of this report.

Stakeholder feedback has been important to shaping IIS' analysis and helping us understand where the key problems or issues lay in relation to the Rules. Comments received via submissions and roundtable sessions have been summarised and appear in the 'Stakeholder views' subsection of each section of the report.

[3] Office of the Privacy Commissioner, *Report of the Privacy Commissioner's Review of the Privacy Guidelines for the Handling of Medicare and PBS claims information*, August 2006.

[4] Office of the Privacy Commissioner, *Report of the Privacy Commissioner's Review of the Privacy Guidelines for the Handling of Medicare and PBS claims information*, August 2006.

[5] National Health (Privacy) Rules 2018 Explanatory Statement.

How to read this report

Analysis of the Rules is organised by theme in sections 1 to 11. Recommendations appear at the end of each section. Sections 1-5 consider a range of general matters related to the Rules and how they apply to agencies. In that analysis, IIS proposes simplifying the way that the Rules apply to agencies and introduces the concepts of 'primary agency' and 'secondary agency.' Sections 6-10 then analyse provisions in the Rules that regulate the activities of primary agencies, while section 11 focuses on provisions applying to secondary agencies. The main sections are as follows:

1. *Form and function of the Rules* – in which IIS addresses questions of whether the Rules should be prescriptive or principle-based, technology specific or technology neutral.
2. *How the Rules apply to agencies* – in which IIS suggests simplifying the way the Rules apply to different agencies and introduces the concepts of 'primary agency' and 'secondary agency.'
3. *The Rules in context* – in which IIS considers the broader government information policy landscape and the interaction of the Rules with the Data Availability and Transparency Bill.
4. *Interaction with the APPs* – in which IIS suggests that elements of APP 1 and 11 be introduced into the Rules, noting that this 'raises the bar' as protections will apply to de-identified claims information as well as identified.
5. *Data separation* – in which IIS addresses some areas of difficult associated with storing MBS and PBS data in separate databases and considers how this requirement applies to data integration projects that use de-identified data.

Analysis of provisions that regulate claims information handling by primary agencies:

6. *Technical standards and PINs* – in which IIS suggests strengthening security requirements applying to claims information.
7. *Disclosure of claims information* – in which IIS draws together the various disclosure provisions in the Rules and considers how they may be simplified and reframed.
8. *Linkage, retention and reporting* – in which IIS reviews linkage provisions applying to primary agencies and suggests greater transparency in reporting.
9. *Handling old information* – in which IIS addresses inefficiencies created by separate storage requirements applying to old information and suggests the Rules clarify some aspects of the relevant provision.
10. *Medical research* – in which IIS considers issues raised by stakeholders about the operation of disclosure mechanisms for medical research and suggests some revisions to the applicable provision in the Rules.

Analysis of provisions that regulate claims information handling by secondary agencies:

11. *Use and disclosure* – in which IIS considers how the Rules should apply to secondary agencies and whether existing provisions (applying to Department of Health) need to be revised.

Throughout the report, IIS uses ‘claims information’ interchangeably with ‘MBS and PBS data’. By ‘claims information’ we mean ‘information to which the Rules apply.’ IIS also refers to ‘personal identification components’ as ‘PICs’. Claims information, PICs and other terms are defined in the Glossary at the end of the report.

1. Form and function of the Rules

The Rules are relatively prescriptive in form. They give specific instructions on how specific agencies must store and handle claims information and the limited circumstances in which claims information may be linked, retained or rendered identifiable. This contrasts with the APPs, for example, which take a principles-based approach to regulating personal information, allowing entities greater discretion in interpreting the application of the legislation to their own circumstances.

Generally, subordinate legislation – like the Rules – would be expected to be more prescriptive than primary legislation. It adds detail and specificity to the framework established by legislation. Specificity is encouraged because subordinate legislation can be revised and updated more easily than primary legislation – it does not have to be passed by Parliament, though may be disallowable. A prescriptive approach can have the positive effect of eliminating known privacy risks that would otherwise confront an agency when, for example, making decisions about claims data linkage. On the other hand, an overly prescriptive approach can inadvertently block reasonable activities or be complex to apply in practice.

The Consultation Paper asked stakeholders whether it was desirable for the Rules to take a prescriptive or principles-based approach. While more stakeholders were in favour of a prescriptive approach to ensure certainty about use of claims information, some noted that the complexity of the Rules was undermining their effectiveness.

1.1 Stakeholder views

1.1.1 Prescriptive versus principles-based

More stakeholders were in favour of the Rules taking a prescriptive approach than a principles-based approach.[6] Those in favour of a prescriptive approach were concerned to avoid ambiguity and loose interpretations of the Rules that might enable function creep.[7] A prescriptive approach would also give the public certainty in how claims data may be handled.[8] Some stakeholders suggested that the Rules be more prescriptive in certain areas, for example: that Part 2 be more prescriptive; that the Rules contain more specificity in relation to cybersecurity requirements, and that the Rules introduce provisions to manage re-identification threats.[9] Figure 1 illustrates the general split in stakeholder views:

[6] Stakeholders in favour of a prescriptive approach included AIDH, APF, CHF, the Law Society of NSW, MSIA, NSWCCL, and the Pharmacy Guild of Australia. HIMAA was in favour of a more prescriptive approach on consent but less prescriptive approach on Rule 7. Stakeholders in favour of a more principles-based approach included ABS, AHHA, Department of Health and Monash University.

[7] See for example, CHF p 6, MSIA p 5, Pharmacy Guild of Australia p 3.

[8] See CHF pp 5-6.

[9] See AIDH p 2, Law Society of NSW p 1, APF pp 5, 7.

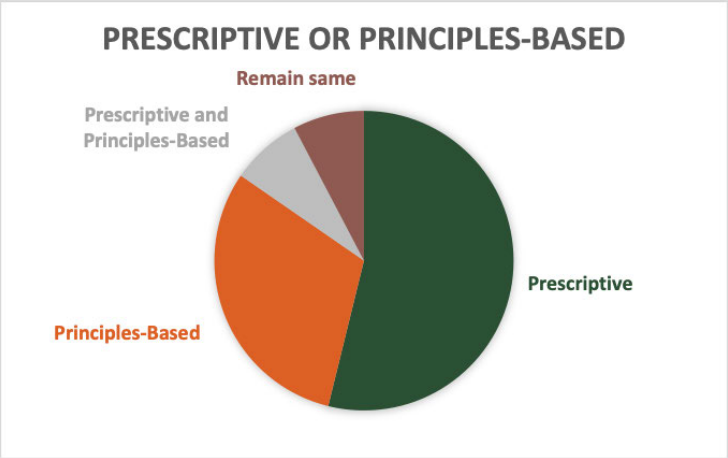


Figure 1.

Those in favour of a principles-based approach pointed out that this would allow greater flexibility in accommodating changing technology and aligning with Government policy on data use.[10] The Department of Health observed that some provisions imposing specific requirements were not clearly associated with managing privacy risk.[11] This created uncertainty as to the intent of individual clauses – an issue that could be addressed via a principles-based format.

1.1.2 Technology specific versus technology neutral

Stakeholders were generally in favour of the Rules being technology neutral to better accommodate technological change.[12] Some believed that the Rules were already adequately technology neutral[13] and did not see a problem with how the Rules dealt with 'databases'[14] and data separation.[15] A roundtable participant pointed out that the National Health Act definition for database was 'a discrete body of information stored by means of a computer' and that this did not appear to unreasonably limit the operation of this term in the Rules. The Professional Services Review Agency (PSRA) noted that a change to the storage related provisions may have cost implications for those agencies that had invested in adjusting IT systems to comply with the Rules.[16]

[10] See ABS pp 3-4, AHHA p 2, Department of Health p 4.

[11] See Department of Health p 3.

[12] See ADHA pp 1, 2, AHHA p 2, Department of Health p 4, HIMAA p 6, Law Society of NSW p 2, MSIA p 5.

[13] See Liberty Victoria p 1.

[14] See HIMAA p 6, Law Society of NSW p 2.

[15] See NSWCCL p 5.

[16] See PSRA p 1.

Others thought the Rules had been overtaken by changes to technology. In this regard, the Department of Health pointed to references to 'databases' and 'paper copies'.[17] Some stakeholders believed that data separation requirements were out-of-date and no longer meaningful[18] particularly given that there were now more secure options available than data separation for use and storage of claims information.[19] Data separation is discussed in more detail in section 5.

While the Consumer Health Forum (CHF) supported updating the Rules to reflect changes to technology-related terminology, particularly in relation to data storage systems, other civil society groups emphasised that technological advances should not be used to justify changes to the Rules that overrode privacy protections.[20]

The Australian Privacy Foundation (APF) wished to see greater specificity in the Rules concerning requirements for agencies to use privacy enhancing technologies such as homomorphic encryption.[21] The Australasian Institute of Digital Health (AIDH) suggested the Rules be more prescriptive on de-identification requirements, given increasing re-identification risks.[22]

1.2 Review findings

The Rules should remain prescriptive but must be simplified. The current complexity of the Rules – partly an effect of incremental change over time – is undermining their effectiveness, creating undue difficulty in applying the Rules in practice and needless delays for authorised uses of the information. IIS recommends that the way the Rules apply to agencies be simplified and that the narrow remit of Part 2 of the Rules (applying to all agencies) be widened. It is not logical for the Department of Health to be regulated heavily by the Rules in relation to its handling of claims information while the Rules remain nearly silent on the activities of other agencies that handle claims information. These issues are taken up in more detail in section 2 and section 11.

IIS agrees with many stakeholders that the Rules should be technology neutral, to the extent permitted by s 135AA. Although outside the scope of this review, there is a case to be made for amending s 135AA to better align with current storage technologies and approaches. Certainly, requirements under s 135AA(5)(a) related to 'paper copies' are no longer meaningful and should be removed. That said, claims information must be securely stored. We recommend specifically requiring agencies to comply with APP 11.1 and otherwise uplifting security settings in the Rules. (For further information, see section 4 and section 6.)

[17] See Department of Health p 4.

[18] See ABS p 4, AIDH p 3, NPS Medicinewise p 2.

[19] HIMAA p 1, Monash University p 6, NPS Medicinewise p 2.

[20] See CHF p 3, Liberty Victory p 1, NSWCCL p 5.

[21] See APF p 9.

[22] See AIDH p 2.

1.3 Recommendation

Recommendation 1 – Keep the rules as technology neutral as possible

When revising the Rules, the Information Commissioner should aim to keep the Rules as technology neutral as possible within the bounds of what is permitted by s 135AA.

Observation – 135AA would benefit from a review of technologically specific terms

Section 135AA would benefit from a review to ascertain whether it requires update in light of technological change. Concepts and other matters that would particularly benefit from review include:

- References to 'database'
- The requirement to store information in separate databases
- How restrictions on linkage should interact with government data integration programs
- Whether new privacy enhancing approaches should be required (to replace data separation, for example).

Requirements in s 135AA related to 'paper copies' should be removed. Any review of s 135AA should take care to maintain strong privacy requirements – modernising s 135AA should aim to adjust it in light of developments in technology without weakening privacy protections. This may, for example, require new privacy requirements to be introduced into s 135AA(5) to replace outmoded ones. Section 135AA should be technology neutral, to the extent possible. Technological specificity, where necessary, should appear in the Rules rather than the primary legislation.

2. How the rules apply to agencies

In the Rules, 'agency' carries the same meaning as in the Privacy Act.[23] In their current form, the Rules contain one provision that applies to all agencies that handle claims information. All subsequent provisions in the Rules apply to Services Australia or the Department of Health or both. In terms of agency coverage, the provisions in the Rules can be broadly divided into four categories:

- The first category includes provisions applying to all agencies – currently this is just clause 7 (which requires agencies to store MBS and PBS data in separate databases).
- The second category includes provisions that apply to Services Australia only – currently this encompasses clauses 8 and 12 (which cover management and storage of claims information, technical standards, use of the Medicare PIN, disclosure to the Department of Health and disclosure for medical research).
- The third category includes provisions that apply to Services Australia and the Department of Health but only in relation to the Department's role in performing 'health provider compliance functions.' The third category encompasses clauses 9, 10 and 11.
- The fourth category includes provisions that apply to the Department of Health but only in relation to handling of claims information that excludes performance of the health provider compliance functions. The fourth category encompasses clauses 13 and 14.

The final clause in the Rules – clause 15 – applies to Services Australia and the Department of Health in a broad sense.

2.1 Stakeholder views

The consultation paper did not ask directly for feedback on how the Rules apply to agencies however some stakeholders drew attention to their convoluted application and uneven coverage.

The APF referred to the 'opaque and complex matrix of responsibilities outlined in the Rules'.[24] The Law Society of NSW highlighted the arbitrary inconsistency of application, pointing out that Part 3 of the Rules (applying to Services Australia and the Department of Health) was significantly more comprehensive than Part 2 (applying to all agencies), and yet it was clear that other agencies handle claims information. In the Law Society's view, if a prescriptive approach to the Rules was maintained: 'then Part 2 of the Rules should also adopt a more prescriptive approach in relation to the disclosure, linkage, and retention requirements of MBS and PBS information by any Government Agency that deals with such data.'[25]

[23] *National Health Act 1953,* s 135AA(11).

[24] APF p 2.

[25] Law Society of NSW p 1.

Both the Department of Health and the Law Society of NSW noted that the handling of claims information by entities outside of the Australian Government (such as by state and territory agencies) fell outside of the Rules.[26] The Law Society queried whether there was scope for greater compliance requirements, in the Rules or elsewhere, for state agencies handling that data.[27]

This uneven coverage means that when Services Australia or the Department of Health disclose claims information (in accordance with the Rules or disclosure provisions in the National Health Act), recipients of the information are free to use the data as they chose, without heeding restrictions on data storage, linkage and retention contained in the Rules.[28] This unevenness is also evident within the Commonwealth. In practice this might mean that when the Department of Health lawfully discloses claims information to another Commonwealth agency, that agency is entitled to undertake linkage activities that the Department itself is not entitled to perform.

The Department of Health also noted that machinery of government changes had impacted the Rules, rendering references to the 'Department of Human Services' (now Services Australia) out of date. The Department suggested the Rules be revised to better accommodate such changes.[29]

2.2 Review findings

2.2.1 Health provider compliance functions

Some of the complexity in how the Rules apply to agencies is due to machinery of government changes. Central among these was a change that moved health provider compliance functions out of the Department of Human Services (now Services Australia) and into the Department of Health. This has meant that provisions in the Rules that originally only applied to Services Australia had to be redrafted to apply to the Department of Health as well, but only in relation the Department of Health's health provider compliance functions and not in relation to its other activities involving handling of claims information.

Category 3 provisions (see above) contain an awkward formulation to accommodate this change. Where previously a provision would have read: 'The Department of Human Services must…' or 'Medicare Australia must…' it now reads 'The Department of Human Services and the Department of Health (where the Department of Health is enabling the Chief Executive Medicare to perform health provider compliance functions) must…'. There are times when this formulation is particularly complicated, for example when the Rules specify how the Department of Health may handle claims information other than in connection with the health provider compliance functions.

[26] Department of Health p 3, Law Society of NSW p 1.

[27] Law Society of NSW p 1.

[28] Department of Health p 3.

[29] Department of Health p 4.

At a minimum, this formulation could be simplified by removing the reference to the Chief Executive Medicare as the role of the Chief Executive Medicare is already encompassed in the definition of 'health provider compliance functions' so repeating this wording is redundant. A simpler formulation might be 'where the Department of Health is supporting the performance of the health provider compliance functions.' Though even this remains complex. IIS believes a more significant change to simplify the Rules is needed.

2.2.2 Simplifying the categories of agencies

There is no inherent reason why the Rules must differentiate between four categories of agency. This approach is both complex and prone to being disrupted by machinery of government changes. That said, there is good reason for agencies like Services Australia, which has the main administrative responsibility for the MBS and PBS (and is therefore the main custodian and conduit for claims information), to be treated differently to others. IIS suggests that the four categories outlined above be collapsed into two categories – 'primary agencies' and 'secondary agencies.' The Rules should then be divided into parts applying to each category.

2.2.3 Primary agencies

Categories 2 and 3 should be merged and treated as one category. In this report, we refer to these agencies as 'primary agencies' but it is open to the OAIC to choose a naming convention that it finds appropriate. The objective should be to move away from referring to specific agencies within the Rules to better future-proof them.

Primary agencies would include Services Australia and the Department of Health where the Department is performing health provider compliance functions. Subject to further advice from the agencies concerned, IIS suggests that the Rules define primary agencies as 'any agency or agencies:

(a) administered by the Minister with administrative responsibility for the Human Services (Medicare) Act 1973 and responsible for enabling administration MBS and PBS schemes or

(b) responsible for enabling the performance of health provider compliance functions.'

IIS has reviewed provisions applying to Services Australia only (category 2) and those provisions lend themselves to being extended to category 3 agencies (with some changes outlined in later sections of this report). The part of the Rules applying to primary agencies should encompass clauses 8, 9, 10, 11 and 12. This part should make clear that it applies to primary agencies only in relation to activities connected with administering the MBS and PBS schemes under the Human Services (Medicare) Act 1973 or connected with supporting the performance of health provider compliance functions.

2.2.4 Secondary agencies

The Rules treat the Department of Health differently to other agencies that handle claims information. It is not clear why this is so. The Rules enable the Department to use and retain claims information for policy and research (as long as the information does not include PICs).[30] However, any such uses involving linkage of MBS and PBS data are strictly limited. Yet such restrictions do not apply to other agencies that handle claims information. In practice, this means that the Department may disclose de-identified claims information to another agency to carry out linkage of MBS and PBS data but cannot conduct such linkage itself.

IIS recommends that this inconsistency be corrected and that the Department of Health be treated the same as other agencies that handle claims information. To that end, we suggest that categories 1 and 4 be merged and treated as one category – 'secondary agencies.' Secondary agencies should be defined as any agency that handles claims information. The part of the Rules applying to secondary agencies should encompass clauses 7, 13 and 14 – though with changes proposed in later sections of this report. This part should make clear that it applies to secondary agencies excluding activities connected with administering the MBS and PBS schemes under the *Human Services (Medicare) Act 1973* or connected with supporting the performance of health provider compliance functions.

2.3 Recommendations

Recommendation 2 – Simplify how the Rules apply to agencies

2.1 Revise the Rules to apply to 'primary agencies' and 'secondary agencies'

The Information Commissioner should revise the Rules to apply to two categories of agency – primary agencies and secondary agencies. Primary agencies would encompass category 2 and 3 agencies. These are the agencies that use claims information for the primary purpose of administering the MBS and PBS schemes and for overseeing health provider compliance with the schemes. Secondary agencies would encompass category 1 and 4 agencies. These are agencies that use claims information for a secondary purpose including public policy and research.

2.2 Define 'primary agency'

Subject to further advice from the agencies concerned, the Rules should define primary agencies as 'any agency or agencies:

(a) administered by the Minister with administrative responsibility for the Human Services (Medicare) Act 1973 and responsible for enabling administration of the MBS and PBS schemes or

(b) responsible for enabling the performance of health provider compliance functions.'

2.3 Define 'secondary agency'

[30] See National Health (Privacy) Rules 2018, cl 13(5).

Subject to further advice from the agencies concerned, the Rules should define a secondary agency as any agency that handles claims information.

An agency may be both a primary agency in relation to some of its activities and a secondary agency in relation to other activities, as is the case currently with the Department of Health. Recommendation 2.5 addresses this matter.

2.4 Divide the Rules into parts

Currently, Part 1 of the Rules contains introductory provisions and definitions. The rest of the Rules should be divided into three parts. Part 2 should apply to both primary and secondary agencies. It would encompass existing cl 7 along with other matters recommended in this report applying to both agency types.

Part 3 should apply to primary agencies. This part would include existing clauses 8, 9, 10, 11 and 12. Part 4 should apply to secondary agencies. This part would include existing clauses 13 and 14.

2.5 Specify the application of Parts 3 and 4

The Rules should specify that Part 3 applies to primary agencies only in relation to activities connected with administering the MBS and PBS schemes under the *Human Services (Medicare) Act 1973* or connected to supporting the performance of health provider compliance functions.

The Rules should specify that Part 4 applies to secondary agencies excluding activities connected with administering the MBS and PBS schemes under the *Human Services (Medicare) Act 1973* or connected with supporting the performance of health provider compliance functions.

3. The Rules in context

The Commissioner cannot create rules that ignore or weaken the application of section 135AA of the National Health Act. Section 135AA prescribes certain matters that must be contained in the Rules. However, there may be opportunities within the Rules and the parameters of section 135AA to retain privacy safeguards while acknowledging Australia's maturing approach to data use and the government's ongoing digital transformation.

Some now believe that the Rules get the balance wrong between privacy and data use. A chief criticism of the Rules in a recent Senate Committee report was that the heavy weighting of information privacy considerations denied legitimate opportunities to access MBS and PBS datasets for research in the public interest. The Rules were characterised in some submissions to the Senate Committee as over-cautious, cumbersome and, according to the Productivity Commission, 'complex with the restrictions creating unnecessary downsides and delays for evidence-based policy formulation'.[31]

3.1 Government information policy

Over the past decade, the movement in government has been towards unlocking the value of public sector information. This has occurred via a range of initiatives beginning with reforms to the Freedom of *Information Act 1982* (FOI Act) in 2010 which sought to change the FOI Act from a 'pull model' for information release to a 'push model', placing an obligation on agencies to proactively publish information.[32] In conjunction with those FOI reforms, the government established the OAIC which, soon after its formation, published Principles on open public sector information. The principles identify information held by agencies as a 'valuable national resource' and encourage agencies to adopt a default position of open access to information where there is no legal need to protect information.[33]

In 2015, the Australian Government became a member of the Open Government Partnership (OGP), an international initiative aimed at increasing the transparency and accountability of government.[34] Australia's 2018-20 OGP National Action Plan committed Australia to improving the sharing, use and reuse of public sector data.[35] According to the Action Plan, this is to be achieved largely through the enactment of the Data Availability and Transparency Bill (DATB) and the establishment of a National Data Commissioner. If enacted, the DATB will create a national scheme for organisations to request access to government-held data in a controlled manner for prescribed purposes, namely: improving government service delivery; informing government policy and programs; and research and development.

[31] Senate Select Committee on Health, Sixth Interim Report, Big health data: Australia's big potential, 2016, at 4.19.

[32] See OAIC, *FOI guide*, Part A.

[33] See OAIC, *Principles on open public sector information*, principle 1.

[34] See OAIC, *Open government*.

[35] See Department of the Prime Minister and Cabinet, *Australia's second Open Government National Action Plan 2018-20*, Improve the sharing, use and reuse of public sector data.

Numerous other reports and initiatives have sought to foster the movement towards greater use of government data, particularly for research and public policy outcomes, including: the *Multi-Agency Data Integration Project (MADIP)* (commenced in 2015) which occurs in conjunction with the *Commonwealth arrangements for data integration for statistical and research purposes*; the *Public sector data management* report (2015) leading to, amongst other things, the Government's *Public Data Policy Statement* (2015); the Productivity Commission's *Data Availability and Use* report (2017); and the Department of the Prime Minister and Cabinet's (DPMC) *Best practice guide to applying the data sharing principles* (2019).

In the health context, this has also included the aforementioned Senate Committee's report, *Big health data: Australia's big potential* (2016) and the signing of the *National Health Reform Agreement* (2020-25). The National Health Reform Agreement commits Commonwealth, state and territory governments to six long-term health reforms including 'enhanced health data' and outlines an intention to expand government use of health data, including through review of 'relevant legislation and regulations across Australia to provide recommendations on ways to support better data linkage while ensuring appropriate protections for patient privacy.'[36]

The Senate Committee's *Big Health Data* report recommended the Australian Information Commissioner review the Rules to enable 'improve[d] access to de-identified MBS and PBS data for the purpose of health policy evaluation and development as well as research undertaken in the public interest, in ways that don't decrease privacy.'[37]

3.2 Stakeholder views

There was a distinct split in stakeholder views on how permissive or restrictive the Rules should be regarding use of claims information – particularly secondary use. The split was between government agencies and researchers on one hand and civil society groups on the other.

3.2.1 Use of claims information for policy and research

Commonwealth government agencies that made submissions to the review supported use of claims data for public policy and research.[38] Researchers and health-related entities were particularly concerned to ensure that the Rules continued to enable medical research and that revisions to the Rules removed obstacles or inefficiencies affecting use of claims information for that purpose.[39]

[36] *Addendum to the National Health Reform Agreement*, 2020-25, pp 63-64.

[37] Senate Select Committee on Health, *Sixth Interim Report, Big health data: Australia's big potential*, 2016, recommendation 5.

[38] See ABS p 2, Department of Health pp 1-2, DPMC p 2, ADHA p 1.

[39] See AHHA p 1, AIHW p 1, Department of Health, Tasmania, p 1, HIMAA p 1, Monash University p 3, PHRN p 2.

In line with existing government data policy, the Department of Health and DPMC both noted that claims data was a national resource that should be used for public benefit.[40] Indeed, DPMC pointed out that the *Best practice guide to applying the data sharing principles* created a 'responsibility to share' for agencies and suggested that the Rules better align with the data sharing principles.[41]

The Department of Health particularly noted the importance of linked datasets in analysing complex questions by allowing new insights that might not be available from a single data source.[42] Such insights could support best practice policy, evaluation and service planning. The Department observed that '[t]he ability to link key health datasets is critical to understanding patient pathways through the health system, and implications for patient health outcomes.'[43] However, at present the Rules strictly limit the Department's ability to link MBS and PBS data. For example, it would, in the Department's view, be 'extremely beneficial' if the Rules enabled the analysis of a linked MBS and PBS dataset to inform the Government's response to the COVID-19 pandemic and to evaluate the policy and program interventions being put in place.[44] This activity is currently blocked by the Rules.

While advocating greater use of claims information or greater clarity on permitted uses of claims information, all agencies and researchers noted the importance of privacy protections, particularly in maintaining public trust.

3.2.2 Restrictions on use of claims information

Civil society groups were united in calling for strict protection of claims information and no loosening of restrictions applying to its use. Some pointed out that people want more privacy not less and cited figures from the OAIC's most recent community attitudes survey which found that 83% of Australians want government to provide more protection of the privacy of their data and 84% of Australians consider it to be a misuse of their information when supplied to an organisation for a specific purpose and then used for another purpose.[45] The same survey found moderate concern with government agencies sharing personal information with other agencies (36% were comfortable with sharing versus 40% uncomfortable) and high concern with agencies sharing personal information with businesses (15% comfortable with sharing and 70% uncomfortable).[46]

[40] See Department of Health p 1, DPMC p 1.
[41] See DPMC p 2.
[42] See Department of Health p 2.
[43] Department of Health p 2.
[44] Department of Health p 2.
[45] See Calabash Solutions p 8, CHF p 3, NSWCCL p 3.
[46] OAIC, *Australian Community Attitudes to Privacy Survey*, 2020.

Generally, civil society groups and others found the Rules got the balance right on privacy and that it was appropriate that the Rules heavily constrained secondary use of claims information.[47] Indeed, some believed the Rules did not go far enough in controlling secondary use – particularly where this involved identified information.[48] Liberty Victoria and APF were both concerned that the desires of governments and researchers were eclipsing privacy rights and that personal information was wrongly treated as an asset rather than as a record of individual treatment.[49] This got the balance wrong in their view. Protecting privacy should be the starting point for revising the Rules, not opportunities created by new technologies.[50]

The Law Society of NSW and NSW Council for Civil Liberties (NSWCCL) both observed that individuals had little control over their interaction with services like healthcare and therefore data use must be fair and proportionate to ensure ongoing public trust in the system.[51] This should mean that secondary use of claims data is extremely limited. Moreover, MBS and PBS data is highly sensitive, potentially revealing information about a person's mental health, or whether they have a sexually transmitted infection or a rare disease.[52] Access to, and use of, that data should therefore be heavily constrained, to ensure public confidence in providing it.[53]

3.2.3 Other initiatives that use claims information

Stakeholders identified a range of other initiatives and frameworks that form part of the landscape in which the Rules operate. MBS and PBS data is included in integrated data assets established under MADIP and the Australian Institute of Health and Welfare's (AIHW) National Integrated Health Services Information Analysis Asset (NIHSIAA).[54] Such datasets are made available to government and non-government researchers in de-identified form in accordance with data governance arrangements such as the Five Safes. The Australian Digital Health Agency (ADHA) gives individuals access to their own MBS and PBS data via the My Health Record system, however, the provision of such information in that context is excluded from the operation of the Rules by s 135AA(5AA).[55] More broadly, the *My Health Records Act 2012* authorises secondary use of My Health Record data (which includes MBS and PBS data) for research or public health purposes.

MBS and PBS information and other health data is also collected and used under the Practice Incentives Program. Under the program, Primary Health Networks (PHNs) collect de-identified health information from general practices and use it to provide feedback to general practices to help practices identify priority areas and quality improvement activities.

---

[47] See CHF p 4, Law Society of NSW p 1, NSWCCL p 4, Pharmacy Guild p 3.

[48] See Law Society of NSW p 5.

[49] See APF p 3, Liberty Victoria p 1.

[50] See AIDH p 2, APF p 6, Liberty Victoria p 1, NSWCCL p 5.

[51] See Law Society of NSW p 3, NSWCCL pp 4-5.

[52] See Law Society of NSW p 3.

[53] See Law Society of NSW p 3.

[54] See Department of Health p 2.

[55] See ADHA p 1.

The APF was concerned about this widening use of claims information and the over-reliance on imperfect de-identification techniques to protect privacy.[56] Some roundtable participants also expressed concern about the seemingly unconstrained expansion in the use of government-held health information, exemplified by data collection and use under the Practice Incentives Program. Stakeholders observed that incremental encroachment of governments and researchers on the privacy of individuals was flying under the radar due to its dispersed and incremental nature.

The activities of PHNs, researchers (outside government), state and territory agencies and others fall outside the operation of the Rules (though may be regulated by the Privacy Act or state or territory privacy law). To enhance the protection of claims information when it is disclosed to a recipient that is not covered by the Rules, we suggest that disclosure of claims information be subject to formal data sharing agreements that place conditions on the recipient – this is discussed further below.

3.2.4 Interaction with the Data Transparency and Availability Bill

Several stakeholders asked for more clarity on how the Rules would interact with the data sharing scheme to be introduced by the DATB.[57] Some wanted the Rules to align with the DATB[58] while others were concerned that the DATB would remove protections for claims information contained in the Rules.[59]

3.3 Review findings

MBS and PBS data is highly sensitive and deserves strong protections. It is sensitive because it reveals health information about individuals and because it covers most of Australia's population. Public confidence in the health system relies on strong privacy protections and strict limits on secondary use. The National Health Act requires the Rules to regulate storage, use and disclosure of claims information. It also requires the Rules to prohibit agencies from storing MBS and PBS information in the same database, from linking such information other than as prescribed in the Rules and from storing old information with identifiers. The OAIC cannot revise the Rules in a way that would derogate from those requirements in the primary legislation.

That said, new legislation such as the DATB and agreements such as the National Health Reform Agreement will necessarily impact the operation of the Rules and the handling of claims information. Such developments are out of the hands of the Information Commissioner but must be taken into account in reviewing and revising the Rules.

[56] See APF pp 5-7.

[57] See APF p 10, Calabash Solutions p 9, Law Society of NSW p 3, NPS Medicinewise p 2.

[58] See Monash University p 6.

[59] See APF p 10, Calabash p 9, NSWCCL p 5.

In recognition of the sensitivity of claims information and new risks arising in the digital age, IIS recommends some new protections, including that the Rules: prohibit open release of unit-level claims information, regardless of whether it is de-identified or not (see recommendation 6); prohibit use or disclosure for individuated intervention (see recommendation 4); and require data sharing agreements for disclosures of claims information to ensure data recipients are bound by certain conditions (see recommendation 5). IIS also recommends some revisions to the Rules to take account of the impact of the DATB – if it is passed.

3.3.1 Interaction with the Data Transparency and Availability Bill

If passed, the DATB and related subordinate rules and frameworks will override the Rules and enable government agencies to share claims information as long as the agency and recipient of the information meet the requirements set down in the Bill. This is enabled by cl 23 in the DATB which creates an authorisation to share information that overrides other prohibitions on collection, use and disclosure contained in Commonwealth, state or territory laws.[60]

This means that Services Australia would be able to disclose claims information under the data sharing scheme established by the DATB without breaching restrictions on disclosure in the Rules.[61] It could, for example, disclose claims information for other forms of research in the public interest, beyond medical research.

It also means that another agency will be able to collect and use claims information under the scheme without breaching restrictions on use and linkage in the Rules – as long as the agency follows the requirements in the Bill and only uses the data for the purpose for which the data was shared.[62] For example, it would be open to the Department of Health to establish a data sharing arrangement with Services Australia to enable the Department to collect claims information for the purpose of 'informing government policy and programs' (one of three permitted purposes in the Bill).[63] In doing so, the Department of Health would be able to circumvent restrictions on use and linkage of claims information contained in clause 13 of the Rules.

While the DATB may override restrictions in the Rules relating to linkage, use and disclosure, it seems reasonable to expect that other provisions in the Rules would continue to apply such as those relating to management of claims information, technical standards, retention and reporting of linked claims information and linking old information with PICs.[64]

[60] Data Availability and Transparency Bill 2020, first reading, cl 23.

[61] Data Availability and Transparency Bill 2020, first reading, see cl 23(1) and 13(1).

[62] Data Availability and Transparency Bill 2020, first reading, see cl 23(2) and 13(3).

[63] Data Availability and Transparency Bill 2020, first reading, see cl 15(1).

[64] See National Health (Privacy) Rules 2018, cl 8, 9, 10, 11 and 15.

The DATB has been introduced into, but not passed by, parliament. This creates some uncertainty for the purposes of this review. If the Bill is passed, it would formally permit use of claims information for service delivery, government policy and programs and research and development – thereby moving such matters out of the hands of the Information Commissioner and this review. Recommendation 3 suggests revisions to the Rules if the DATB is passed. The revisions aim to clarify the interaction of the Rules with the DATB and build in some additional protections for claims information shared under the Bill.

If the Bill is not passed, or is passed in a different form, the review is left to clarify a position on secondary use of claims information.

3.3.2 Use and linkage for public policy purposes

Use of claims information for policy and research is already provided for under the Rules but due to their complexity and uneven application, there is both uncertainty about what activities are allowed and gaps in protection. IIS finds that the use of de-identified claims information for policy and research should continue to be allowed by the Rules, as long as such activity is accompanied by strong protections. This would align with the Senate Committee recommendation that the Rules be revised to 'improve access to de-identified MBS and PBS data for the purpose of health policy evaluation and development as well as research undertaken in the public interest, in ways that don't decrease privacy.'[65]

The most effective way to address risks associated with secondary use of claims information is to ensure the Rules prescribe and limit permitted uses and disclosures, address gaps in how the Rules apply to agencies and establish clear safeguards – the recommendations in this report seek to do this.

3.3.3 Use and disclosure for individuated interventions

While secondary use for policy and research should be allowed, secondary use for individuated intervention should be very limited. By 'individuated intervention' we mean an intervention by an agency that targets a specific identified individual.[66] This contrasts with data use for policy which presupposes that the use is for general purposes. That is, the data provides an evidence base to inform the development of public policy and, while it may involve seeking to better understand a particular cohort of individuals or subpopulation, it does not involve a direct impact on any one individual.

[65] Senate Select Committee on Health, *Sixth Interim Report, Big health data: Australia's big potential*, 2016, recommendation 5.

[66] There has been much commentary on privacy risks associated with individuation. See for example, Anna Johnston, *Individuation: Re-imagining data privacy laws to protect against digital harms*, July 2020. In this report, we are concerned with the issue of using data to identify a person based on certain features or attributes in order to treat the person differently. Our analysis does not consider wider risks associated with being able to differentiate a person from others while still not knowing the person's identity.

This issue was raised by the Law Society of NSW which noted that data could be used to impose individuated outcomes upon individuals and that the lack of individual control over such algorithmic individuation was concerning.[67] Of particular concern to the Law Society was linkage of datasets that enabled imposition of differentiated outcomes upon individuals or small cohorts of individuals. A differentiated outcome could include 'the denial of offer of a service, a different price for a service, withdrawal of a service, a demand for payment or reimbursement, an investigation or enforcement action.'[68]

There are three layers of privacy risk in this scenario:

- *Secondary use:* the use is a secondary use and is likely to have been outside the expectations of the individual when they provided the information.
- *Individual lack of control over inferences drawn:* data linkage and analytics is used to infer information about an individual and the individual has no control over those inferences.
- *Direct impact on the individual*: based on those inferences, an agency makes decisions about, or imposes differentiated outcomes on, the individual – that is, there is a specific and direct impact on the individual.

The second two risks can also arise in relation to 'primary use'. Privacy laws elsewhere have begun to address this matter. For example, the GDPR now regulates automated decision-making and gives individuals rights to request human intervention and challenge a decision.[69] However, here IIS is specifically concerned with individuated intervention by secondary agencies. It would not be practicable for the Rules to restrict individuated intervention by primary agencies because this would interfere with the administration and oversight of the MBS and PBS schemes and with exceptions that allow for individuated intervention in prescribed circumstances (such as those set out in cl 9(1)).

The privacy risks associated with individuated intervention will be reduced to the extent that the Rules limit the sharing of identifiable claims information and proscribe re-identification by data recipients during their use or linkage of the information. Strict de-identification practices would stop data use for government policy from sliding into data use resulting in individuated intervention. However, the DATB would override this protection, enabling the sharing of identifiable claims information in some circumstances. Despite that, IIS understands that the DATB intends that sharing of the data not be for a purpose that would involve a direct impact on an individual.[70] To underline this intention and remove doubt, IIS recommends that the Rules formally prohibit use or disclosure of claims information for individuated intervention.

---

[67] Law Society of NSW p 3.

[68] Law Society of NSW p 3.

[69] *General Data Protection Regulation*, art 22.

[70] See Data Availability and Transparency Bill 2020, *Explanatory Memorandum*, p 22, paragraph 105; Note that the DATB also explicitly excludes sharing for enforcement related purposes, see Data Availability and Transparency Bill 2020, first reading, see cl 15(2).

In recommending this, IIS accepts that there are some exceptions. For example, individuated intervention is provided for under the data-matching provisions contained in Part VIIIA of the National Health Act. Data-matching under those provisions is formally carved out of the Rules by s 135AA(5C). Further, individuated intervention will be necessary in some cases, such as where is it to enable an agency to seek consent from an individual to use their information in research or where the agency is responding to an access or correction request under APPs 12 or 13. See recommendation 4.

3.3.4 Disclosure of claims information

The Rules permit disclosure of claims information in a number of circumstances in both identified and de-identified form. For example, the Rules permit the operation of s 130 of the *Health Insurance Act 1973* and s 135A of the National Health Act which allow the Department of Health to 'divulge' information in accordance with a public interest certificate.[71] They also allow the Department of Health to disclose claims information to a recipient in de-identified form. Under recommendations in this report, the Rules would also regulate disclosure of claims information by 'secondary agencies'

Later sections of this report consider specific disclosure provisions in the Rules and suggest revisions (see particularly section 7). However, in relation to disclosure of claims information generally, IIS suggests that some additional measures be put in place to ensure appropriate protections. In particular, an agency that discloses claims information, whether in identifiable or de-identified form, should have to have a data sharing agreement or similar in place that binds the recipient of the information to certain conditions of access. IIS understands that this is already common practice for agencies that handle claims information. For the avoidance of doubt, however, the Rules should make this a formal requirement and mandate the inclusion of certain matters in any such agreement (see recommendation 5.2). In addition, disclosure must be governed by the principle of 'data minimisation' – this is discussed in section 11.

3.3.5 Open release of de-identified claims information

Some stakeholders were concerned about the fallibility of de-identification and felt that an overreliance on de-identification to permit greater sharing or secondary use of claims information put privacy at risk, given growing re-identification risks. IIS agrees that while de-identification may help lessen privacy impacts, it does not remove all privacy risk. Here it is worth drawing a distinction between data sharing and data release. In the Office of the National Data Commissioner's Best Practice Guide, data sharing is defined as making data available to another agency, organisation or person under agreed conditions, whereas data release means making data publicly available with no or few restrictions on who may access the data and what they may do with it. De-identification may reduce privacy risks, but risks remain high when data is released.

[71] See National Health (Privacy) Rules 2018, cl 13(6)(b).

IIS is concerned about the increasing pressure on government agencies to publish public sector information in useable form (via websites such as data.gov.au) and how that pressure may be brought to bear on claims information. Successive reports and initiatives have recognised the value to be gained from publication of public sector information where it is safe to do so. However, claims information requires some different policy settings because of its sensitivity. IIS finds that public release of claims information in unit level form is a high-risk activity, even taking into account the many rigorous de-identification techniques available, and risks compound as more and more data is released into the public domain. While individuals may be comfortable with their de-identified information being used to support policy and research, IIS finds it unlikely that it would be within people's reasonable expectations that such information would be made publicly available.

Therefore, IIS is recommending a strengthening of the Rules on this point – that they explicitly prohibit release of unit-level claims information in an open access environment, regardless of whether the information is de-identified or not. This prohibition should apply regardless of whether the claims information appears on its own or is integrated into a larger dataset. In making this revision, the Information Commissioner would be introducing a higher bar than exists under the Privacy Act, which would otherwise permit disclosure of de-identified claims information. IIS finds this appropriate, given both the sensitivity of the information and the fact that individuals have limited choice about their interaction with the health system.

A prohibition on publication should not affect use of, or access to, existing data assets containing MBS and PBS data (such as MADIP) as those assets are made available in a secure, restricted environment rather than an open one.

3.4 Recommendations

Recommendation 3 – Amend the Rules to clarify application of the DATB

3.1 Clarify the provisions in the Rules that are unaffected by the DATB

If the DATB is passed, the Information Commissioner should revise the Rules to specify the provisions that are unaffected by the operation of the data sharing scheme under the DATB. In the Rules' existing form, this would include clauses 8, 9, 10, 11 and 15. The purpose of this revision would be to ensure that agencies understand that the DATB does not override the Rules in their entirety.

3.2 Revise disclosure provisions in the Rules to clarify interaction with the DATB

If the DATB is passed, the Information Commissioner should revise the medical research provisions in the Rules, and any other provisions that permit disclosure of claims information, to make clear that claims information may be disclosed in accordance with the DATB. The purpose of this change is to give certainty to participants and transparency to the public about the interaction of the Rules with the DATB.

3.3 Apply data minimisation to DATB sharing requests

If the DATB is passed, the Rules should require that, when considering data sharing requests for claims information made under the DATB, an agency covered by the Rules should make a decision that minimises the sharing of identified or identifiable claims information in recognition of its special sensitivity – in alignment with cl 16(8) of the DATB. The Explanatory Statement should make clear that the purpose of this requirement is to emphasise the data minimisation requirement in the DATB and encourage a default position of 'de-identification'.

3.4 Require data sharing agreements to prohibit re-identification

If the DATB is passed, the Rules should require an agency that is a data custodian to include terms in any data sharing agreement involving sharing of claims information that:

- prohibit a recipient of de-identified claims information from re-identifying the information or from producing output that contains identifiable information.
- require the recipient to notify the data custodian of intentional or inadvertent re-identification of information related to any individual and the steps it has taken to rectify the situation and stop re-identification occurring again
- prohibit the recipient of claims information from making unit-level claims information available in an open release environment, regardless of whether the information is de-identified or not and regardless of whether the information forms part of a larger integrated dataset.

The inclusion of additional matters in a data sharing agreement is permitted by the DATB under cl 18(2).

Recommendation 4 – Prohibit secondary use resulting in individuated interventions

4.1 Prohibit secondary use for the purpose of individuated intervention

The Information Commissioner should revise the Rules to prohibit 'secondary agencies' from using claims information to impose individuated interventions on individuals other than when the intervention is:

- to seek consent for a secondary use of claims information permitted by the Rules (for example, for medical research).
- to address a request for access or correction under APPs 12 or 13.
- authorised under Part VIIIA of the National Health Act.
- This prohibition should not apply to 'primary agencies'.

4.2 Prohibit disclosure for a purpose that would result in individuated intervention

The Rules should also prohibit secondary agencies from disclosing claims information to a recipient for a purpose that would result in the recipient imposing individuated interventions on individuals, subject to the same exceptions listed under 4.1 above.

4.3 Define the meaning of individuated intervention

The Rules should define an 'individuated intervention' to mean an intervention, action or contact by an entity that targets specific identified individuals. The Explanatory Statement can explain that this would, for example, prevent a secondary agency from using claims information to contact an individual directly to recruit them to a non-smoking program or require their attendance at such a program in return for a benefit. It would not, however, stop the agency from using de-identified claims information to better understand smokers' pathways through the health system in order to better design a non-smoking program or better target a cohort of the population identified as having high rates of smoking.

Recommendation 5 – Require use of data sharing agreements for disclosure

5.1 Require agencies to use data sharing agreements when disclosing claims information

The Information Commissioner should revise the Rules to require agencies to put in place a data sharing agreement or similar (for example, a contract, confidentiality agreement or set of terms and conditions) that must be agreed to by the intended data recipient prior to the agency disclosing claims information to the recipient. The requirement to have an agreement in place should apply to any agency disclosure of claims information, other than a disclosure:

- between primary agencies in accordance with the Rules (proposed Part 3)

- under cl 9(1)(b) or cl 9(1)(e)
- to the subject of the information or their authorised representative.

Otherwise, the requirement to have a data sharing agreement in place should apply regardless of whether:

- the disclosure involves identified or de-identified information
- the recipient is another agency or not.

5.2 Require the data sharing agreement to include certain mandatory items

The Rules should require a data sharing agreement to:

- prohibit a recipient of de-identified claims information from re-identifying the information or from producing output that contains identifiable information.
- (where the recipient is authorised to receive identifiable claims information) specify the extent to which any associated output created by the recipient may contain identifiable information with a default position that, where reasonable and practicable, outputs contain no identifiable information or as little identifiable information as possible.
- require the recipient of de-identified claims information to notify the agency of intentional or inadvertent re-identification of information related to any individual and the steps it has taken to rectify the situation and stop re-identification occurring again.
- describe the permitted purpose that the claims information may be put to by the recipient and restrict the recipient from using the information for another purpose.
- describe the public interest served by the disclosure for the specified permitted purpose.

Where the recipient is not an agency covered by the Rules, the Rules should require the data sharing agreement to also:

- prohibit the recipient from using the claims information for a purpose that would result in the recipient imposing individuated interventions on individuals other than:
- to seek consent for a lawful secondary use of claims information.
- to address a request for access or correction under APPs 12 or 13.
- prohibit the recipient of claims information from making unit-level claims information available in an open release environment, regardless of whether the information is de-identified or not and regardless of whether the information forms part of a larger integrated dataset.
- require the recipient to comply with the APPs in relation to claims information that is personal information, if the recipient is not already covered by the Privacy Act or a state or territory privacy law.
- specify the storage and security requirements that apply to the data.

- specify when the claims information must be disposed of.

5.3 Remove overlap with data sharing agreement requirements under the DATB

If the DATB is passed, the Information Commissioner should specify that an agency does not need to comply with data sharing agreement requirements in the Rules, if the agency enters into a data sharing agreement under cl 18 of the DATB. However, it must still include in the DATB agreement the specific items outlined in recommendation 3.4.

5.4 Include the data sharing agreement requirement in Part 2 of the Rules

The Information Commissioner should include this requirement to implement a data sharing agreement for disclosures of claims information in Part 2. The requirement should apply to both primary and secondary agencies.

Recommendation 6 – Prohibit release of unit level claims information as open data

The Information Commissioner should revise the Rules to prohibit the release of unit-level claims information in an open access environment, regardless of whether the information is de-identified or not, and regardless of whether the information forms part of a larger integrated dataset or not. The prohibition should include Medicare PINs. This prohibition should apply to both primary and secondary agencies. Any such prohibition should not affect data made available in a controlled environment such as MADIP.

4. Interaction with the APPs

In 2012 the *Privacy Act 1988* was significantly amended with the introduction of the Australian Privacy Principles (APPs). The APPs regulate the handling of personal information, including health information, and establish requirements for each stage of the information lifecycle from collection of personal information through to use, storage, disclosure to disposal. The APPs replaced the Information Privacy Principles (IPPs) and National Privacy Principles (NPPs), which applied to Australian government agencies and the private sector respectively.

To the extent that the Rules impose more specific obligations than the APPs, the Rules prevail.[72] In all other cases, the APPs apply as normal to personal information handling.

The Rules have not been significantly revised or updated since the introduction of the APPs. In practice, this means that the way the Rules interact with the APPs – and any gaps or overlap in this regard – has not yet been formally canvassed. In the consultation paper stakeholders were asked what additional requirements should apply to MBS and PBS information over and above the APPs and which parts of the Rules should be removed or adjusted in light of the APPs.

4.1 Stakeholder views

4.1.1 General interaction with APPs

Some felt that the APPs and other legislative frameworks already provided a high level of protection for claims data.[73] The Pharmacy Guild of Australia did not believe that additional requirements were needed above and beyond the APPs, though did believe that the Rules should unambiguously provide for the use of claims information for medical and public policy research.[74]

Others viewed the APPs as the bare minimum and, on their own, not adequate for regulating handling and use of claims information.[75] Many felt that it was appropriate for the Rules to be more prescriptive than the principles-based framework provided under the Privacy Act – see section 1. Further, it would be inappropriate if the Rules were revised in a way that undermined the strength of the APPs.[76] Liberty Victoria suggested that revisions to the Rules remove needless overlap with the APPs to avoid the vagaries of dual wording and therefore slightly different interpretations of requirements.[77] The Medical Software Industry Association (MSIA), on the other hand, thought that overlap between the Rules and the APPs was not a concern as the Rules take precedence.[78] The APF said that the review should closely

[72] See National Health (Privacy) Rules 2018, cl 15(4).
[73] See Department of Health p 4, PSRA p 2.
[74] Pharmacy Guild of Australia p 4.
[75] See Law Society of NSW p 2, NSWCCL p 5.
[76] See AIDH pp 4-5.
[77] See Liberty Victoria p 1.
[78] See MSIA p 5.

consider the consistency of the Rules with other requirements, noting that 'a consistent legislative tool set is as important as its content.'[79]

4.1.2 Interaction with APP 1

The Health Information Management Association of Australia (HIMAA) told the review that the Rules should more specifically impose the requirements of APP 1 on agencies using claims information.[80] This could include imposing clear data governance requirements in line with APP 1.2 and specifying information that agencies must include in their privacy policies in addition to the information specified under APP 1.4.

More generally, several stakeholders remarked on the importance of transparency in relation to agency use of claims information.[81] Technical standards, linkage reports and other reporting (currently required under the Rules) did not appear to be publicly available.[82] The APF was particularly concerned about the lack of transparency around decision-making on data linkage.[83] Inadequate transparency was compounded by the complexity of the Rules which made it difficult for people outside government to understand how the Rules were being interpreted or applied in practice.[84] The Australian Healthcare and Hospitals Association (AHHA) and CHF both observed the importance of communicating privacy arrangements in plain English to individuals to ensure ongoing public confidence.[85] Relatedly, HIMAA suggested that the Rules require automatic notification to individuals about collection and use of their claims information, in line with APP 5 requirements.[86]

Discussion of specific reporting requirements under cl 10 are discussed in section 8.

4.1.3 Interaction with APP 6

Those that commented on the interaction of the Rules with APP 6 generally felt that, on its own, APP 6 was insufficient for regulating use and disclosure of claims information.[87] The Law Society of NSW found that the Rules had been effective in restricting the use of claims information and that ensuring information was not disclosed for purposes other than those for which it was collected had enhanced confidence in the system.[88] In its view, wider disclosure of claims information would expose the data to risks of misuse and secondary uses beyond the purposes for which it was collected.[89]

---

[79] APF p 2.
[80] See HIMAA p 4.
[81] See AHHA p 1, AFP p 2, AIDH p 10, CHF pp 4-5, HIMAA p 4, NSWCCL p 6.
[82] See NSWCCL p 6.
[83] See APF pp 2, 4.
[84] See APF p 2.
[85] See AHHA p 1, CHF pp 4-5.
[86] See HIMAA 4.
[87] See AIDH p 8, Calabash Solutions p 8, HIMAA p 5, Law Society of NSW p 4.
[88] See Law Society of NSW p 4.
[89] See Law Society of NSW p 4.

HIMAA suggested that the Rules should contain a higher level of consent than is required under APP 6 and that they should also require agencies to record disclosures involving identified data.

4.1.4 Interaction with APP 11

Many stakeholders commented on security arrangements applying to claims information and whether, and to what extent, the Rules should add to or defer to existing arrangements – including the security requirements contained in APP 11. Those comments are taken up in section 6.

APP 11 also requires entities to dispose of personal information once it is no longer needed. The Rules contain strict disposal requirements, particularly in relation to linkage conducted by the Department of Health. Some thought that APP 11 was sufficient for regulating data disposal while others were in favour of retaining strict disposal schedules. Data disposal is discussed further in a number of sections, including section 8 and section 11.

4.2 Review findings

IIS finds that the Rules largely continue to interact appropriately with the Privacy Act, notwithstanding the introduction of the APPs. IIS makes some recommendations later in the report to better align data disposal requirements in the Rules with disposal requirements under APP 11.2 – see section 10 and section 11.

4.2.1 'Claims information' versus 'personal information'

The Rules regulate a broader form of information than personal information as defined in the Privacy Act. In the Explanatory Statement to the Rules, the Information Commissioner points out that:

> the Rules apply to a broader category of information that 'relates to' an individual, by virtue of section 135AA(1). The Australian Information Commissioner believes that information that 'relates to' an individual need not necessarily identify that individual. In this way, claims information that is stripped of its 'personal identification components', that is – names, addresses and Medicare card and Pharmaceutical entitlement numbers – would still fall within the scope of the Rules (though may not, in such circumstances, be regulated by the general provisions of the Privacy Act).[90]

This is an important distinction because it means that the Rules can 'raise the bar' by applying privacy protections to de-identified claims information also. It is also important for considering gaps between the APPs and the Rules.

[90] National Health (Privacy) Rules 2018 Explanatory Statement.

4.2.2 Formally imposing an APP 1.2-like requirement

APP 1 (along with the Privacy (Australian Government Agencies – Governance) APP Code 2017) plays crucial role in getting agencies to take proactive steps to protect information and comply with the Privacy Act. Proactive steps would include having policies, procedures and systems in place to govern the agency's information handling practices. The technical standards provision plays this role to some extent by requiring Services Australia to establish standards that specify how it will restrict data linkage and secure linked information. As we note in our analysis of this provision, by focusing on risks associated with linked information, the standards requirement fails to deal with wider privacy and security risks. IIS recommends that, in addition to other recommendations we make in relation to the technical standards provision, the Information Commissioner revises the Rules to impose an APP 1.2-like requirement on all agencies that handle claims information, not just Services Australia.

4.2.3 Formally imposing transparency requirements

Numerous stakeholders raised concerns about lack of transparency in relation to agency use and disclosure of claims information. This made it harder to find out about how their information was being handled, an issue compounded by the current complexity of the Rules. While there may have been barriers to disseminating privacy information about claims handling back in the early nineties when the Rules were first introduced, there is no reason now, in the digital age, for such information to be withheld. Moreover, agencies should be providing the information in plain English to facilitate understanding by the public. This accords with the views of the Productivity Commission which stated in its inquiry into data availability and use that '[a]ll development of data practice – whether in the private sector or public sector – must take the creation and preservation of understanding and trust as its first consideration.'[91]

IIS recommends that – in addition to their APP privacy policies – agencies publish information about their collection, use, storage and disclosure of claims information (including de-identified claims information). In section 8, IIS recommends that agency reports of linkage activities be published.

4.3 Recommendations

Recommendation 7 – Formally impose governance and security requirements that align with APPs 1 and 11

7.1 Introduce an APP 1.2-like requirement into the Rules

The Information Commissioner should revise the Rules to require agencies to take such steps as are reasonable in the circumstances to implement practices, procedures and systems that:

- will ensure that the agency complies with the Rules; and
- will enable the agency to deal with inquiries or complaints from individuals about the agency's compliance with the Rules.

[91] Productivity Commission, *Data availability and use: Inquiry report*, no. 82, 31 March 2017, p 122.

This requirement should apply to both primary and secondary agencies and appear in (proposed) Part 2 of the Rules.

7.2 Move cl 15(3) to (proposed) Part 2 of the Rules

The Information Commissioner should revise the Rules to move existing cl 15(3) to proposed Part 2 of the Rules. The objective of this change would be to expand the application of this requirement to all agencies, both primary and secondary. Moving this clause to Part 2 would allow it to be grouped with the APP 1.2 requirement (see recommendation 7.1 above) which is closely related.

7.3 Require agencies to publish information about their handling of claims information

The Information Commissioner should revise the Rules to require agencies to publish clearly expressed and up-to-date information about how they collect, use, store and disclose claims information (including de-identified claims information). This obligation should apply in addition to any obligations under APP 1.3. It should apply to both primary and secondary agencies and appear in (proposed) Part 2.

7.4 Introduce an APP 11.1-like requirement into the Rules

The Information Commissioner should revise the Rules to require an agency to take such steps as are reasonable in the circumstances to protect the claims information it holds:

- from misuse, interference and loss; and
- from unauthorised access, modification or disclosure.

This requirement should apply to both primary and secondary agencies and appear in (proposed) Part 2 of the Rules.

5. Data separation

5.1 Overview

Clause 7 requires agencies to store MBS claims information in a separate database to PBS claims information.[92] The Commissioner explains the policy intent of the Rules in the Explanatory Statement – that the Rules 'recognise the sensitivity of health information and restrict the linkage of claims information. Such linkages may reveal detailed information on the health status and history of the majority of Australians, beyond what is necessary for the administration of the respective programs.'[93]

Clauses 8(1), 8(2) and 8(3) impose some additional data separation requirements on Services Australia, namely that:

- The MBS claims database and PBS claims database be kept separate from enrolment and entitlement databases.
- The MBS claims database must not include personal identification components other than the Medicare card number.
- The PBS claims database must not include personal identification components other than the pharmaceutical entitlement number.

5.2 Stakeholder views

Stakeholders were divided on the requirement to store MBS and PBS data in separate databases. On one side, agencies and researchers favoured relaxing data separation requirements.[94] On the other, civil society groups and others favoured maintaining data separation requirements.[95] Figure 2 illustrates:

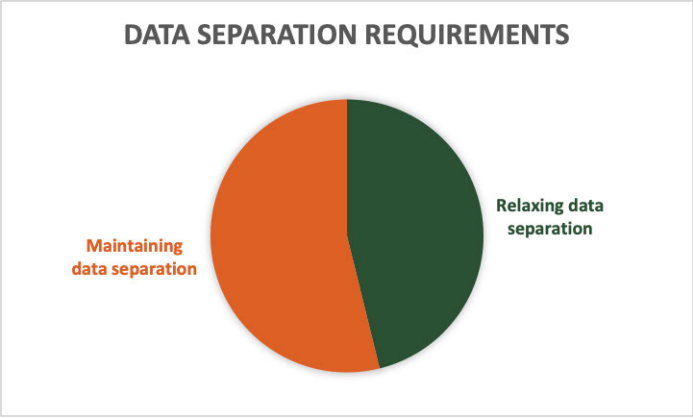


Figure 2.

[92] See National Health (Privacy) Rules 2018, cl 7.

[93] National Health (Privacy) Rules 2018 Explanatory Statement.

[94] See ABS p 4, Department of Health p 4, HIMAA p 1, Monash University p 5, NPS Medicinewise p 2 and PHRN p 2.

[95] See AIDH p 6, APF p 9, Calabash Solutions p 4, Law Society of NSW pp 3-4, NSWCCL p 5, Pharmacy Guild of Australia p 5, PSRA p 1.

The former group viewed existing data separation requirements as outmoded and overtaken by developments in technology – including developments in privacy enhancing technology.[96] According to NPS Medicinewise, privacy preserving linkage methods were available which provided lower risk solutions for record linkage than the separation requirements in the Rules.[97] Monash University commented that separate storage created significant inefficiencies for Services Australia which had to re-establish links for each set of requested data, resulting in 2 to 3 year delays for researchers from study commencement to receipt of claims information.[98] In its view, 'advancements in information security, storage and management as well as secure environments for data access should mitigate the privacy and function creep risks for which the Rules were originally established.'[99]

In addition, data separation requirements generated confusion for agencies conducting linkage activities, with the Australian Bureau of Statistics (ABS) suggesting that cl 7 be clarified in relation to agency data integration involving de-identified data.[100]

The latter group believed data separation offered important privacy protections for claims information and that the requirement to store MBS and PBS data in separate databases should remain. Calabash Solutions said that it minimised the risk of unintended or unauthorised secondary uses of claims information.[101] Regarding whether technological advance meant that data separation had been outmoded, the AIDH thought not. It noted that modern interoperability between database and information technologies could provide integrations for data-sources.[102] It also pointed out that merged databases risked becoming a single point of failure from a systems and privacy standpoint and were difficult, expensive, and time-consuming to remediate following an adverse privacy event.[103]

5.3 Review findings

5.3.1 Data separation under cl 7

Section 135AA requires the Rules to prohibit storage of MBS and PBS claims information in the same database and the Information Commissioner has no discretion to alter this requirement.[104] This means that this this review cannot recommend a change in this regard. However, there is an uneasy relationship between this provision and others in the Rules that authorise linkage in prescribed circumstances. In such cases, MBS and PBS data is stored together in linked form, even if for a limited time.

[96] See ABS p 4, HIMAA p 1, Monash University p 5, NPS Medicinewise p 2 and PHRN p 2.
[97] See NPS Medicinewise p 2.
[98] See Monash University p 5.
[99] See Monash University p 6.
[100] ABS p 4.
[101] Calabash Solutions p 4.
[102] See AIDH p 6.
[103] See AIDH p 6.
[104] See *National Health Act 1953*, s 135AA(5)(d).

In the case of government-held data assets like MADIP or NIHSIAA, MBS and PBS information is stored together indefinitely as part of a larger integrated dataset– albeit in de-identified form. On the face of it, those data assets would appear to be at odds with cl 7 of the Rules given that cl 7 applies to all agencies and all forms of claims information – both identified and de-identified. Data linkage by secondary agencies is discussed further in section 11.

In section 1, IIS observed that the technologically specific terms and concepts in s 135AA would benefit from review, including data separation requirements. In the interim, IIS suggests that the Information Commissioner explore options to modulate the language in cl 7 while remaining true to the requirements of s 135AA(5)(d). For example, could cl 7 be amended to require agencies to store MBS claims information in a separate database to PBS claims information, other than where storage in the same database is necessary for a linkage activity authorised by the Rules? This would align with s 135AA(5)(e) which allows the Rules to authorise specific linkage activities.

5.3.2 Data separation by Services Australia under cl 8

Given that the data separation requirement cannot be removed from the Rules due to s 135AA(5)(d), this requirement must also remain a feature of the provisions applying to Services Australia also. In light of this, IIS does not find there to be a strong case for removing other data separation provisions applying to Services Australia under clauses 8(2) and 8(3) which require separation of claims information from enrolments and entitlements and from PICs (other than the Medicare number and pharmaceutical entitlements number). Those arrangements continue to be appropriate, in IIS' view, given the comprehensive nature of Services Australia's data holdings and the associated privacy and security risks.

Furthermore, such arrangements should apply to the Department of Health also, which handles identified claims information in connection with its health provider compliance functions. IIS therefore recommends that clauses 8(1), 8(2) and 8(3) be extended to apply to 'primary agencies' rather than only Services Australia.

5.4 Recommendation

Recommendation 8 – Clarify data separation requirements
8.1 Explore options to modulate cl 7 to clarify relationship with linkage provisions The Information Commissioner should explore options to modulate cl 7 to clarify its relationship with linkage provisions in the Rules. For example, could cl 7 to amended to require agencies to store MBS claims information in a separate database to PBS claims information, other than where storage in the same database is necessary for a linkage activity authorised by the Rules? This may be a matter on which the OAIC could seek legal advice.

8.2 Extend cl 8(1), 8(2) and 8(3) to 'primary agencies'

The Information Commissioner should revise the application of cl 8(1), 8(2) and 8(3) to cover primary agencies (rather than only Services Australia). Before making this change, the Commissioner should consult with the Department of Health to ensure that this does not interfere with the performance of health provider compliance functions.

8.3 Remove duplication between cl 7 and cl 8(1)

The Information Commissioner should explore options for removing duplication between cl 7 and cl 8(1). IIS proposes elsewhere that cl 7 be encompassed within proposed Part 2 of the Rules which would apply to both primary and secondary agencies. Therefore, it does not appear necessary for such duplication to exist. In removing duplication, the Information Commissioner should consider including the qualification in cl 8(1) - that the data separation requirement does not prevent databases being located within the same computer system – in cl 7.

6. Primary agencies: Technical standards and PINs

6.1 Overview

The Rules require Services Australia to establish standards to ensure a range of technical matters are adequately dealt with in designing a computer system to store claims information.[105] If Services Australia changes the standards, it must inform the OAIC.[106] The standards must:

- Specify access controls
- Limit access to only those officers or contractors who reasonably require access
- Specify security procedures and controls to prevent unauthorised linkage of MBS and PBS data
- Identify how linkages conducted under the Rules can be traced
- Describe special arrangements for security of claims information that has been linked in accordance with the Rules
- Specify destruction schedules for linked data.

The Rules also allow Services Australia to use Medicare personal identification numbers (PINs) to enable identification of individuals in the MBS and PBS databases. Medicare PINs may be stored in claims databases. However, the Rules require that PINs not be derived from the individual's personal information and not reveal any personal or health information about the individual from the PIN alone.

6.2 Stakeholder views

6.2.1 Technical standards

The Consultation Paper asked whether the requirement for Services Australia to have technical standards was necessary given the other information security requirements that apply, including the Protective Security Policy Framework (PSPF) and Information Security Manual (ISM). As shown at Figure 3, of those that commented on the technical standards provision, the majority favoured either retaining the requirement or making it more detailed.[107]

[105] See National Health (Privacy) Rules 2018, cl 8(4). See also National Health (Privacy) Rules 2018 Explanatory Statement.

[106] National Health (Privacy) Rules 2018, cl 8(5).

[107] See AIDH p 7, APF p 7, CHF p 5, NSWCCL p 6, Calabash p 6, HIMAA p 7, Law Society of NSW p 4, Pharmacy Guild of Australia p 5.

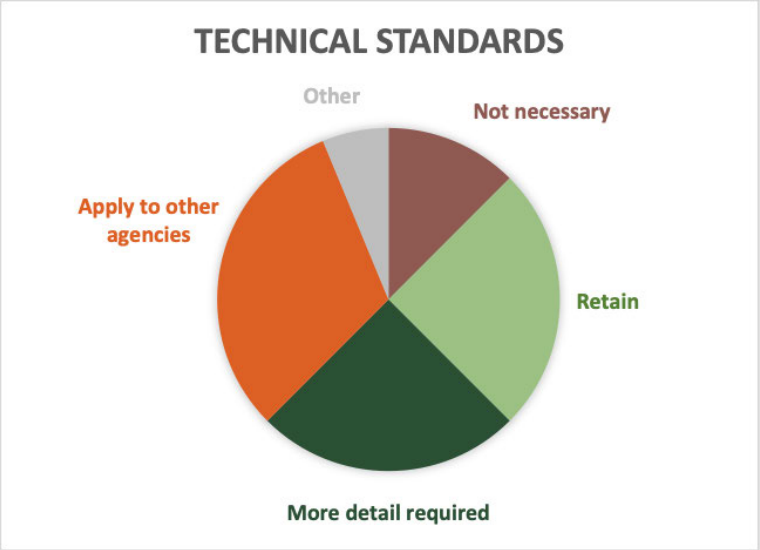


Figure 3.

NSWCCL and Calabash Solutions both pointed out that agencies had been the subject of a number of data breaches and cybersecurity incidents which highlighted the importance of retaining strong security requirements for claims information.[108] Indeed, several stakeholders commented that the technical standards requirement should apply to other agencies, not just Services Australia.[109]

The Department of Health and NPS Medicinewise both thought that technical standards were not necessary given the many other security standards that apply to agencies such as the PSPF and ISM.[110] NPS Medicinewise said that its own technical frameworks were guided by the PSPF and ISM and that those frameworks provided more detailed assurance than the Rules.[111] While APF wished to see the Rules revised to contain more detailed security requirements, it also noted that clarification was needed on the relationship between security arrangements in the Rules and other security frameworks such as the Australian Cyber Security Centre's Essential Eight Strategies to Mitigate Cyber Security Incidents, the Commonwealth Secure Cloud Strategy, the Information Security Registered Assessors Program and so on.[112]

[108] See Calabash Solutions p 6, NSWCCL p 6. NSWCCL noted that Services Australia reported 20 cybersecurity incidents to the Australian Cyber Security Centre in 2019-20.

[109] See Calabash Solutions p 6, HIMAA p 7, Law Society of NSW p 4, NSWCCL p 6, Pharmacy Guild of Australia p 5.

[110] See Department of Health p 5, NPS Medicinewise p 3.

[111] See NPS Medicinewise p 3

[112] See APF p 7.

6.2.2 Medicare PINs

Of those that commented on the provisions in the Rules applying to Medicare PINs, more favoured maintaining tight restrictions on use and disclosure of PINs[113] than favoured easing restrictions.[114] Figure 4 shows the general split of stakeholder responses.

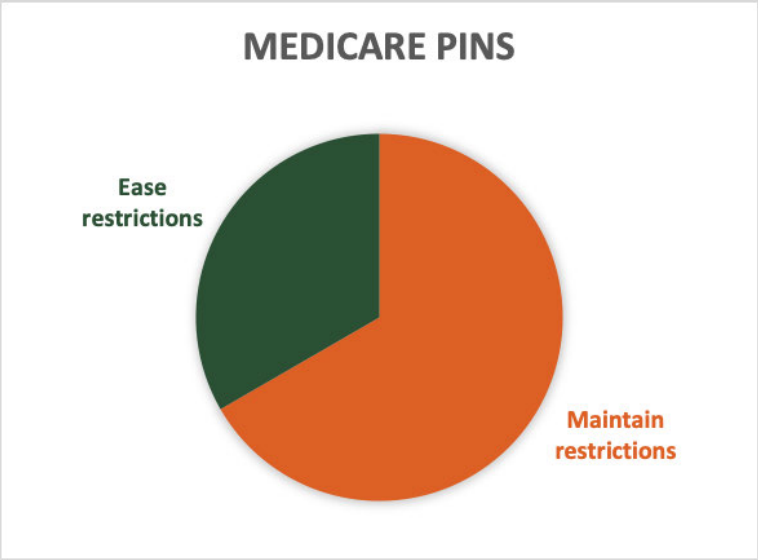


Figure 4.

Those who supported restrictions were concerned to ensure that the integrity and uniqueness of the PIN be protected and that disclosure of the PIN be tightly regulated. APF wished to see more privacy preserving linkage approaches used than the PIN while HIMAA suggested the Rules require recordkeeping of access and use of the PIN.[115]

Agencies that use the PIN in practice pointed out how crucial PINs were for streamlined data linkage and interoperability of data assets, noting that use of the PIN reduced costs and privacy risks associated with data integration.[116] It was also not clear to some why the PIN needed to be a controlled item, given its main function was to enable linkage.[117]

[113] See AIDH p 7, APF pp 7-8, Calabash Solutions p 7, HIMAA p 7.
[114] See ABS p 5, Department of Health p 5.
[115] See APF pp 7-8, HIMAA p 7.
[116] See ABS p 5, Department of Health p 5.
[117] See Department of Health p 5.

6.3 Review findings

6.3.1 Technical standards and security

The technical standards requirement under cl 8(4) plays an important role in ensuring that Services Australia has a documented approach in place that governs how it accesses, links, stores and destroys claims information. That said, the requirements in cl 8(4) for the content of standards are patchy. For example, cl 8(4) requires the standards to contain security procedures for linked claims information and to prevent unauthorised linkage but does not contain any more comprehensive security requirement for storage of claims information generally. By focusing on risks associated with linkage, the provision fails to address risks associated with situations where MBS or PBS data is used or stored separately or where it is linked with other data (and not just one with the other).

IIS agrees with stakeholders that called for more detail on security requirements including in relation to information, personnel and physical security and governance. That detail exists already in external frameworks including the PSPF, the ISM and the Essential Eight.[118] IIS recommends that the Rules formally bind all agencies covered by the Rules – not just Services Australia – to those frameworks in relation to their storage of claims information. In this way, the Rules would remain up-to-date with detailed government advice and policy on information security, as those policies are updated.

It is worth noting that most agencies are already bound by the PSPF and it looks likely that the PSPF will soon be amended to require compliance with the Essential Eight.[119] Despite this, IIS still finds that it would be worthwhile to amend the Rules to impose those frameworks in relation to storage of claims information. It would mean that failure to follow the PSPF and Essential Eight in relation to claims information may then be investigated by the Information Commissioner as an 'interference with privacy'. In this way, it offers both agencies and the Commissioner more certainty on security. In section 4, IIS also recommends formally imposing an APP 11.1-like requirement into the Rules to ensure an overarching principle of 'reasonable steps' on security – see recommendation 7.4.

Along with these recommendations, IIS is recommending the introduction of an APP 1.2-like requirement requiring agencies to have practices, procedures, systems in place to ensure the agency complies with the Rules – this would be the provision under which agencies would establish technical standards to comply with the Rules.

With those arrangements in place to uplift the security settings in the Rules along with other measures set out in the sections that immediately follow, IIS recommends repealing the technical standards requirement, along with the requirements, under clauses 10(2) and 11(4), that primary agencies make 'special arrangements' for security for linked records. Those clauses imply that strong security is not required for other storage and handling of claims information – an implication that should be reversed.

---

[118] The ACSC's Essential Eight is a series of baseline mitigation strategies taken from the *Strategies to Mitigate Cyber Security Incidents* recommended for organisations. The mitigation strategies that constitute the Essential Eight are: application control; patch applications; configure Microsoft Office macro settings; user application hardening; restrict administrative privileges; patch operating systems; multi-factor authentication; and daily backups. Implementing these strategies as a baseline makes it much harder for adversaries to compromise systems.

[119] See Justin Hendry, 'Govt to mandate Essential Eight cyber security controls,' *IT news,* 9 June 2021.

6.3.2 Assurance

Strong assurance will be critical to ensuring that agencies are applying security measures appropriately and that risks are being managed. Agencies are already required to comply with the PSPF and so should have a security plan in place at an agency-wide level. Given the heightened risks associated with the data holdings of primary agencies, IIS recommends that such agencies be required to develop a security plan specifically in relation to their handling and storage of claims information and measure their maturity of the Essential Eight. Furthermore, such agencies should report annually on their performance against the security plan by ongoing testing and monitoring control effectiveness and by independent third party auditing the design and operating effectiveness of information security controls.

6.3.3 Technical standards and access controls

Clause 8(4) also requires the technical standards to specify access controls. While access control is a matter that is covered in the PSPF and ISM, IIS finds that specific requirements relating to information access should continue to be a feature of the Rules, as they apply to primary agencies, given the heightened risks associated with their data holdings. The main change we are proposing is that, rather than require access arrangements to be contained in technical standards, the Rules should directly impose such requirements.

6.3.4 Technical standards and data linkage

As with access controls, arrangements to enable linkages conducted under the Rules to be traceable should be a direct requirement on primary agencies rather than one deferred to standards developed by respective agencies. The matters of linkage traceability and data destruction are discussed further in section 8.

6.3.5 Medicare PIN

The Medicare PIN plays an important role because it facilitates linkage of datasets and reduces privacy risks by allowing linkage to occur without use of a direct identifier such as a name, address or date of birth. While the PIN does not in itself reveal personal information about the individual to which it pertains, it acts as a key to MBS and PBS data, along with other datasets including the Australian Immunisation Register and Medicare Consumer Directory.

According to the Explanatory Statement, it is intended that any such unique number be kept, as far as possible, within Services Australia and not used as an identifier for other purposes.[120]

Clauses 8(6), 8(7) and 8(8) address the creation and use of Medicare PINs by Services Australia. IIS believes that these provisions should remain as is. A range of other provisions regulate certain aspects of use and disclosure of the PIN. These include provisions that:

[120] National Health (Privacy) Rules 2018 Explanatory Statement.

- Enable Services Australia to disclose the PIN to the Department of Health (cl 8(9)) and to disclose an algorithm that the Department may use to validate that a PIN is authentic (cl 8(11))
- Enable Services Australia to disclose both a name and a PIN to the Department of Health following a name linkage request under cl 14 (cl 8(12))
- Prohibit Services Australia from disclosing both a name and PIN to a recipient of claims information (that is not the Department of Health) unless required by law (cl 8(14))
- Prohibit primary agencies from disclosing the PIN with linked claims information (where the disclosure of the linked claims information is required by law) unless disclosure of the PIN is also required by law (cl 9(3))
- Prescribe the circumstances in which primary agencies may use PINs to link old information with PICs (cl 11(2))
- Enable the Department of Health to link claims information using the PIN as long as the use of the PIN is only an intermediate step to obtain de-identified information and the linkage is temporary and there is no practical alternative (cl 13(3) and 13(4))
- Prescribe the circumstances in which the Department of Health may ask for the name corresponding to a PIN (cl 14(1)).

IIS believes that existing restrictions applying to the use and disclosure of the PIN are appropriate, though makes some recommendations for changes to disclosure provisions generally affect the operation of the provisions above. For example, IIS recommends that provisions enabling Services Australia to disclose claims information to the Department of Health should be broadened to enable disclosure to secondary agencies generally – as long as disclosure meets permitted purpose requirements. See recommendation 10.

6.4 Recommendations

Recommendation 9 – Strengthen security requirements
9.1 Formally bind agencies to the ISM, PSPF and Essential Eight The Information Commissioner should revise the Rules to formally bind agencies to the ISM, PSPF and the Essential Eight or any successor standards in relation to their handling and storage of claims information – to the extent that they are applicable. This requirement should apply to both primary and secondary agencies and be incorporated into (proposed) Part 2 of the Rules.

9.2 Require primary agencies to develop, and report against, a security plan

The Information Commissioner should revise the Rules to require primary agencies to develop a security plan specific to their handling and storage of claims information. The security plan should align with requirements for security plans in the PSPF. Primary agencies should report annually on their performance against the security plan and measure their maturity against the Essential Eight by ongoing testing and monitoring control effectiveness and by independent, third party auditing the design and operating effectiveness of information security controls. This provision should be incorporated into (proposed) Part 3 of the Rules.

9.3 Require primary agencies to impose access controls

The Information Commissioner should revise the Rules to require agencies to implement access controls in relation to systems or databases that hold claims information. This should include requiring a primary agency to:

- Give privacy and security training in which the key requirements in the Rules are explained to a staff member before granting the staff member access.
- Implement unique user identification, authentication and authorisation practices on each occasion where system access is granted.
- Limit access to systems or data repositories that hold claims information to that required for the staff member to undertake their duties.
- Monitor and audit both standard and privileged user activities in relation to systems or data repositories that hold claims information.
- Impose technical security controls to prevent privileged users from reading emails, browsing the internet and obtaining files via online services.
- Remove or suspend staff member access:
    - On the same day that the staff member no longer legitimately requires access
    - If malicious activity is detected or
    - After one month of inactivity.

9.4 Repeal the technical standards provision

In light of the above arrangements and recommendation 7.4, the Information Commissioner should repeal cl 8(4).

7. Primary agencies: Disclosure of claims information

7.1 Overview

The Rules contain several provisions that specify how Services Australia (and, in some cases, the Department of Health but only in connection with performing health provider compliance functions) may disclose claims information. In this report, we refer to those agencies as 'primary agencies'.

The circumstances in which disclosure is permitted in the current Rules is given in the following table. Note that this table focuses on disclosure by primary agencies – mostly Services Australia – and does not include disclosure by secondary agencies which is dealt with in section 11.

Disclosure to whom	Type	Clause	Circumstances	Form
Department of Health (when performing health provider compliance functions)	**Sharing between primary agencies**	8(9)	Services Australia may disclose claims information to the Department where this is directly connected to the Department performing the health provider compliance functions.	With PICs
Authorised recipient	**Disclosure under law**	9(1)(b)(i)	Primary agencies may disclose *linked* claims information where the disclosure is required by law.	Linked With PICs (implied) Without PIN (unless expressly required by law)
Enforcement body	**Disclosure to enforcement body**	9(1)(b)(ii)	Primary agencies may disclose *linked* claims information to an enforcement body for a specific case for: enforcement of criminal law; or enforcement of law imposing pecuniary penalty; or protection of public revenue.	Linked With PICs (implied) Without PIN (unless expressly required by law
An individual	**Individual access**	9(1)(e)	Primary agencies may disclose *linked* claims information to an individual where that individual has given their consent.	Linked With PICs

Disclosure to whom	Type	Clause	Circumstances	Form
Department of Health	**Disclosure for public policy**	8(9)	Services Australia may disclose claims information to the Department of Health as long as it does not include PICs. The information may include Medicare PINs, encrypted Medicare numbers, individual current or past participation in MBS or PBS schemes or safety net arrangements.	Without PICs With PIN With encrypted Medicare no.
Agency, organisation or individual (other than Department of Health)	**Disclosure is lawful**	8(15)	Services Australia may disclose claims information to a recipient other than the Department of Health as long as the disclosure is lawful and Services Australia does not disclose both the name and the Medicare PIN (unless this is expressly required by or under law.	With PICs (implied) as long as not both name and PIN)
An individual	**Individual access**	11(2)(f)	Primary agencies may link old information with PICs for the purpose of fulfilling a request for that information from the individual concerned or from a person acting on behalf of that individual.	With PICs
Authorised recipient	**Disclosure under law**	11(2)(g)	Primary agencies may link old information with PICs for the purpose of lawfully disclosing identified information in accordance with the secrecy provisions of the relevant legislation and the Rules.	With PICs
Services Australia	**Sharing between primary agencies**	11(7)	Department of Health may disclose old information to Services Australia to enable storage under cl 11(1) or linkage with PICs as permitted under cl 11(2).	Not clear (without PICs with PIN implied)
Medical researcher	**Disclosure for research**	12(1)	Services Australia may disclose identifiable claims information to a researcher if relevant individuals have consented or the research is being conducted in conjunction with the NHMRC s 95 guidelines.	With PICs

7.2 Stakeholder views

It was clear that a number of stakeholders, particularly those representing civil society, were concerned about secondary use of claims information. Their view – set out in section 3 – was that secondary use (and by extension, disclosure enabling secondary use) should be very constrained. Agencies and researchers, on the other hand, supported the use of claims information for public policy and research and encouraged the removal of obstacles to such use – their views are also set out in section 3.

Those that commented on disclosure under the Rules and under APP 6 generally felt that, on its own, APP 6 was insufficient for regulating use and disclosure of claims information.[121] The Law Society of NSW found that the Rules had been effective in restricting the use of claims information and that ensuring information was not disclosed for purposes other than those for which it was collected had enhanced confidence in the system.[122] In its view, wider disclosure of claims information would expose the data to risks of misuse and secondary uses beyond the purposes for which it was collected.[123] HIMAA suggested that the Rules should contain a higher level of consent than is required under APP 6 and that they should also require agencies to record disclosures involving identified data.

The Department of Health, which is directly regulated by disclosure provisions in the Rules (particularly cl 8(9)), said that it was 'currently precluded from forming its own patient centred view of health (and aged care) using the data it has available or could readily acquire, which constrains effectiveness in discharging duties under primary legislation.'[124] This is partly the effect of restrictions on disclosure which mean Services Australia cannot disclose PICs with claims information to the Department (other than when the Department is performing health provider compliance functions). It is also partly the effect of restrictions on linkage applying to the Department of Health – discussed further in section 11.

The Department of Health suggested that the Rules allow Services Australia to disclose PICs to the Department. This would enable the Department to use the PICs as a variable to support linkage of claims information with other health and aged care datasets and thus allow evidence-based analyses in support of improvements in the health system and patient outcomes.[125]

[121] See AIDH p 8, Calabash Solutions p 8, HIMAA p 5, Law Society of NSW p 4.

[122] See Law Society of NSW p 4.

[123] See Law Society of NSW p 4.

[124] Department of Health p 5.

[125] See Department of Health p 5.

7.3 Review findings

7.3.1 Disclosure provisions generally

IIS supports the disclosure provisions in the Rules remaining narrowly defined. Function creep is a serious concern, particularly in a public policy climate that is increasingly geared towards reuse of public sector data. Some revisions are necessary, however, to accommodate the change to 'primary' and 'secondary' agencies (and the consequent expansion of the secondary agency category to encompass all agencies that handle claims information rather than just the Department of Health). IIS also suggests that, in certain places, the disclosure provisions make clearer the permitted purposes enabling disclosure to ensure such purposes are unambiguous and activities falling outside those purposes are formally ruled out.

One thing that became clear when reviewing disclosure provisions (outlined in the table above) was that they were scattered across several clauses. This makes it difficult for agencies regulated by the Rules to get a clear picture of the full range of allowable disclosures. It also makes it difficult for the public to interpret how the Rules restrict disclosure. IIS therefore recommends that the Rules be amended to bring disclosure provisions regulating primary agencies together in one section of the Rules – to the extent that this is feasible and enhances clarity.

A further point of difficulty is that the disclosure provisions all deal with different forms of information – linked, old, identified, with or without PICs – and this added to the overall obscurity of the Rules, making it difficult to grasp the accumulative privacy impact. Some areas of inconsistency appeared unjustified. Why, for example, do the Rules allow Services Australia to disclose identifiable old claims information where this is required by law, whereas 'new' claims information may be disclosed if 'lawful' and as long as the name and PIN are not both disclosed? Opportunities to rationalise disclosure provisions is taken up in the sections that follow.

7.3.2 Information sharing between primary agencies

The Rules enable Services Australia to disclose identifiable claims information to the Department of Health to enable the Department to perform health provider compliance functions (cl 8(9)) and allow the Department of Health to disclose old information to Services Australia to enable compliance with 'old information' requirements (cl 11(7)). Disclosure provisions should be simplified and reframed to facilitate appropriate sharing between primary agencies in accordance with (proposed) Part 3 of the Rules – see recommendation 10.2.

7.3.3 Disclosure to an individual of their own information

Primary agencies may disclose identifiable claims information (whether old information or 'new') in response to an access request from an individual for their own information. In responding to such a request, an agency may link MBS and PBS information. The Explanatory Statement to the Rules explains that: 'Linkages are enabled for the purpose of disclosure to an individual, when the individual consents, permits individuals to receive, at their request, a single report of their Medicare Benefits and Pharmaceutical Benefits programs claims histories (section 9(1)(e)).' Further, 'this provision is not intended to be a consent mechanism to link claims information for unspecified secondary uses.'[126]

If this mechanism is to enable the operation of individual access requests under APP 12 or the FOI Act, it is not clear why consent is necessary, as the access is request-driven. It is also not clear why provision for individual access must be split across two separate clauses (one for linked claims information and one for old information). Nor is it logical for the wording to vary between provisions with one making reference to consent and the other making reference to access by 'a person acting on behalf of [the] individual.' The wording of cl 9(1)(e) is potentially misleading as it does not make clear that the information to be disclosed to the individual is their own claims information. We recommend some clarification to the wording of these provisions.

7.3.4 Disclosure to an enforcement body

Clause 9(1)(b)(ii) permits a primary agency to disclose linked claims information to an enforcement body where that disclosure is reasonably necessary in a specific case or in a specific set of circumstances, for: the enforcement of the criminal law; or the enforcement of a law imposing a pecuniary penalty; or the protection of public revenue. Such disclosures must be reported annually to the Information Commissioner under cl 10(3). The review did not receive specific comments about the operation of this clause. IIS finds that this clause is appropriate and has no changes to suggest.

7.3.5 Disclosure of claims information to a secondary agency

The Rules permit Services Australia to disclose claims information to the Department of Health as long as it does not include PICs (cl 8(9)). It may include Medicare PINs or encrypted Medicare numbers. As foreshadowed in section 2, IIS is recommending that a broader category of agency – secondary agencies – be regulated by the Rules including this provision.

Reframing cl 8(9) to be about a primary agency disclosing claims information to a secondary agency, rather than Services Australia disclosing to the Department of Health, raises implications that warrant careful consideration. In particular, what new restrictions might be needed to moderate the operation of cl 8(9) if reframed in this way?

[126] National Health (Privacy) Rules 2018 Explanatory Statement.

IIS believes that cl 8(9) should add a 'purpose limitation' element to disclosure. Currently, Services Australia may disclose claims information to the Department of Health without needing to know what the Department's use of the information will be, as long as the information does not include PICs. In moving to a primary/secondary agency formulation, IIS believes cl 8(9) should prevent disclosure to a secondary agency unless it is for a permitted purpose in the public interest. Permitted purposes should include where disclosure is:

- to inform government policy and programs and
- for research or statistical analysis.

Services Australia can otherwise disclose claims information with PICs as long as the disclosure is lawful and Services Australia does not disclose both the name and the Medicare PIN (cl 8(15)). However, this provision only applies to disclosures to an agency, organisation or individual that is not the Department of Health. It is not clear to IIS what the original reasoning here was for excluding the Department of Health while allowing such disclosure to other agencies or organisations.

The Department has suggested that Services Australia be able to disclose claims information with PICs to the Department to enable other forms of linkage. IIS believes that such disclosure may be better managed under the DATB rather than the Rules as the DATB introduces a range of accompanying protections that would be difficult to reproduce in the Rules (such as accreditation, consent requirements, data minimisation, data sharing principles and so on). The Information Commissioner should be cautious to avoid any case where the Rules become an avenue for data sharing with weaker protections than the DATB.

In any case, the proposal for sharing claims information with PICs should be considered in the wider sense – whether there should be circumstances where primary agencies should be able to disclose claims information with PICs to secondary agencies for the same permitted purposes outlined above – in certain prescribed circumstances. In considering this option, the Information Commissioner should take into account the privacy risks associated with secondary use and disclosure of identifiable information and implement strict limits and protections alongside any such disclosure arrangement.

The Department of Health stated that it would be useful if, in authorising disclosure to the Department of Health (or secondary agencies) (currently under cl 8(9)), the Rules also authorised the Department to collect this information. This may not be possible as s 135AA(5) does not provide for the Rules to regulate collection of claims information. In IIS' view, such an authorisation would be better placed in primary legislation.

7.3.6 Disclosure required by law or 'lawful' disclosure

The Rules permit disclosure of claims information where such disclosures are required by law or are 'lawful'. One provision requires disclosure to be 'required by law':

- *Disclosure of linked information* – disclosure of linked claims information is permitted where the disclosure is required by law (must not include PINs unless expressly required by law; may include PICs but this is implied not explicit).

Disclosure is also permitted in certain cases when 'lawful' which appears to refer to disclosure that is not otherwise blocked by a law:

- *Disclosure of identified old information* – linkage of old information with PICs and disclosure of that information is permitted for the purpose of lawfully disclosing identified information in accordance with the secrecy provisions of the relevant legislation and the Rules.

IIS has no changes to suggest with regards to these provisions.

7.3.7 Disclosure to a medical researcher

Disclosure carried out under cl 12 is discussed in section 10.

7.4 Recommendations

Recommendation 10 – Clarify disclosure requirements for primary agencies

10.1 Group disclosure requirements (applying to primary agencies) in one place

To the extent that it is feasible and clarifying, the Information Commissioner should revise the Rules to group primary agency disclosure provisions together.

10.2 Simplify provisions enabling data sharing between primary agencies

The Information Commissioner should revise the Rules to simplify and reframe the disclosure provisions enabling sharing of claims information between primary agencies. A primary agency should be permitted to disclose claims information to another primary agency to enable that other primary agency to:

- comply with a requirement under, or conduct an activity authorised by, (proposed) Part 3 of the Rules or
- enable the performance of health provider compliance functions.

10.3 Clarify and rationalise individual access provisions

The Information Commissioner should revise the Rules to replace the individual access provisions under 9(1)(e) and 11(2)(f) with a single provision, if this is feasible and logical. The new provision should remove the concept of 'consent' from individual access, in recognition that access in these cases is request-driven. The new provision should also make clear that the access is in relation to the individual's own claims information.

10.4 Broaden the application of cl 8(9)

The Information Commissioner should broaden the operation of cl 8(9) to enable a primary agency to disclose claims information without PICs (but with the Medicare PIN) to a secondary agency for the purpose of informing government policy and programs or for research or statistical analysis. The clauses that follow (8(10), 8(11), 8(12), 8(13) and 8(14)) should also be updated to use primary/secondary agency formulation.

10.5 Consider whether Rules should permit disclosure with PICs to secondary agencies

The Information Commissioner should consider whether there should be circumstances in which primary agencies should be able to disclose claims information with PICs to secondary agencies for the same permitted purposes outlined in recommendation 10.4 – in certain prescribed circumstances. In considering this option, the Information Commissioner should take into account the privacy risks associated with secondary use and disclosure of identifiable information and the desirability of strictly limiting disclosure of identifiable information. The Commissioner should also take into account the possible operation of the DATB which would enable such disclosure in controlled circumstances. In that eventuality, the Rules should not offer a weaker avenue for data sharing. An option may be to introduce a 'required or authorised by or under law' exception for disclosure to secondary agencies (rather than extending cl 8(15) to secondary agencies). The aim should be to restrict disclosure to a reasonable extent without preventing legitimate activities of secondary agencies.

Any change to disclosure arrangements may require a subsequent adjustment to cl 8(15).

10.6 Clarify disclosure provisions where agency is both a primary and secondary agency

The Information Commissioner should include a clause clarifying how disclosure provisions apply to an agency that is a primary agency in relation to some of its activities and a secondary agency in relation to others (as in the case of the Department of Health). The aim of any such provision should be to ensure that any such agency follows an internal disclosure-like process when deciding to make information held for primary agency activities available for secondary agency activities.

8. Primary agencies: Linkage, retention and reporting

8.1 Overview

The Rules allow Services Australia or the Department of Health (where the Department is performing health provider compliance functions) (what we are referring to as 'primary agencies') to link claims information held in the MBS and PBS databases but only in prescribed circumstances. These include where the linkage is:[127]

- for internal use that is authorised or required by law and is reasonably necessary for the enforcement of the criminal law; a law imposing a pecuniary penalty; or for the protection of public revenue
- for disclosure required by law to an enforcement body where the disclosure is reasonably necessary for certain prescribed enforcement activities
- necessary to determine an individual's eligibility for benefits
- necessary to prevent or lessen a serious and imminent threat to the life or health of any individual
- to enable disclosure to an individual when that individual has given their consent.

The Rules state that linked claims information that is disclosed to an enforcement body must not include the Medicare PIN (unless this is required by law). Historically, the Rules have stopped Services Australia or the Department of Health from establishing a data-matching program between MBS and PBS data. However, this provision has been affected by recent amendments to the National Health Act which allow data-matching involving certain information that is held or has been obtained by the Chief Executive Medicare for compliance-related permitted purposes.

In addition, the Rules require Services Australia and the Department of Health to destroy linked claims information as soon as practicable after meeting the purpose for which it was linked. They must also report to the OAIC certain information about their linkage activities including the number of records linked, the purposes of the linkage, number of linked records that were destroyed and so on.

[127] See National Health (Privacy) Rules 2018, cl 9(1).

8.2 Stakeholder views

Of those that commented on data linkage under the Rules, more were in favour of reducing restrictions on linkage[128] than on maintaining restrictions.[129] That said, a number of stakeholders commented more broadly on the need to restrict secondary use – see section 3. Those in favour of reducing restrictions viewed the existing approach in the Rules as out of touch with present-day linkage activities. According to NPS Medicinewise, the Rules incorrectly focused on linkage between MBS and PBS data or disclosure of identifiable claims information for medical research rather than linkage of de-identified claims data with other external datasets.[130] Others thought that linkage should be permitted in a wider range of circumstances.[131]

Those in favour of maintaining restrictions on linkage drew attention to the privacy risks associated with linkage, particularly associated with secondary use and function creep.[132]

Regarding retention of linked claims information, those that commented mostly favoured retaining existing restrictions on retention.[133] In relation to reporting linkage activities, AHHA, AIDH and Calabash Solutions all suggested that such reports be published.

8.3 Review findings

8.3.1 Linkage by primary agencies

It is important to note that this section concerns linkage activities by Services Australia and the Department of Health (when performing health provider compliance functions) – that is, primary agencies. Linkage by secondary agencies is discussed in section 11.

Data linkage is a privacy risk point because, in bringing datasets together, it generates a richer picture of an individual. It may also enable inferences to be drawn about the individual. Risks are heightened in this context by the sensitivity of the information and the fact that data linkage is a secondary use that may be outside the expectations of the individual. Section 135AA addresses this risk by requiring the Rules to prohibit linkage of MBS and PBS data unless the linkage is authorised in a way specified in the Rules.[134] IIS believes that the intention of this framing is to emphasise ‘no linkage’ as the default.

[128] See AHHA p 2, Department of Health p 6, HIMAA p 8, Monash University p 5, NSP Medicinewise p 2, PHRN p 2.

[129] APF p 8, Calabash p 9, Law Society of NSW p 4.

[130] See NPS Medicinewise p 2.

[131] See AHHA p 2, HIMAA p 8, Monash University p 5, PHRN, p 2.

[132] APF p 8, Calabash Solutions p 9, Law Society of NSW p 4.

[133] See AIDH p 10, Calabash Solutions p 10, Law Society of NSW p 4, NSWCCL p 6.

[134] See *National Health Act 1953*, s 135AA(5)(e).

There is no doubt that data practices have changed since the nineties when s 135AA was introduced. Certainly, linkage activities are widespread in government and elsewhere and, as NPS Medicinewise indicated, increasingly involve linkage of claims information with other datasets. What has not changed is the sensitivity of the information in question. For that reason, IIS advises a conservative approach when considering expansion of data linkage involving claims information.

In IIS' view, data linkage arrangements set out in cl 9 are appropriately narrow. However, it may be that wider linkage activities should be possible for secondary agencies in limited circumstances and where the resulting linked dataset is de-identified. This is discussed further in section 11.

8.3.2 Retention of linked claims information

Given the formulation of s 135AA(5)(e) discussed above and the corresponding requirement that MBS and PBS data be stored in separate databases (s 135AA(5)(d)), it is unlikely that current disposal requirements under cl 10 can be relaxed in a material way. Extended or indefinite storage is likely to contradict the requirements for the Rules contained in the National Health Act.

8.3.3 Reporting of linkages

IIS agrees that linkage reports should be published. Secondary use of claims information should be clear to the public. IIS also recommends that primary agencies put measures in place that ensure that linkages conducted under (current) cl 9 or 11 can be traced. This aligns with an obligation in (current) cl 8(4). In section 6 of the report, IIS recommends repealing the tech standards requirement under cl 8(4) and imposing some different stronger security requirements. However, linkage traceability is worth retaining to ensure that agencies have adequate governance capabilities.

8.4 Recommendations

Recommendation 11 – Require publication of reports and linkage traceability
11.1 Require primary agencies to publish linkage reports The Information Commissioner should revise the Rules to require primary agencies to publish linkage reports at prescribed intervals rather than submit them to the OAIC. The intention of this requirement is to enhance transparency of use and linkage of claims information. **11.2 Ensure linkage under cl 9 and 11 is traceable** The Information Commissioner should revise the Rules to require primary agencies to put measures in place that ensure that linkages conducted under cl 9 or 11 can be traced.

9. Primary agencies: Handling of old information

9.1 Overview

'Old information' (meaning claims information that is five or more years old) is treated differently under the Rules. MBS and PBS claims information that classifies as 'old' must be stored in separate databases with personal identification components removed. Old information may only be linked with personal identification components in certain circumstances prescribed in the Rules. Some of these requirements are dictated by the s 135AA(5)(f). Therefore, the Information Commissioner cannot revise the Rules in a way that would derogate from those requirements contained in the primary legislation. However, the Information Commissioner can vary the circumstances in which old information may be re-linked.

9.2 Stakeholder views

The consultation paper asked whether the provisions applying to old information were appropriate. Figure 5 illustrates stakeholder feedback.

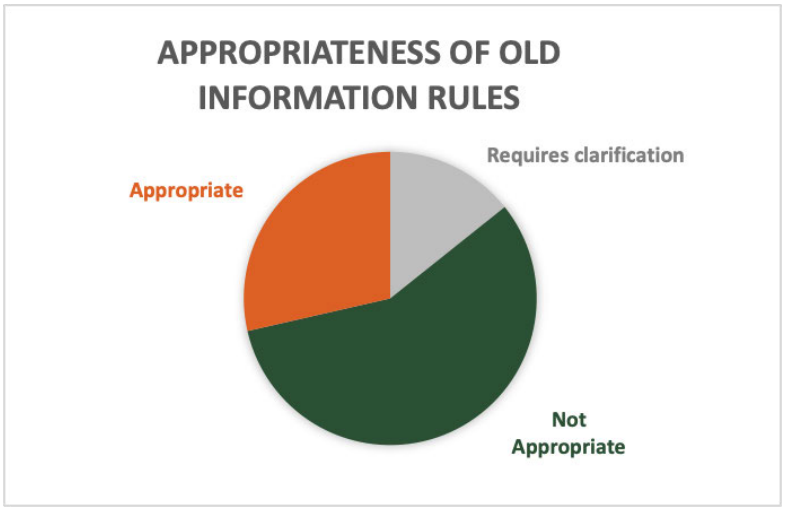


Figure 5.

Researchers responded that the provisions were not appropriate and interfered with research.[135] According to Monash University, the requirements around old information were 'arbitrary and burdensome' for longitudinal research. Both Monash and the Population Health Research Network (PHRN) highlighted how the different treatment of old information made the application process for access to claims information needlessly complicated.[136] It meant, for example, that researchers had to submit multiple access requests for a study that covered five years or more. Monash and the Department of Health noted the importance of longitudinal studies in understanding causation and examining change over time.[137] This is particularly so when studies investigate associations between medication or

[135] See Monash University pp 5-6, PHRN p 3.

[136] See Monash University pp 5-6, PHRN p 3.

[137] See Department of Health pp 6-7, Monash University pp 5-6.

treatment exposures and long-term health outcomes.[138] Stakeholders that criticised the old information provisions supported either removing the distinction between old and new claims information, or else allowing a longer period before information was categorised as 'old'.[139]

A few stakeholders believed that current restrictions applying to old information were appropriate but thought that the circumstances in which old information could be re-linked with PICs should be described in more detail or clarified.[140] HIMAA, for example, pointed out that the meaning of 'investigation and prosecution' (under cl 11(2)(b)) was unclear, while the Department of Health noted that linkage with PICs was sometimes necessary to resolve data quality issues.[141] Calabash Solutions suggested that reporting requirements (under cl 11(5)) be changed to require agencies to publish reports rather than submit them to the OAIC – IIS agrees (see recommendation 11.1).

9.3 Review findings

As noted above, s 135AA dictates many of the requirements that must apply to old information and the Information Commissioner cannot revise the Rules in a way that would derogate from those requirements. It is s 135AA that sets the definition of old information to mean claims information that is five years or older. It is also s 135AA that states that the Rules must:[142]

- require the information to be stored separately from PICs;
- provide for the longer-term storage and retrieval of the information; and
- specify the circumstances in which PICs may be re-linked with the information.

For these reasons, IIS is unable to recommend changes to how 'old information' is defined. Nor can IIS recommend changes that would vary the requirement that MBS and PBS claims information that is old information be stored in separate databases in a form that does not include PICs.

With regard to the issues raised by stakeholders, it is not clear to IIS why the different treatment of old information must result in such inefficiencies for researchers. Some of the inefficiency may be able to be resolved administratively by primary agencies. For example, researchers should not have to submit separate access requests for claims information that crosses the five-year threshold – nothing in the Rules requires this and the medical research provisions under cl 12 apply regardless of whether the claims information is 'old' or not. In terms of obstacles to linkage created by the requirement that old information be stored without PICs, IIS assumes that linkage can be undertaken using the PIN instead.

[138] See Monash University pp 5-6.

[139] See AHHA p 2, Department of Health p 6, Monash University p 6, PHRN p 3.

[140] See Calabash Solutions p 11, HIMAA p 8.

[141] See Department of Health p 7, HIMAA p 8.

[142] See *National Health Act 1953*, s 135AA(5)(f).

That said, there are some aspects of cl 11 (which contains the 'old information' provisions) that would benefit from clarification. IIS agrees with HIMAA that cl 11(2)(b) should be revised to make clear what activities are covered by 'investigation and prosecution' as such a provision may be interpreted narrowly or broadly. IIS further notes that 11(1)(a) also has the potential to be interpreted in different ways. It requires Services Australia to store old information from the MBS and PBS schemes 'in separate databases.' IIS assumes that means to give ongoing affect to s 135AA(5)(d) in the National Health Act. However, it is not clear whether this clause also means to require that old information be stored separately from claims information that is not old.

9.4 Recommendations

Observation – Review of old information requirements
Section 135AA would benefit from a review to ascertain whether requirements for old information remain fit for purpose. IIS' view is that existing provisions establish important protections for claims information as it ages and enables agencies to better manage risks associated with long-term storage. However, it would be helpful if a review considered how obstacles to use of claims information for longitudinal research could be removed while maintaining privacy protections.

Observation – Explore streamlining agency access request process
Noting the issues raised by researchers about difficulties encountered when requesting claims information that crosses the five-year threshold, we suggest that agencies explore administrative options to streamline the process.

Recommendation 12 – Clarify certain aspects of the old information provisions

12.1 Reframe cl 11 to apply to primary agencies

The Information Commissioner should reframe cl 11 to apply to primary agencies. This clause should be incorporated into (proposed) Part 3.

12.2 Clarify the scope of cl 11(1)(b)

The Information Commissioner should clarify the scope of cl 11(1)(b) either within the Rules themselves or in the Explanatory Statement. The objective of such a clarification should be to make clear what activity falls within the scope of 'investigation or prosecution'.

12.3 Clarify whether old information must be stored separately from new

The Information Commissioner should clarify the wording of cl 11(1)(a) to make clear whether, in storing MBS and PBS data that is old information in separate databases, such information must also be stored separately from 'new' claims information.

10. Primary agencies: Disclosure for medical research

10.1 Overview

The Rules permit Services Australia to disclose claims information to researchers for the purpose of medical research in certain circumstances. Claims information that identifies an individual may only be disclosed with that individual's consent or in compliance with the guidelines issued by the National Health and Medical Research Council (NHMRC) under section 95 of the Privacy Act (Guidelines).

These arrangements reflect obligations that would apply under the Privacy Act and related laws regardless. The Explanatory Statement to the Rules explains that the reason for including these provisions is to clarify and provide certainty regarding how claims information may be used for medical research purposes.[143]

10.2 Stakeholder views

Department of Health confirmed that it considers that cl 12 applies to both it and Services Australia given the functional consultation and decision-making relationship in place to facilitate compliance with the rule.[144]

Monash University reported having its medical research processes being particularly frustrated by navigating the consent requirements of cl 12(1), including adverse impacts on the timeliness of the research as a result.[145] Other research stakeholder submissions, too, reported inconsistency of Services Australia requirements in relation to informed consent where presumably an application already satisfies cl 12(1)(b).[146]

Round table consultation raised that much could be construed as medical research if, for example, the research relates to the health of the community. Representatives of civil society argued for the interpretation of medical research to remain as narrow as possible to curtail research uses of identifying MBS and PBS in manners contrary to privacy expectations of the community.[147] Conversely, the agency and research stakeholders generally considered that research in relation to social and economic determinants of health, health system effectiveness, public policy development and health expenditure analysis could be included in scope of medical research for the purposes of cl 12.[148] These stakeholders expressed desirability of a mechanism for disclosure of identifying MBS and PBS data for avenues of research with medical relevance – by way of a public interest test, or similar.[149]

---

[143] See National Health (Privacy) Rules 2018, Explanatory Statement.

[144] Follow-up consultation with Department of Health to clarify how cl 12 is administered in practice.

[145] See Monash University p 4.

[146] See ACTA pp 1-2, Willers pp 1-2, PHRN p 3.

[147] See AIDH p 11, NSWCCL p 4, Law Society NSW p 5.

[148] See PHRN p 4, Department of Health p 7, HIMAA p 9.

[149] See Department of Health p 7, Monash University p 5.

Common across stakeholder submissions was the desirability of continuing to afford protections to identifying MBS and PBS data by way of clear data retention requirements, however some research stakeholders noted inconsistency of the cl 12(2) requirements with research standards.[150]

10.3 Review findings

10.3.1 Agencies to which the rules applies

Clause 12 prevents disclosure of identifying MBS and PBS data for medical research purposes unless the specified conditions are met. This rule as drafted appears to apply to the primary agency that holds identifying MBS and PBS data – that is, Services Australia. The Department of Health also holds some of this information (in respect of its provider compliance monitoring functions). In practice, both Services Australia and the Department of Health receive medical research applications for access to identifying MBS and PBS data, however the point of disclosure of that data is Services Australia. Both Services Australia and the Department of Health are responsible at a health system level for ensuring disclosures of identifying MBS and PBS data are made in accordance with the Rules and other statutory requirements where applicable.

When assessing medical research applications for access to identifying MBS and PBS data, cl 12 is applied in practice whereby – when the nature and complexity of the research application necessitates the involvement of the Department of Health – the Department of Health supports Services Australia in decision-making. Where the Department of Health is satisfied that the conditions of the rule, and (if applicable) any other statutory requirements outside the rule, are met, the Department of Health verifies that Services Australia may disclose the data. The support rendered by the Department of Health assists Services Australia in ensuring disclosure is appropriate in the circumstance.

As the rule itself does not obviously acknowledge the role of the Department of Health, cl 12 should be updated to reflect that Services Australia and the Department of Health are the primary agencies required to comply with this rule.

Additionally important is that cl 12, if taken to apply to both Services Australia and the Department of Health, should not prevent consultation between those primary agencies in the practical manner that such consultation already occurs. Likewise, either or both of the primary agencies may need to consult with other agencies bound by the Rules as to the appropriateness of disclosing identifying MBS and PBS data for medical research.

In addition to clarifying the primary agencies to which this rule applies, cl 12 should be updated to include that it is open to the primary agencies to consult with other agencies in relation to decisions about disclosure.

[150] See ACTA p 2, Willers p 3.

10.3.2 Alignment with Privacy Act research provisions

The medical research provisions in the Rules (enabling primary agencies to disclose identifiable claims information for medical research) broadly align with similar provisions in the Privacy Act (enabling private sector organisations to do the same, in certain circumstances). Under the Privacy Act, as under cl 12(1)(a) of the Rules, health information may be disclosed with consent. Additionally, as under cl 12(1)(b), the Privacy Act allows health information to be disclosed without consent as long as the research is conducted in accordance with the s 95A guidelines.[151] However, while the Privacy Act allows for a broader category of research than the Rules, it also includes additional protections that are not provided for under the Rules. These include that:

- it must be impracticable for the organisation to obtain the individual's consent for the disclosure and
- in disclosing the information for medical research—the organisation reasonably believes that the recipient of the information will not disclose the information, or personal information derived from that information.

IIS believes there is value in exploring the desirability of the Rules aligning with, and incorporating similar protections from, the Privacy Act in this regard. Any alignment, however, should not interfere with data sharing assessed as reasonable and necessary by the relevant Human Research and Ethics Committee (HREC) (for example, where such data sharing is necessary for peer review). See recommendation 13.2.

10.3.3 Inefficiencies related to consent

Clause 12 offers an 'either this or that' approach (as opposed to a 'this and that' approach) in respect of disclosure of identifying MBS and PBS data by the primary agencies for the purposes of medical research. Disclosure can occur on the basis of informed consent obtained by the researcher in a manner that satisfies Services Australia (cl 12(1)(a)) or on the basis that the research will be conducted in compliance with NHMRC Guidelines issued under s 95 of the Privacy Act (cl 12(1)(b)). Clause 12 is clear that the disclosure must satisfy the requirements of one basis or the other. While consent may still be a feature of the latter option, consent requirements are left to the HREC to determine in accordance with requirements set out in the NHRMC Guidelines.

The either/ or approach set out in cl 12(1) acknowledges the potential for medical research applications for identifying MBS and PBS data to be made to the primary agencies by various other agencies, organisations and independent researchers and, accordingly, provides two mechanisms for assessing the appropriateness of disclosure of the data – either of which should be workable in practice.

[151] See *Privacy Act 1988,* s 16B(3).

The APPs do not permit agencies to use or disclose personal information for medical research purposes, unless the individual has consented to the use or disclosure or the use or disclosure is allowable through an exception contained in the Privacy Act. Clause 12(1)(a) requires informed consent prior to disclosure by Services Australia of identifying MBS and PBS data – full stop – which, by virtue of excluding implied consent and any other exceptions to APP 6 that may permit use or disclosure of personal information for medical research purposes, imposes a stronger protection than envisaged by APPs.

Alternatively, cl 12(1)(b) may be used as a basis for disclosure, whereby disclosure is made for medical research that is to be conducted in accordance with NHMRC Guidelines. While informed consent would still generally be required to satisfy cl 12(1)(b), and would generally be part of HREC approval processes, this option acknowledges (through reading of the NHMRC Guidelines) that there will be research situations where there is demonstrable public interest in the disclosure of the identifying MBS or PBS data however the researcher's ability to obtain informed consent is impractical, if not impossible.[152]

Clause 12 includes an assessment role whereby Services Australia must determine whether a consent is an 'informed consent' for the purposes of cl 12(1)(a). Where deciding to disclose on the basis of cl 12(1)(a), and for consistency in its decision-making, Services Australia requires that consent for access to identifying MBS and PBS data is sought by researchers using Service Australia's formal template.

Consultation with the primary agencies revealed that applications for access to identifying MBS and PBS data that have HREC approval are sometimes made to the Department of Health in the first instance, such as in respect of more complex medical research applications. Such applications would include confirmation by the researcher of having received informed consent (using a HREC-approved consent form, as part of conducting research in accordance with NHMRC Guidelines), where applicable. On the face of it, these applications should satisfy cl 12(1)(b) and the Department of Health should be able to verify that Services Australia can then disclose the data.

Indeed, where informed consent for access to identifying MBS and PBS data has been sought by a researcher (satisfying either cl 12(1)(a)) or cl 12(1)(b)), irrespective of the primary agency to which their application was initially made, researchers would reasonably expect that the consent aspect of cl 12 is satisfied. However, research stakeholders reported experiencing a duplicate consent-related requirement from Services Australia whereby Services Australia seeks to make consent that would be satisfactory for the purposes of cl 12(1)(b) conform with the template it has issued to satisfy cl 12(1)(a). The effect is that cl 12(1) becomes a 'this and that' approach, rather than an 'either this or that' approach as written.

There appears an abundance of caution on the part of Services Australia to ensure that informed consent, where relevant to a medical research application, has been properly obtained – whether through HREC processes or otherwise – prior to its disclosure of identifying MBS and PBS data. Such caution aligns with the intent of the Rules, broadly, and would likely reassure the individuals to whom the information relates. This caution does, however, have the effect of duplicating consent processes required to satisfy cl 12(1).

[152] See 2.4(i), Guidelines Under s 95 of the Privacy Act 1988 (2014)

IIS considers that this matter is not a function of the drafting of cl 12 but is more appropriately a matter requiring administrative clarification by Services Australia.

10.3.4 Whether disclosure should be allowed for other forms of research

The primary agencies receive many and varied requests for access to identifying MBS and PBS data for medical research; however there appears to be some uncertainty as to what, exactly, falls into this category of research for the purposes of cl 12. Round table consultation raised that much could be construed as medical research if, for example, the research relates to the health of the community.

Medical research is not defined in the Rules, and the Privacy Act's definition simply includes epidemiological research as within the definition of medical research. It does not, however, define medical research itself. The NHMRC's Australian Code for the Responsible Conduct of Research does not define medical research as distinct from that of other disciplines, rather, stating that research is 'original investigation undertaken to gain knowledge, understanding and insight. It is a broad concept and there is no simple, single way to define research for all disciplines.'[153]

Stakeholder submissions, as well as roundtable consultation, revealed that the applied understanding of what is medical research for the purposes of cl 12 generally excludes health system and public policy related research that would benefit from the use of identifying MBS and PBS data. Examples of research in this grey area of research with medical relevance include studies that support health provider education, seek to enhance clinical quality and safety, assess community lifestyle impacts on health outcomes, or uncover social determinants of health for elderly populations. The Department of Health considered that research in relation to socio-economic health determinants, health system effectiveness and health expenditure analysis provide strong argument for widening the scope of what is medical research for the purposes of cl 12.

Nevertheless, limiting the disclosure by primary agencies of identifying MBS and PBS data is not an accidental function of the Rules. Privacy law, generally, is intended to be a beneficial scheme for citizens – wherein the privacy rights of individuals are to be interpreted as broadly as possible, and the ability for agencies to curtail those rights is to be interpreted as narrowly as possible. The Rules offer one such beneficial scheme in respect of application of s 135AA of the National Health Act. The retaining of a circumspect view as regards what constitutes medical research (and what would therefore prompt disclosure of identifying MBS and PBS data by the primary agencies) appears consistent with the intent of the Rules.

This review considers that cl 12 was purpose built to limit disclosures of identifying MBS and PBS data for medical research, and that this rule is not the place to interrogate or potentially minimise those protections. It is noted, too, that the Rules themselves enable disclosure of de-identified MBS and PBS data, which may well be sufficient for many broader research purposes.

[153] Australian Code for the Responsible Conduct of Research

Stakeholders expressed that there should, at least, be a mechanism for disclosure of identifying MBS and PBS data for the additional avenues of research discussed above – by way of a public interest test, or similar. IIS notes that the DATB, were it to be passed, provides a mechanism that would be suitable. The Bill's data sharing scheme contains strong embedded protections – including a public interest test – and could provide an avenue of access to identifying MBS and PBS data for researchers outside the operation of the Rules.

10.3.5 Whether retention periods should be extended

Curtailing re-uses of identifying claims information by researchers – simply because it is available and, therefore, expedient to access it – is an important aspect of privacy protection. So too is ensuring that personal information, once it has outlived its utility for the purpose, is deidentified or securely destroyed. It is specified at cl 12(2) that the primary agencies must obtain a written undertaking from the researcher that the claims information will be securely destroyed at the conclusion of the research project. The intent is to address the material privacy considerations noted.[154]

Common across stakeholder submissions was the desirability of continuing to afford protections to identifying MBS and PBS data by way of clear data retention requirements.

Noted is the narrowness of the current cl 12(2) requirement, as compared with APP 11, which requires that reasonable steps are taken to destroy personal information or ensure it is de identified if the information is no longer needed for any purpose for which it may be used or disclosed under the APPs (APP 11.2). This narrow approach was noted as desirable by civil society stakeholders, as it has the effect of limiting further uses of identifying MBS and PBS data and exploitation risks to such data posed by long-term retention.

Research stakeholders raised that cl 12(2) imposes a records destruction requirement that is inconsistent with NHMRC guidance on the matter and does not sufficiently address circumstances where research projects are ongoing (e.g. longitudinal studies), intended to be leveraged from other research projects, are of a specified medical nature (e.g. gene therapy studies) or are of community, cultural or historical significance such that retention in perpetuity is advised.

In Management of Data and Information in Research: A guide supporting the Australian Code for the Responsible Conduct of Research (Guide), the NHMRC addresses the matter of records retention and states:

> 'The period for which data should be retained should be determined by prevailing standards for the specific type of research and any applicable state, territory or national legislation.
>
> In general, the minimum period for retention of research data is 5 years from the date of publication. However, for any particular case, the period for which the data should be retained should be determined by the specific type of research, subject to any applicable state, territory or national legislation. For example:

[154] See National Health (Privacy) Rules 2018, Explanatory Statement.

- for short-term research projects that are for assessment purposes only, such as research projects completed by students, retaining research data for 12 months after the completion of the project may be sufficient
- for most clinical trials, retaining research data for 15 years or more may be necessary
- for areas such as gene therapy, research data must be retained permanently (e.g. data in the form of patient records)
- if the work has community, cultural or historical value, research data should be kept permanently, preferably within a national collection.'[155]

Considering the NHMRC Guide, there is potential that researchers will be signing undertakings to destroy the identifying MBS and PBS data where, in fact, a more nuanced decision-making approach with respect to data retention is required. IIS is of the view that undertakings in relation to data destruction could align more closely with NHRMC guidance on the topic.

10.4 Recommendations

Recommendation 13 – Clarify certain aspects of the old information provisions

13.1 Clarify that cl 12 applies to primary agencies

The Information Commissioner should clarify that cl 12 applies to primary agencies; that is, Services Australia and the Department of Health.

13.2 Explore the desirability of the Rules aligning more closely with the format of s 16B(3)

The Information Commissioner should explore further whether it would be desirable for the Rules to align more closely with the format of s 16B of the Privacy Act, to ensure appropriate protection of privacy in medical research.

13.3 Provide for consultation between agencies subject to the Rules

The Information Commissioner should add to cl 12 a provision for primary agencies to consult with other agencies subject to the Rules in respect of decisions about disclosure of identifying MBS and PBS data for medical research.

The **Explanatory Statement** should clarify that cl 12 is intended to facilitate consultation between the primary agencies, and between either or both of the primary agencies and another agency subject to the Rules.

[155] Management of Data and Information in Research: A guide supporting the Australian Code for the Responsible Conduct of Research, NHMRC, s 2.3.

Observation – Services Australia to address administratively consent inefficiencies

It is desirable for Services Australia to address administratively the apparent doubling-up of consent requirements when deciding whether to disclose identifying MBS and PBS data for medical research.

This includes assessing why Services Australia is seeking to be 'satisfied' of a consent in the manner prescribed by 12(1)(a) where a researcher is clearly seeking for disclosure to occur on the basis of the alternate 12(1)(b). Such assessment may involve:

- Identifying whether there is some other statutory requirement that prevents Services Australia from disclosing the identifying MBS and PBS data on the basis of 12(1)(b); and, if so,
- Consultation with the NHMRC in relation to the format of an HREC-approved consent form that is desirable, from the perspective of Services Australia, to be included in medical research approval documentation.

In any event, Services Australia should clarify its requirements through some form of communication to the medical research community on its website or via some other method.

Recommendation 14 – Do not extend clause 12 to include other forms of research

The Information Commissioner should not revise clause 12 to include other forms of research.

Observation – Consider the definition of 'medical research' in the Privacy Act

As part of the review of the Privacy Act, the Information Commissioner may consider expanding on the definition of 'medical research' at s 6(1) to provide further clarity as to what is included in this area of research.

This would have the dual effect of enhancing the practical application of the NHMRC Guidelines issued under s 95 of the Privacy Act, as well as informing the primary agencies with responsibility under clause 12 of the Rules with respect to research applications that are not in scope of that clause.

Recommendation 15 – Revise signed undertaking requirements to account for varied data retention needs

Taking account of the varied timelines for medical research, and the potential that some research may implicate keeping the identifying MBS and PBS data for a certain predefined period of time, the Information Commissioner should revise the signed undertaking aspect of clause 12(2) to include that, prior to disclosure,

- Services Australia must agree on a disposal or de-identification date with the researcher
- The written undertaking (agreement) must be made in an approved format
- The researcher may seek an extension of the disposal or de-identification date where this is necessary for the completion of the research
- An application for extension must be made in an approved format and
- An application for extension is to be decided by Services Australia on a case-by-case basis.

11. Secondary agencies: Use and disclosure

11.1 Overview

Clauses 13 and 14 regulate the Department of Health. Under cl 13, the Rules enable the Secretary of the Department of Health to authorise use of claims information, however any authorised use that involves data linkage is very restricted and may only occur where there is no practical alternative. Clause 14 also enables the Department to collect from Services Australia the PICs corresponding to a PIN in two circumstances:

To clarify which information relates to a particular individual where doubt has arisen in the conduct of an activity involving the linkage of de-identified information.

For the purpose of disclosing personal information in a specific case or in a specific set of circumstances as expressly authorised or required by or under law.

11.2 Stakeholder views

The APF expressed low confidence in secondary use frameworks, and pointed to a lack of transparency in some data linkage projects in the health sector being compounded by relatively immature secondary agency practices in respect of secure data storage and governance.[156] HIMAA presented that expanding use of claims data to inform and support future health sector funding could enable better identification of initial and ongoing costs for care bundling and larger programs or schemes, such NDIS.[157] NSWCCL conversely commented on the inherent power imbalance when the community provides personal information in exchange for receiving government services or benefits.[158]

There was not a wealth of stakeholder comments in relation to name linkage, however the tenor of the submissions echoed those in relation to previous sections dealing with matters of use and linkage of claims data. The notion of relaxing the requirements of cl 14 was not supported by civil society representatives,[159] whereas agency and researcher stakeholders suggested that there is a reasonable additional rationale for name linkage that should be explored.[160]

ADHA observed that name linkage can cause ‘considerable data quality issues’ and indicated its current involvement in a body of work to improve consistency in practice.[161] AIAIDH expressed that name linkage provisions are insufficient due to the difficulty of ensuring adequate de-identification.[162]

[156] See APF p 8.
[157] See HIMAA pp 1-2.
[158] See NSWCCL pp 4-5.
[159] See Calabash p 14, MSIA p 7.
[160] See HIMAA p 9, PHRN p 4.
[161] See ADHA p 2.
[162] See AIDH p 13.

Contrary to the APF's concerns about data storage and governance practices broadly in the health sector,[163] PHRN expressed confidence in the 'extremely high levels of data security' employed by specialist data linkage units using identifiers such as name, address and date of birth.[164]

11.3 Review findings

In line with earlier analysis, IIS is proposing that the Rules be reframed to refer to primary and secondary agencies. We suggest that cl 13 and 14 be reframed in that vein – expanding the operation of these clauses to apply to secondary agencies, rather than only the Department of Health.

This is no small change, however it is necessary to bring the Rules up-to-date with a setting in which many other agencies now handle (and link) claims information. As mentioned in earlier sections of this report, it is not clear why the Department of Health is treated differently to other agencies that handle claims information. In IIS' view, it is preferrable that agencies that handle claims information be treated the same, unless there is a material reason for differentiation. Changing the application of cl 13 and 14 would require a significant reframing of existing requirements to allow the Rules to apply to agencies that conduct data integration regularly – such as the ABS and AIHW. To be clear, IIS is not proposing curtailing those agencies existing activities. Rather we are proposing that the Rules apply to secondary agencies broadly and add specific protections for claims information as necessary.

In revising this section, the Information Commissioner should consult with affected agencies and any other interested stakeholders.

11.3.1 Linkage including name linkage

Linkage provisions under cl 13 and 14 have significantly curtailed the data linkage activities of the Department of Health to the point that, as IIS understands it, the Department conducts almost no linkage of MBS and PBS data to support its public policy activities. This has meant that the Department has been unable to conduct data linkage to support its response to the Covid 19 pandemic, for example. Stakeholder feedback revealed that civil society groups were understandably concerned about greater data linkage or other secondary use. In addition, as described elsewhere in this report, s 135AA itself takes a restrictive approach adopting 'no linkage' as the default position, with exceptions to be specified in the Rules. This collides with modern-day data linkage activities in government. IIS suggests that the Information Commissioner explore options to reframe clauses 13 and 14 to enable sensible interaction with existing integration initiatives such as those being undertaken by accredited integrating authorities under the *Commonwealth arrangements for data integration for statistical and research purposes*.

[163] See APF p 8.

[164] See PHRN p 4.

11.3.2 Retention of de-identified claims information

Clause 13(5) allows the Department of Health to retain claims information indefinitely for policy and research purposes as long as the information is stored without PICs. IIS recommends that, in extending cl 13 to secondary agencies, this provision be repealed and APP 11.2 be left to regulate retention in these circumstances. The intention here is to align with standard practice on data disposal – generally, an open-ended retention arrangement would be considered poor practice.

11.3.3 Secondary agency disclosure of claims information

Clause 13(6) enables the Department of Health to disclose claims information where reasonably satisfied that the recipient is not in a position of identify the individual to which the information relates.

There are two exceptions to this rule that allow the Department of Health to disclose identifiable information. One exception allows the Department to disclose information to Services Australia in connection with the 'old information' provisions under cl 11 – IIS discusses this disclosure provision in section 7 (as an example of information sharing between primary agencies). We suggest this be grouped with other provisions applying to primary agency disclosure and hence removed from cl 13.

The other exception enables the Department to disclose identifiable claims information under s 130 of the *Health Insurance Act 1973* or s 135A of the National Health Act. Under those sections, the Minister or Secretary may issue a public interest certificate permitting disclosure. In expanding this provision to apply to secondary agencies, the Information Commissioner should consult affected agencies to determine whether any other legislated disclosure mechanisms should be called out in cl 13(6) along with those under the Health Insurance Act and the National Health Act.

Regarding de-identification, IIS recommends that the Explanatory Statement to the Rules offer more guidance on what 'being reasonably satisfied that the recipient is not in a position of identify the individual' means in practice. For example, the standard could point to OAIC guidance on de-identification such as the De-identification decision making framework or Five Safes.

In section 3, IIS discusses disclosure generally and recommends that agencies be required to formalise a data sharing agreement that places certain conditions on the recipient (see recommendation 5). In addition to the default position that information be disclosed in de-identified form, cl 13(6) should be revised to impose a data minimisation requirement on disclosure.

11.4 Recommendations

Recommendation 16 Explore options to apply clauses 13 and 14 to secondary agencies

16.1 Explore options for reframing clauses 13 and 14 to cover secondary agencies

The Information Commissioner should explore options to reframe clauses 13 and 14 to cover secondary agencies. Reframing those clauses in that way would require material changes to how the Rules regulate agencies. The aim of such a change would be to ensure agencies that handle claims information are appropriately regulated by the Rules, as s 135AA intends. Any resulting revised provisions should be encompassed in (proposed) Part 4 of the Rules.

16.2 Explore options to enable the Rules to better interact with existing integration initiatives

The Information Commissioner should explore options to reframe clauses 13 and 14 to enable sensible interaction with existing integration initiatives such as those being undertaken by accredited integrating authorities under the Commonwealth arrangements for data integration for statistical and research purposes.

16.3 Consult with affected agencies on reframing clauses 13 and 14

Given that the change proposed under 16.1 above would involve material changes to the application of the Rules to secondary agencies, the Information Commissioner should consult with affected agencies and interested stakeholders on any such change.

16.4 Repeal the indefinite retention provision under cl 13(5)

The Information Commissioner should revise the Rules to repeal the indefinite retention provision under cl 13(5). Retention should be regulated by APP 11.2.

16.5 Clarify de-identification standards in the Explanatory Statement

The Information Commissioner should revise the Explanatory Statement to the Rules to offer more guidance on what 'being reasonably satisfied that the recipient is not in a position of identify the individual' means in practice. For example, the standard could point to OAIC guidance on de-identification such as the De-identification decision making framework or disclosure control frameworks like the Five Safes.

16.6 Apply the data minimisation principle to disclosure under cl 13(6)

The Information Commissioner should revise cl 13(6) to require that agencies only disclose that information that is reasonably necessary to meet the purpose of the disclosure.

12. Glossary

Names marked with * are organisations that made submissions to the review. For a full list of stakeholders that responded to the consultation paper, see Appendix B.

Term or acronym	Meaning
ABS*	Australian Bureau of Statistics
ACTA*	Australian Clinical Trials Alliance
ADHA*	Australian Digital Health Agency
Agency	Australian government agency; has the same meaning as under the Privacy Act.
AHHA*	Australian Healthcare and Hospitals Association
AIDH*	Australian Institute of Digital Health
AIHW*	Australian Institute of Health and Welfare
APF*	Australian Privacy Foundation
APPs	Australian Privacy Principles (contained in the Privacy Act)
CHF*	Consumer Health Forum
Claims information	MBS and PBS data; formally, information to which the Rules applies defined in s 135AA(1) of the National Health Act.
Data release	Making data publicly available with no or few restrictions on who may access the data and what they may do with it.
Data sharing	Making data available to another agency, organisation or person under agreed conditions.
DATB	Data Availability and Transparency Bill 2020
DPMC*	Department of the Prime Minister and Cabinet

Term or acronym	Meaning
Essential Eight	The ACSC's Essential Eight is a series of baseline mitigation strategies taken from the *Strategies to Mitigate Cyber Security Incidents* recommended for organisations. The mitigation strategies that constitute the Essential Eight are: application control; patch applications; configure Microsoft Office macro settings; user application hardening; restrict administrative privileges; patch operating systems; multi-factor authentication; and daily backups. Implementing these strategies as a baseline makes it much harder for adversaries to compromise systems.
Five safes	A framework for helping make decisions about making effective use of data which is confidential or sensitive.
FOI Act	*Freedom of Information Act 1982* (Cth)
Health provider compliance functions	A statutory function, duty or power of the Chief Executive Medicare under either the *Health Insurance Act 1973* or the National Health Act or the *Dental Benefits Act 2008* or the *Human Services (Medicare) Act 1973*, where a health provider is the subject of the performance of the function or the exercise of the power or duty.
HIMAA*	Health Information Management Association of Australia
HREC	Human Research Ethics Committee
IIS	Information Integrity Solutions (report author)
ISM	Australian Government Information Security Manual
MADIP	Multi Agency Data Integration Project
MBS	Medicare Benefits Schedule
MSIA*	Medical Software Industry Association
National Health Act	*National Health Act 1953* (Cth)

Term or acronym	Meaning
NHMRC s 95 guidelines	National Health and Medical Research Council privacy guidelines issued under s 95 of the Privacy Act; the guidelines provide a framework in which medical research involving personal information obtained by Commonwealth agencies should be conducted, to ensure the information is protected.
NIHSIAA	National Integrated Health Services Information Analysis Asset (established and maintained by AIHW)
NSWCCL*	NSW Council for Civil Liberties
OAIC	Office of the Information Commissioner
OGP	Open Government Partnership
Old information	Defined in s 135AA(11); claims information that has been held by one or more agencies for at least the preceding 5 years.
PBS	Pharmaceutical Benefits Schedule
PHRN*	Population Health Research Network
PIC	Personal Identification Component, defined in the National Health Act in s 135AA(11) (in relation to claims information) to mean any of the following: (a) the name of the person to whom the information relates; (b) the person's address; (c) the person's Medicare card number; (d) the person's Pharmaceutical entitlements number.
Privacy Act	*Privacy Act 1988* (Cth)
PSPF	Protective Security Policy Framework
PSRA*	Professional Services Review Agency
the Rules	National Health (Privacy) Rules 2018

Appendix A. Questions we asked

A.1 Key issues and general questions

Key questions for this review	
1.	What provisions in the Rules work well and should remain as they are or with minimal changes?
2.	What provisions in the Rules are no longer fit for purpose? Why?
3.	Do the Rules get the balance right between protection of privacy on the one hand and use of claims information on the other? Why or why not?
Form and function of the Rules - Prescriptive versus principles-based	
4.	Which provisions in the Rules are too prescriptive / not prescriptive enough?
5.	Would any parts of the Rules benefit from being made more principles-based? Why?
Form and function of the Rules – Technological specificity versus technological neutrality	
6.	How could the Rules be updated to better accommodate current information technologies and modern data practices in a way that continues to protect privacy?
7.	Which parts of the Rules are no longer fit for purpose due to technological change or need adjustment?
Form and function of the Rules – Interaction with the APPs	
8.	What additional requirements should apply to MBS and PBS information over and above the APPs? Why?
9.	Which provisions in the Rules (if any) should be removed or adjusted in light of the APPs?
The Rules in practice – Modernisation and trends in government information policy	
10.	How can the Rules be modernised or made more effective, while remaining within the parameters of the primary legislation?
11.	How might the Rules better align with current government policies pertaining to information use, re-use and sharing while still protecting privacy?

A.2 Specific questions about the rules

Management of claims information by Services Australia	
12.	Should these requirements (about separation of claims information from enrolments and entitlements and exclusion of personal identification components) stay the same or be changed? Why?
Requirements for Services Australia to maintain technical standards	
13.	Is having dedicated detailed technical standards for MBS and PBS claims databases necessary given the range of other information security requirements applying to Services Australia?
14.	Should the technical standards cover any other matters?
15.	Should any other agencies be required to have technical standards of this sort? Which agencies and why?
Medicare PINs	
16.	Are the provisions regulating the creation, use and disclosure of Medicare PINs fit for purpose?
17.	Should there be more permissive or more restrictive use of Medicare PINs? Why?
Disclosure to the Department of Health	
18.	Do disclosure provisions get the balance right between data sharing and protection of privacy? Why or why not?
19.	Is APP 6 adequate for regulating disclosure of claims information? What additional requirements, if any, need to be spelt out in the Rules?
Linkage of claims information	
20.	Should linkage of MBS and PBS claims information be allowed in other circumstances? What circumstances and why? How could this be done in a way that continues to protect privacy?
Retention and reporting of linked claims information	
21.	Are the data retention requirements appropriate? Should linked claims information be able to be retained for longer?
22.	Are reporting arrangements appropriate? Should reporting categories be changed in any way?

Old information	
23.	Are the provisions applying to old information appropriate?
24.	In what circumstances (if any) should old information be able to be re-linked with personal identification components? How could this be done in a way that continues to protect privacy?
Disclosure of claims information for medical research	
25.	Is this provision necessary given it already applies under the Privacy Act? If yes, does it need to be modified in any way? Should claims information be able to be used for other forms of research? If yes, should there be any limitation on this use?
Use of claims information	
26.	Should the Department of Health be able to link claims information in a wider range of circumstances? What circumstances?
27.	Are provisions enabling disclosure of claims information by the Department of Health appropriate?
Name linkage	
28.	Are name linkage provisions appropriate? Should name linkage be allowed in any other circumstances?
Other matters including management of paper copies	
29.	Are provisions relating to paper copies of claims information appropriate? Why or why not?

Appendix B. Stakeholders who made submissions

Submissions received from:
Australasian Institute of Digital Health
Australian Bureau of Statistics
Australian Clinical Trials Alliance
Australian Digital Health Agency
Australian Healthcare and Hospitals Association
Australian Institute of Health and Welfare
Australian Privacy Foundation
Calabash Solutions
Commonwealth Department of Health
Consumer Health Forum
Craig Willers
Department of the Prime Minister and Cabinet
Health Information Management Association of Australia
Law Society of NSW
Liberty Victoria
Medical Software Industry Association
Monash University
NPS Medicinewise
NSW Council for Civil Liberties
Pharmacy Guild of Australia

Submissions received from:
Population Health Research Network
Professional Services Review Agency
Tasmanian Department of Health

Appendix C. Stakeholders who attended roundtable discussion

Attendees at roundtables:
Australasian Institute of Digital Health
Australian Bureau of Statistics
Australian Digital Health Agency
Australian Institute of Health and Welfare
Australian Medical Association
Australian Privacy Foundation
Commonwealth Department of Health
Digital Transformation Agency
Health Issues Centre
Liberty Victoria
NSW Council for Civil Liberties
Services Australia

INFORMATION INTEGRITY SOLUTIONS PTY LTD
PO Box 978, Strawberry Hills NSW 2012, Australia

P: +61 2 8303 2438
F: +61 2 9319 5754
E: contact@iispartners.com
www.iispartners.com

ABN 78 107 611 898
ACN 107 611 898

IIS Partners
INFORMATION INTEGRITY SOLUTIONS