



Australian Government

Office of the Australian Information Commissioner

EXPLANATORY STATEMENT

National Health (Privacy) Rules 2025

Issued by the authority of the Australian Information Commissioner under section 135AA of the *National Health Act 1953*.

Authority

Subsection 135AA(3) of the *National Health Act 1953* (the National Health Act) provides that the Australian Information Commissioner (the Information Commissioner) must, by legislative instrument, issue rules relating to information to which section 135AA applies. Information to which section 135AA does and does not apply is prescribed in subsections (1) and (2). The issuing of rules under section 135AA is a privacy function for the purposes of the *Australian Information Commissioner Act 2010* (see subsection 135AA(3A) of the National Health Act).

Subsection 135AA(5) of the National Health Act prescribes certain matters that rules issued under section 135AA must deal with and provides that, so far as practicable, the rules must:

- (a) specify the ways in which information may be stored and, in particular, specify the circumstances in which creating copies of information in paper or similar form is prohibited; and
- (b) specify the uses to which agencies may put information; and
- (c) specify the circumstances in which agencies may disclose information; and
- (d) prohibit agencies from storing in the same database:
 - (i) information that was obtained under the Medicare Benefits Program; and
 - (ii) information that was obtained under the Pharmaceutical Benefits Program; and
- (e) prohibit linkage of:
 - (i) information that is held in a database maintained for the purposes of the Medicare Benefits Program; and
 - (ii) information that is held in a database maintained for the purposes of the Pharmaceutical Benefits Program;unless the linkage is authorised in the way specified in the rules; and
- (f) specify the requirements with which agencies must comply in relation to old information, in particular requirements that:
 - (i) require the information to be stored in such a way that the personal identification components of the information are not linked with the rest of the information; and
 - (ii) provide for the longer term storage and retrieval of the information; and
 - (iii) specify the circumstances in which, and the conditions subject to which, the personal identification components of the information may later be re-linked with the rest of the information.

Subsection 135AA(4) of the National Health Act provides authority for the Information Commissioner, by legislative instrument, to issue further rules that vary the existing rules.

Subsection 135AA(6) sets out a statutory precondition to the making of the Rules. It provides that, before issuing rules, the Information Commissioner must take reasonable steps to consult with organisations (including agencies) whose interests would be affected by the rules. This precondition was satisfied prior to the making of the rules. The consultation process is described in further detail below.

Subsection 33(3) of the *Acts Interpretation Act 1901* provides that where an Act confers a power to make, grant or issue any instrument of a legislative or administrative character (including rules, regulations or by-laws), the power shall be construed as including a power exercisable in the like manner and subject to the like conditions (if any) to repeal, rescind, revoke, amend, or vary any such instrument.

Purpose and policy intent

The *National Health (Privacy) Rules 2025* (the Rules) concern the handling, by agencies, of information obtained by any agency in connection with a claim for a payment or benefit under the Medicare Benefits Program and the Pharmaceutical Benefits Program ('claims information'). Subsection 135AA(1) of the National Health Act specifies that the Rules apply to information relating to an individual that is held by an agency and was obtained by the agency or any other agency in connection with a claim for payment of a benefit under the Medicare Benefits Program or the Pharmaceutical Benefits Program; or a supply of a pharmaceutical benefit to which subsection 98AC(1) applies. The Australian Information Commissioner is required to issue such rules under subsection 135AA(3) of the National Health Act. These Rules are a legislative instrument for the purposes of the *Legislation Act 2003*. Details of the Rules are set out in **Attachment A**. The Rules replace and substantially revise the *National Health (Privacy) Rules 2021* (old rules), as explained below.

The Rules are legally binding and ensure that claims information is linked and used only for limited purposes and in particular circumstances. A breach of the Rules constitutes an interference with privacy under section 13 of the *Privacy Act 1988* (the Privacy Act) (see paragraph 13(5)(b) of the Privacy Act and subsection 135AB(1) of the National Health Act). In turn, an individual may complain to the Information Commissioner about an alleged interference with their privacy (see subsection 135AB(2) of the National Health Act).

The policy intent of section 135AA of the National Health Act is to recognise the sensitivity of health information and restrict the linkage of claims information. Such linkages may reveal detailed information about the health status and history of the majority of Australians, beyond what is necessary for the administration of most government programs. As discussed further below, it should be noted that provision remains for the use of such information for health policy and medical research purposes in certain circumstances.

The purpose of the Rules is to give effect to section 135AA of the National Health Act. The Rules provide specific standards and safeguards for the way that individuals' claims information is to be handled by agencies when stored in computer databases. These standards are in addition to any requirements that may be imposed by the Australian Privacy Principles ('APPs') contained in Schedule 1 to the Privacy Act. The Rules are not intended to set out exhaustively how claims data may be collected, used and disclosed. Agencies may wish to consider the interaction between these Rules and other primary legislation authorising the handling of claims information.

The key objectives of the Rules are to ensure that claims information collected under the Medicare Benefits Program and the Pharmaceutical Benefits Program are held on separate databases, as well

as establishing the circumstances under which this information may be linked and retained in linked form. In addition, the Rules prescribe the circumstances in which claims information may be retained in various forms, such as paper form, or where the claims information is separated from personal identification components.

Background

Section 135AA was first introduced into the National Health Act in 1991 by the *Health Legislation (Pharmaceutical Benefits) Amendment Act 1991*. In 1993, section 135AA was repealed and substituted by the *National Health Amendment Act 1993*. The then Privacy Commissioner first issued what were then guidelines under section 135AA on 24 November 1993, which came into effect on 15 April 1994.

In 2012, the National Health Act was amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* to provide that the Australian Information Commissioner issue rules, rather than guidelines, under section 135AA. The *National Health (Privacy) Rules 2018* (the 2018 Rules) were issued in 2018. These rules were made in substantively the same terms as the previous guidelines in the *National Health Act 1953 – Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs* (the 2008 guidelines).

In May 2021, the Information Commissioner published a consultation paper for the *National Health (Privacy) Rules 2018* review. The old rules were a remake, in substantially the same terms, of the 2018 Rules, for three years until 1 April 2025 to allow time for the consultation and redrafting of the rules to be finalised following the review, noting that subsection 135AA(8) requires any remade Rules to be lodged in advance of the sunset or repeal date commencing from the first day on which they are no longer liable to be disallowed.

Consultation and review of the old rules

Before issuing rules under section 135AA of the National Health Act, the Information Commissioner is required under subsection 135AA(6) to take reasonable steps to consult with organisations, including agencies, whose interests would be affected by those rules. Consultation is also required in accordance with section 17 of the *Legislation Act 2003*.

The Office of the Australian Information Commissioner (OAIC) has now completed a review to consider the operation of the Rules, which included targeted and public consultation.

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

On 1 July 2021, IIS provided its draft Report to the OAIC. The OAIC had an opportunity to review the draft report and provide feedback before the Final Report was finalised on 27 July 2021.

On 14 September 2021, the OAIC provided a copy of the Final Report to the Department of Health, Services Australia, the Australian Digital Health Agency (ADHA), and the Office of the National Data Commissioner (ONDC) and commenced further targeted consultation.

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

The IIS recommendations were also developed before the *Data Availability and Transparency Act 2022* (the DAT Act) came into operation on 1 April 2022. The OAIC's response to the IIS recommendations has since been adjusted to reflect the impact of the DAT Act, which may also apply to the sharing of claims information by government agencies (and overrides the application of the Rules in some instances).

The OAIC also conducted frequent targeted consultation with the Department of Health and Aged Care and Services Australia and provided them with the opportunity to comment on the drafting instructions and draft versions of the new Rules. Services Australia and the Department of Health and Aged Care have functions that assist in enabling administration of the Medicare Benefits Schedule and Pharmaceutical Benefits Schedule (MBS and PBS) schemes and for enabling the Department of Health's performance of health provider compliance functions. The OAIC has also engaged with the Office of the National Data Commissioner, Professional Services Review, Australian Bureau of Statistics, Australian Institute of Health and Welfare, Australian Digital Health Agency and other interested agencies while developing the new Rules.

The OAIC released a draft version of the Rules for public consultation on 2 April 2024. Consultation documents, including the IIS Final Report, were made available on the OAIC's website during a 4-week consultation period. Comment was invited from the public and the consultation was shared on relevant social media platforms and with relevant OAIC stakeholders through promotion via a monthly newsletter just before the consultation period commenced and towards the end of the period. A direct email was also sent to stakeholders that participated in the 2021 consultation conducted by IIS. The OAIC received 4 public submissions and conducted further targeted consultation with interested stakeholders.

In line with the objects set out in section 2A of the *Privacy Act 1988*, in our review of the Rules we have actively sought to balance privacy considerations with the interests of government and researchers in conducting public health activities, and to promote the responsible handling of personal information by such entities. All feedback received was carefully considered and assisted in progressing the review.

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

The key features of the new draft Rules influenced by the IIS Final Report and stakeholder submissions are:

- simplified structure and greater clarity, including in relation to the Rules' application to government agencies and operation of provisions relating to data separation, old information, and disclosures for medical research purposes
- introduction of express provisions to authorise the use of claims information
- requirements for data-sharing agreements to govern the disclosure of claims information
- introduction of the principle of data minimisation which will apply to most authorised uses and disclosures as well as all authorised linkages of claims information
- aligned destruction of linkage requirements for all agencies subject to the Rules, to ensure valuable public policy uses can continue and for greater consistency with other data governance frameworks
- amendments to ensure the traceability of linkages conducted in accordance with the Rules.

Changes made since the public consultation process to address further comments raised by stakeholders include:

- Extending storage requirements to all agencies to correct the inconsistent application of the Rules, which did not impose requirements on secondary agencies
- Removing technical specification and variation reporting requirements which are no longer justifiable, and would have imposed an unjustifiable reporting burden on agencies
- Extending disclosure requirements regarding medical research to agencies to further ensure the uniform application of the Rules to all recipients of claims information
- Clarifying that the Rules are not intended to override other laws which require or authorise the disclosure of claims information
- Clarifying provisions relating to linkage of claims information, and linkage of old information with personal identification components
- Updating authorisations for linking to reflect developments in government information handling and digital technologies
- Extending linkage reporting requirements to all agencies to ensure appropriate oversight and transparency arrangements in line with the statutory intention behind 135AA
- Specifying 6 months as the applicable transitional period.

The Australian Information Commissioner is of the view that the above consultation process has been appropriate and satisfies the obligation to take reasonable steps to consult with organisations, including agencies, whose interests would be affected by those rules.

Statement of Compatibility with Human Rights

Subsection 9(1) of the *Human Rights (Parliamentary Scrutiny) Act 2011* requires the rule-maker in relation to a legislative instrument to which section 42 (disallowance) of the *Legislation Act 2003* applies, to cause a statement of compatibility to be prepared in respect of that legislative instrument. This instrument is compatible with the human rights and freedoms recognised or declared under section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*. A full statement of compatibility is set out in **Attachment B**.

Details of the *National Health (Privacy) Rules 2025*

Part 1—Preliminary

Section 1 Name

This section states that the name of the instrument is the *National Health (Privacy) Rules 2025*.

Section 2 Commencement

This section relates to the commencement of the Rules. It provides that the whole instrument commences the later of the day after the first day on which this instrument is no longer liable to be disallowed or 1 April 2025. Paragraph (a) of the table item reflects the operation of paragraph 135AA(8)(a) of the National Health Act. Paragraph (b) of the table item is permitted by paragraph 135AA(8)(b) of the National Health Act.

Section 3 Authority

This section states that section 135AA of the National Health Act is the authority under which the instrument is made.

Section 4 Schedule 2

This section states that each instrument that is specified in Schedule 2 to the Rules is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this instrument has effect according to its terms. The effect of section 4 and Schedule 2 is to repeal the old rules, with effect from when the Rules commence.

Section 5 Definitions

This section defines certain terms used in the Rules.

A note to this section explains that a number of terms used in the Rules are defined in subsections 5(1) of the Rules and 135AA(11) of the National Health Act. In defining 'claims information', subsection 5(1) of the Rules adopts the meaning of information to which section 135AA applies contained in subsection 135AA(1) read with subsection 135AA(2) of the National Health Act.

This subsection also adopts the definition of 'enforcement body' in section 6 of the Privacy Act and the definition of 'principal executive' in section 37 of the Privacy Act.

Subsection 5(1) of the Rules now defines the meaning of 'Medicare PIN' or 'Medicare personal identification number'. This definition is based on subsection 7(8) of the old rules.

The Rules also introduce new definitions for 'primary agency' and 'secondary agency', which did not previously appear in the old rules. The Department administered by the Minister administering the *Health Insurance Act 1973* (currently the Department of Health and Aged Care, defined as the 'Health Department') and Services Australia are each a primary agency for the purposes of the Rules. An agency other than the Health Department and Services Australia is a 'secondary agency'. An 'agency' means an agency as defined in section 6 of the Privacy Act, as provided in subsection 135AA(11) of the National Health Act.

The introduction of the terms 'primary agency' and 'secondary agency' is in response to recommendations from the IIS review of the old rules, and are intended to provide greater consistency and clarity in how the Rules apply to all government agencies using claims information. Each Part of the new Rules contains provisions which clearly indicate whether they apply to primary and/or secondary agencies. Certain provisions continue to apply only to primary agencies due to the specific responsibilities and functions of Services Australia and the Health Department in relation to claims information, including the health provider compliance functions.

Subsection 5(1) defines 'health provider compliance function' as a statutory function, duty or power of the Secretary of the Health Department under the National Health Act, or the Chief Executive Medicare under 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. Paragraph 5(1)(c) of the *Human Services (Medicare) Act 1973* provides that the Chief Executive Medicare's functions include any functions conferred on the Chief Executive Medicare under any other Act. The definition of 'health provider compliance function' is therefore intended to capture functions of the Chief Executive Medicare under other Acts including the National Health Act, *Dental Benefits Act 2008* and *Health Insurance Act 1973*.

Subsection 5(1) of the Rules also introduces the 'data minimisation principle', which is that, when disclosing, using or linking claims information for a particular purpose, only the claims information reasonably needed to achieve the purpose is disclosed, used or linked. The data minimisation principle is relevant for the operation of sections 10, 11, 14, 15 and 19 of the Rules. The introduction of a data minimisation requirement partially implements a recommendation of the IIS review of the Rules and is intended to ensure that agencies do not use, disclose or link more claims information than is reasonably necessary.

This section has also been updated to include definitions of references to destroying linked claims information and references to tracing linkages of claims information (see subsections 5(2) and 5(3) of the Rules). These provisions are intended to provide greater clarity for agencies about their obligations in relation to linkages and traceability. Subsection 5(2) clarifies that a reference to destroying linked or re-linked claims information encompasses destroying both the linked or re-linked claims information and any additional information produced in order to link or re-link the claims information, as well as otherwise ensuring that the claims information is no longer linked or re-linked and that the linked or re-linked information is no longer stored. Subsection 5(3) provides that a reference to tracing linkages or re-linkages of claims information means ensuring that the following is reasonably ascertainable: when and what claims information was linked or re-linked, who linked or re-linked the claims information and when the linked or re-linked claims information was destroyed. This expands an obligation under the old rules to all agencies and responds to a recommendation from the IIS review that linkages conducted under the Rules should be traceable.

Section 6 Simplified outline of this instrument

This section provides an overview of the operation of the Rules and is a new addition to the Rules. The structure of the Rules has been substantially revised. In particular, the Rules are now divided into parts that mirror each of the paragraphs of subsection 135AA(5) of the National Health Act.

While the simplified outline is included to assist readers to understand the substantive provisions, the outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions.

Part 2—Ways in which claims information may be stored

Section 7 Storage of claims information

Subsection 7(1) applies to all agencies within the meaning of s 6 of the Privacy Act and provides for certain requirements to be met for an agency to be able to store claims information in a database. This subsection requires an agency to establish and maintain certain technical specifications relating to the database, including measures limiting access to the database, ensuring adequate security arrangements are made and relating to the destruction and tracing of linked claims information (within the meaning of those terms as provided by subsections 5(2) and 5(3) of the Rules). Subsection 7(1) is based on subsections 7(4) and 7(5) of the old rules and is in materially the same terms as the equivalent provisions in the old rules, except subsection 7(1) now applies to all agencies, as opposed to only Services Australia. The requirement for Services Australia to notify the Information Commissioner of the specifications of storage and any variations made to the specifications (subsection 7(7) of the old rules) was, in the exposure draft version of the Rules, going to be expanded so that it applies to all agencies. Instead, it has been removed after consultation, as this requirement would have imposed an unjustifiable burden on agencies.

Subsection 7(2) provides that an agency, within the meaning of s 6 of the Privacy Act, may store a Medicare PIN in a database that stores claims information. This provision is based on subsection 7(7) of the old rules and is in materially the same terms.

Subsection 7(3) ensures that claims information in the Medicare Benefits Program and Pharmaceutical Benefits Program databases are stripped of personal identification components, such as name and address information, with the exception of a Medicare card number, or a Pharmaceutical entitlements number. However, this is subject to the requirements for storage of old information in subsection 18(2) of the Rules. Subsection 7(3) is based on subsection 7(3) of the old rules with some change. In the old rules, the requirement for claims information to be stored without its personal identification components was separated into different provisions relating to claims information that is not old information and old information (subsections 7(3) and 10(1) of the old rules respectively), being claims information that has been held by an agency for at least the preceding 5 years (see subsection 135AA(11) of the National Health Act). Subsection 7(3) now applies to the storage of claims information generally (which includes the storage of old information).

The purpose of extending storage requirements to cover all agencies is to ensure uniform regulation of all agencies storing claims information. The new Rules require all agencies have a documented approach in place that governs how they access, link, store and destroy claims information, providing regulatory assurance that the requirements of the Rules are being met. This reflects the sensitivity of claims information, and the fact that 135AA specifically requires the Rules to stipulate relevant arrangements. Several stakeholders commented that the technical standards requirement should be maintained or more prescriptive. The policy intention is to create consistency between all agencies in the way claims information is handled and stored while not imposing an onerous or duplicative burden on agencies.

Section 8 Prohibition relating to storing claims information with enrolment and entitlement database

This section provides for the separation of databases storing claims information obtained under the Medicare Benefits Program or the Pharmaceutical Benefits Program from databases maintained for the purpose of identifying persons who are eligible to be paid benefits under those programs. As confirmed by paragraph 135AA(2)(b) of the National Health Act, information contained in a database maintained for this purpose of identifying eligibility, that does not contain information relating to claims

for payment of benefits, is not covered by section 135AA and is thus not claims information. This section is based on subsection 7(2) of the old rules and is in materially the same terms.

The prohibition in subsection 8(1) is distinct from the prohibition on storing Medicare Benefits Program claims information in the same database as Pharmaceutical Benefits Program claims information, which is provided for in section 12 of the Rules. Database has been used in accordance with its ordinary meaning for the purpose of the Rules.

The separation of enrolment and entitlement information from claims information reflects the original purpose for which these Rules were created, to recognise the sensitivity of health information and restrict the potential linkage of claims information beyond what is provided for in the Rules.

Section 9 Circumstances in which creating copies of claims information in paper or similar form is prohibited

This section prohibits agencies from copying claims information or Medicare Benefits Program and Pharmaceutical Benefits Program databases in paper or similar form unless it is reasonably necessary to do so for a lawful purpose. This provision gives effect to paragraph 135AA(5)(a) of the National Health Act, which requires the Rules to specify the circumstances in which creating copies of information in paper or similar form is prohibited. Section 9 of the Rules is based on subsection 14(1) of the old rules and is in materially the same terms.

This section applies to all agencies within the meaning of s 6 of the Privacy Act.

Prohibiting the creation of copies of claims information in paper or similar form unless reasonably necessary for a lawful purpose is intended to recognise the sensitive nature of claims information and prevent unnecessary risks to the security of such information outside of the secure storage of the databases required by these Rules. Creating a copy of the whole or major proportion of either database poses similar security risks to the information. A similar form would include information copied to a word document.

Part 3—Uses to which agencies may put claims information

Section 10 Use of claims information

This section provides for the uses to which agencies may put claims information. Section 10 is made for the purposes of paragraph 135AA(5)(b) of the National Health Act, which requires the Rules to specify the uses to which agencies may put information. The Health Department may use the relevant claims information for any of the purposes listed in the 4 items to the table in section 10 and Services Australia may use the relevant claims information for any of the purposes listed in items 2 to 4. Other agencies may use claims information if authorised by items 3 or 4.

Item 1 provides that the Health Department may use any claims information to perform health provider compliance functions. Health provider compliance functions are defined under subsection 5(1). Under item 2, a primary agency may use any claims information for the purposes of medical research, statistical analysis or development of government policies and programs where the use complies with the data minimisation principle.

Item 3 provides that an agency may use claims information that was disclosed to the agency under the Rules to achieve the particular purpose for which it was disclosed, to the extent that the use complies with the data minimisation principle. This applies to any disclosures authorised by section 11 of the Rules. Where a primary agency discloses claims information to a secondary agency in accordance with a data sharing agreement, clause 2 of Schedule 1 requires the agreement to specify the purposes for which the recipient may use the information.

Under item 4, an agency may use any claims information for any use that is required or authorised by law (other than by section 10). This recognises the fact that other legislation may authorise the use of claims information by agencies.

Section 10 is based on subsection 12(1) of the old rules. It has a broader application than its equivalent provision under the old rules in that it provides for permitted uses relating to all government agencies, as opposed to only making provision for the use of information provided to the Health Department by Services Australia. This reflects the recommendation from the IIS review that all government agencies which handle claims information should be regulated by the Rules, and will ensure the Rules are up-to-date for the current environment in which a number of agencies handle claims information.

Part 4—Circumstances in which agencies may disclose claims information

Section 11 Circumstances in which agencies may disclose claims information

This section sets out rules permitting certain disclosures of claims information for the purposes of paragraph 135AA(5)(c) of the National Health Act, which requires the Rules to specify the circumstances in which agencies may disclose information. The section amalgamates the requirements of multiple provisions from the old rules, to simplify the structure of the Rules and improve their useability in line with a recommendation from the IIS review. As the Rules are intended to apply to all agencies handling claims information, the disclosure provisions have been amended to more clearly provide for disclosures by primary agencies to other agencies, pursuant to a data sharing agreement. This section also clarifies that where a disclosure is otherwise required or authorised by another law, the Rules are not intended to override those provisions.

Subsection 11(1) provides that subsections (2) to (9) do not limit each other.

Subsections 11(2) to 11(4) provide that Services Australia may disclose to the Health Department:

- claims information where the disclosure is for the purposes of the performance of the health provider compliance functions, or
- claims information so long as it does not also disclose personal identification components, an algorithm which enables an encrypted Medicare card number to be unencrypted, or the name corresponding to a Medicare PIN, or
- personal identification components that correspond to a particular Medicare PIN where the Secretary has decided that the disclosure is necessary to clarify which information relates to a particular individual or for the purposes of disclosing personal information as expressly authorised or required by or under law.

Subsections (2) to (4) are based on subsections 7(9), 13(1) and 13(2) of the old rules but have been restructured for greater clarity.

This section also introduces a requirement for the use of 'data sharing agreements' when disclosing claims information in certain circumstances. A data sharing agreement is defined in section 4 of the Rules to mean a data sharing agreement that complies with Schedule 1 to the Rules, or such an agreement as varied by the parties. As explained below, Schedule 1 sets out the requirements for data sharing agreements, including the provisions that such agreements must contain. The introduction of data sharing agreement requirements implements a recommendation from the IIS review and is aimed at enhancing the protection of claims information once it has been disclosed.

Subsection 11(5) permits the disclosure of old information from the Health Department to Services Australia for 2 reasons: for a certain permitted purpose specified in paragraph 19(1)(a) or for inclusion in a database in which Services Australia stores old information from the Medicare Benefits Program or the Pharmaceutical Benefits Program. Section 11(5) is made in materially similar terms as subsection 10(7) of the old rules.

Subsection 11(6) provides that a primary agency may disclose claims information to a secondary agency where the disclosure is in accordance with a data sharing agreement, complies with the data minimisation principle and does not include both the name and the Medicare PIN of any person to whom disclosed claims information relates. The disclosure must not be for the purpose of the agency undertaking medical research – disclosures for medical research purposes are covered by subsection 11(7). Subsection 11(6) is based on subsection 7(15) of the old rules, but has been revised to include the new requirements relating to data sharing agreements and the data minimisation principle.

Subsection 11(7) permits a primary agency to disclose claims information to an agency or a person who is not an agency for the purpose of medical research in certain circumstances. Claims information from which an individual is reasonably identifiable may only be disclosed with that individual's consent or where the research is to be conducted in compliance with guidelines issued by the National Health and Medical Research Council under section 95 of the Privacy Act as in force from time to time. Guidelines shall be issued under section 95 of the Privacy Act by being published in the Gazette (see subsection 95(3) of the Privacy Act) and may be freely accessed and used by members of the public on the Federal Register of Legislation.

These arrangements reflect obligations that would apply under the Privacy Act and related laws regardless of whether this section is made. However, the Information Commissioner is satisfied that the inclusion of this section clarifies and provides certainty regarding how claims information may be used for medical research purposes.

Subsection 11(7) is based on section 11 of the old rules and is in materially similar terms. However, subsection 11(7) of the Rules imposes new requirements that the disclosure must be in accordance with a data sharing agreement and comply with the data minimisation principle. The requirement under subsection 11(2) of the old rules to obtain a written undertaking that the claims information will be securely destroyed is now encapsulated in the requirements of a data sharing agreement under Schedule 1 to the Rules. This requirement must be complied with by virtue of paragraph 11(7)(a) of the Rules.

Subsection 11(8) is a new addition to the Rules and permits a primary agency to disclose claims information to another agency for the purposes of consultation about the appropriateness of disclosures for medical research under subsection 11(7). This new section is a result of the IIS review which recommended that a provision be inserted 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 section 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.

Subsection 11(9) is also a new provision and states that an agency may disclose claims information as required or authorised by another law. This is aimed at providing clarity for agencies that the Rules are not intended to override disclosure provisions in other legislation. This section reflects principles of statute law which apply regardless of whether this section is made. However, the Information Commissioner is satisfied that the inclusion of this section clarifies and provides certainty that the Rules are not exhaustive and not intended to prevail over primary legislation. As an example, the DAT Act establishes a regulatory scheme that authorises agencies to share information, provided the requirements of the DAT Act are met, despite anything in another law of the Commonwealth, including these Rules. Similarly, claims information released under section 130 of the *Health Insurance Act 1973* or section 135A of the Act are examples of disclosures that may be required or

authorised by law under section 11(9). Disclosures which are covered by subsection 11(9) do not require a data sharing agreement to be in place (subject to the requirements of the authorising law).

A note beneath subsection 11(9) clarifies how the subsection operates in relation to secrecy provisions that are set out in other Commonwealth laws. It provides, as an example of the operation of the subsection, lawfully disclosing claims information in accordance with the secrecy provisions of a law of the Commonwealth. The effect of an example in legislation is dealt with by section 15AD of the *Acts Interpretation Act 1901* and paragraph 13(1)(a) of the *Legislation Act 2003*, which together have the effect that, if a legislative instrument includes an example of the operation of a provision, the example is not exhaustive, and the example may extend the operation of the provision.

Part 5—Prohibition relating to storage of claims information in the same database

Section 12 Prohibition relating to storage of claims information in the same database

This section prohibits agencies from storing Medicare Benefits Program and Pharmaceutical Benefits Program claims information in the same database and is made for the purposes of paragraph 135AA(5)(d) of the National Health Act, which requires a prohibition against agencies storing claims information on the one database.

The intention of the prohibition is to ensure the functional separation of claims information collected under the Medicare Benefits Program and Pharmaceutical Benefits Program, including to prevent them from being searched and accessed simultaneously through a single search process.

However, under subsection 12(2) of the Rules, a primary agency may store such information in the same database where it is necessary for an activity that is expressly authorised by the Rules. This recognises that s 135AA(5)(e) permits the linkage of claims information in circumstances that are authorised by the Rules, regardless of whether this may also involve storage of the information.

Subsection 12(3) clarifies that subsection 12(1) does not prevent an agency storing claims information in the same computer system. However, where claims information is stored within the same computer system, the data must be subject to functional and/or access controls, as appropriate, to ensure that Medicare Benefits Program and Pharmaceutical Benefits Program claims information cannot be accessed simultaneously through a single process (such as a keyword search).

Section 12 of the Rules amalgamates the requirements of subsections 6(1), 7(1) and 10(1) from the old rules. However, the requirement under subsection 12(2) of the Rules is a new addition. The new consolidated provision is intended to reduce duplication, which was recommended by the IIS Final Report, and provides greater clarity for agencies about the storage restrictions for claims information. New subsection 12(2) clarifies the relationship between the prohibition and the linkage provisions in the Rules, as recommended by IIS.

Part 6—Prohibitions on linkage, and authorisations

Part 6 of the Rules deals with linkages of claims information. It is made for the purposes of paragraph 135AA(5)(e) of the National Health Act. The central prohibition on linkage of claims information is contained in section 13 of the Rules, as mandated by paragraph 135AA(5)(e) of the National Health Act. The authorisations for ways of linking claims information are contained in Part 6 of the Rules, as also provided for by paragraph 135AA(5)(e) of the National Health Act.

It is necessary and appropriate for these matters to be dealt with in delegated legislation, rather than in primary legislation. In the modern world, the use of data and information for a range of purposes by

government and by the private sector is becoming more frequent and important. Information technology, and the uses to which data and information might be put, is a rapidly-advancing and fast-changing area, and is heavily influenced both by technological innovations and by the changing needs of government and other entities. Delegated legislation is a better suited means of regulation in these circumstances, given how much more rapidly delegated legislation can be updated to deal with changing external circumstances, to facilitate additional uses of information that might become beneficial, and to protect against privacy risks that might emerge as technology develops.

Division 1—Prohibition on linkage of claims information

Section 13 Prohibition of linkage of claims information

This section prohibits agencies (within the meaning of that term as defined in the Privacy Act) from linking claims information that is held in a database maintained for the purposes of the Medicare Benefits Program and claims information that is held in a database maintained for the purposes of the Pharmaceutical Benefits Program, unless the linkage is authorised in a way specified in the Rules. Part 6 Division 2 of the Rules makes provision for the circumstances in which the linkage of claims information by a primary agency or a secondary agency is authorised.

The purpose of this section is to in part give express effect to paragraph 135AA(5)(e) of the National Health Act, which requires that rules be made prohibiting the linkage of claims information except in circumstances authorised by the Rules. Section 13 of the Rules is a new addition.

Section 13 provides greater clarity for agencies that sections 14, 15 and 19 of the Rules, which authorise the linkage of MBS and PBS claims information, are intended to exhaustively prescribe the circumstances in which such linkages can be performed under the Rules. However, as noted in the Rules, nothing in the Rules precludes the matching of information under subsection 132B(1) of the Act, or the operation of Part VIIIA of the Act generally: see subsection 135AA(5C).

Linkage is separate from use for the purpose of section 10 of these Rules, and should be treated as an intermediate step to support the use of claims information.

Division 2—General authorisations for linkage of claims information

Section 14 Authorised linkages—all agencies

This section gives effect, in part, to paragraph 135AA(5)(e) of the National Health Act by authorising the linkage of claims information by an agency (including a primary agency) for the purposes of the general prohibition on linkage of claims information in section 13 of the Rules. In particular, section 14 authorises the linkage of claims information relating to the same individual by way of a Medicare PIN in circumstances where:

- the linkage is necessary for a use that is permitted by section 10 of the Rules and is authorised by the principal executive of the relevant primary agency
- the (linking) agency destroys the linked claims information as soon as practicable after the purpose for which the information has been linked has been met
- the agency has in place measures to ensure that the linkages of claims information are traceable
- the agency makes arrangements for the security of records of linked claims information and
- the linkage complies with the data minimisation principle (as defined in section 5 of the Rules).

Section 14 is based on subsections 12(3) and 12(4) of the old rules but has been substantially revised. In particular, the operation of the provision has been extended to apply to all agencies (where the principal executive of the relevant primary agency that disclosed the information approves the linkage), whereas subsection 12(3) of the old rules only explicitly governed the Health Department's linkage of claims information. Section 14 of the Rules also removes the requirement that the claims information be used solely as a necessary intermediate step to obtain aggregate or de-identified information (see paragraph 12(3)(b) of the old rules). However, section 14 incorporates a number of additional privacy protections which will apply to all agencies carrying out linkages, including a requirement to ensure the traceability and security of linked claims information. All agencies conducting linkages must also comply with requirements in relation to the storage of claims information under section 7, as well as annual reporting requirements under section 17.

The IIS Final Report acknowledged that a number of agencies are currently conducting linkage activities in relation to claims information, but that there is uncertainty about what activities are allowed as well as gaps in protection. The broadened scope of the linkage provisions under the Rules is intended to ensure that clear and consistent requirements apply to all agencies in relation to linkages, while enabling valuable activities, such as research, to continue in the public interest where accompanied by strong protections.

Section 15 Authorised linkages—primary agencies only

This section gives effect, in part, to paragraph 135AA(5)(e) of the National Health Act by authorising the linkage of claims information by a primary agency for the purposes of the general prohibition on linkage of claims information in section 13 of the Rules. Section 15 is based on subsections 8(1),9(1) to 9(4) and 10(2) of the old rules but has been substantially revised. Subsection 15(1) authorises the linkage of claims information relating to the same individual for a permitted purpose in circumstances where the primary agency:

- destroys the linked claims information (within the meaning of that term as provided by subsection 5(2) of the Rules) as soon as practicable after the purpose for which the information has been linked has been met
- ensures the linkage is traceable (within the meaning of that term as provided by subsection 5(3) of the Rules) and makes arrangements for the security of records of linked claims information and
- complies with the data minimisation principle (as defined in section 5(1) of the Rules).

Agencies linking information under section 15 will also need to comply with annual reporting requirements under section 17.

The practicability of destruction for the purpose of paragraph 15(1)(c) may be determined in part by reference to the destruction schedules required by paragraph 7(1)(e). For example, where claims information is linked for the purpose of providing an individual's consolidated claims history to that individual, the purpose of that linkage is effectively met at the moment the disclosure occurs. It may not be practicable for that linked dataset to be destroyed instantaneously, though it may be practicable for its destruction to be effected within a defined destruction cycle of a few days.

Any destruction schedule would only be applicable to the extent that it is consistent with the intent of the enabling legislation and Rules. In the above example, it would be unlikely to be appropriate for such datasets to only be deleted as part of a cycle that occurs every few months.

Subsection 15(2) provides for circumstances which constitute a permitted purpose for the linking of claims information by a primary agency. Broadly, permitted purposes include circumstances where the linkage of claims information is:

- reasonably necessary to enforce the criminal law, a law imposing a pecuniary penalty or for the protection of the public revenue
- required or authorised by law
- for determining an individual's eligibility for benefits
- for preventing or lessening a serious and imminent threat to the life or health of any individual
- for disclosing to an individual their own claims information or to another person on their behalf when that individual has given their consent
- for taking action on unresolved compensation, on an investigation or a prosecution, or for recovery of a debt
- for determining entitlements to certain late lodged claims and related services
- for lawfully disclosing identified information in accordance with the secrecy provisions of a law of the Commonwealth
- for the performance of the health provider compliance functions, in the case of the Health Department.

An example of an 'investigation or prosecution' includes an investigation or prosecution of persons for any offences relating to the Medicare Benefits Program or the Pharmaceutical Benefits Program.

Section 16 Circumstance in which linkage is not authorised

This section provides that despite the provisions that provide authorisation for linkage of claims information in Part 6 Division 2, a linkage for the purposes of a primary agency establishing a data-matching program between databases maintained for the purpose of the Medicare Benefits Program and the Pharmaceutical Benefits Program is not authorised. Section 16 of the Rules is based on subsection 8(2) of the old rules and is in materially similar terms.

Preventing the creation of a data-matching program for MBS and PBS information reflects the original purpose for which these Rules were created, to recognise the sensitivity of health information and restrict the potential linkage of claims information beyond what is provided for in the Rules, given such linkages may reveal detailed information on the health status and history of the majority of Australians.

Section 17 Reporting requirements in relation to linkages

Section 17 requires an agency to provide the Information Commissioner with a report on linkage activities for the previous financial year. The purpose of this provision is to provide a form of additional oversight and to promote transparency in how claims information is linked.

The report must include the number of records that were linked and a breakdown of those records by reference to the particular purpose for which the linkage was permitted (see subparagraph 17(b)(i)). These requirements are intended to provide the Information Commissioner with oversight of the extent and nature of data linkage activities being carried out under the Rules by requiring information on how many datasets were created and for what purpose.

The report prepared under section 17 must also include the number of records of linked claims information that were destroyed (within the meaning of that term as provided by subsection 5(2) of the Rules), and a breakdown of those records by reference to the permitted purpose (see subparagraph 17(b)(ii)). With regard to records of linked claims information that have not been destroyed (either during the reporting period or during an earlier reporting period), the report must include the number of such records and the reason that the information was not destroyed (see subparagraphs 17(b)(iii) and (iv)). These requirements are intended to provide the Information Commissioner with an indication as to whether linked datasets are being retained for periods of time that may be longer than envisaged, and if so, why. In particular, if the number of datasets reported

under paragraph 17(b)(iii) were to be significant, it could indicate that these datasets were being retained for periods that are inconsistent with the policy intent of the National Health Act. In such circumstances, it would be open for the Information Commissioner to make further enquiries of the agency (including, where necessary, by exercising formal assessment powers).

Part 7—Requirements with which agencies must comply in relation to old information

Section 18 Requirements relating to storage of old information

Paragraph 135AA(5)(f) of the National Health Act requires the Information Commissioner to make rules concerning the handling of 'old information'. 'Old information' is defined as claims information that has been held by one or more agencies for at least five years (see subsection 135AA(11) of the National Health Act). It particularly requires that this old information be stored without its 'personal identification components' (also defined in subsection 135AA(11)).

Under subsection 18(1), an agency must strip such claims information of its identifying components after five years. This provision is in similar terms to subsection 10(1) of the old rules, but removes the reference to storage of old information from the Medicare Benefits Program and the Pharmaceutical Benefits Program in separate databases, as this requirement is now covered by section 12 of the Rules (which applies to both old information and claims information that is not old information).

Although under subsection 7(3) the storage of Medicare card numbers and Pharmaceutical entitlement numbers with claims information is permissible, this is prohibited in the case of old information (see subsection 18(2)).

Subsection 18(3) provides that section 18 does not prevent an agency from storing old information and claims information that is not old information in the same database, subject to section 12.

Separating old information from personal identification components and from Medicare card numbers and Pharmaceutical entitlement numbers with claims information is an important protection to ensure the security of claims information and prevent potential linkage of claims information beyond what is provided for in the Rules, given such linkages may reveal detailed information on the health status and history of the majority of Australians.

Section 19 Requirements relating to re-linking old information with personal information components

This section specifies the circumstances in which, and the conditions subject to which, personal identification components may later be re-linked with the rest of the information, for the purpose of subparagraph 135AA(5)(f)(iii) of the National Health Act (noting that as set out above, under s 18 agencies must strip claims information of its identifying components after five years).

Under section 19, a primary or secondary agency may only re-link old information with personal identification components by use of a Medicare PIN and for certain permitted purposes. This section has been expanded to all agencies after the IIS report and public consultation highlighted the need for uniform regulation of linkages performed by both primary and secondary agencies. Section 19 stipulates that a primary or secondary agency may re-link old information with personal identification components if necessary to enable a linkage authorised by section 14 or paragraphs 15(2)(f), (g), (h), (i) or (j). Authorisation pursuant to paragraph 15(2)(f), (g), (h), (i) or (j) is materially similar in terms as subsection 10(2) of the old rules.

Once the purpose for which the old information has been re-linked with its personal identification components has been fulfilled, the re-linked dataset must be destroyed (within the meaning of that

term as provided by subsection 5(2) of the Rules) as soon as practicable (see paragraph 19(c) of the Rules). As with linked claims information in section 15, what is a 'practicable' period within which datasets must be deleted may be determined in part by reference to the destruction schedule specified in paragraph 7(1)(e) (although such determination is not bound by this). Paragraph 19(c) of the Rules is made in materially the same terms as subsection 10(3) of the old rules subject to the expansion to all agencies described above.

An agency must ensure that re-linkages of old information with their personal identification components are traceable (within the meaning of that term as provided by subsection 5(3) of the Rules) and must make arrangements for the security of re-linked old information (paragraphs 19(d) and (e)). These requirements are also stipulated by paragraphs 7(1)(a) and (d) of the Rules. Paragraph 19(e) of the Rules is made in materially the same terms as subsection 10(4) of the old rules subject to the expansion to all agencies described above.

Allowing for personal identification components to be re-linked with old information only for the prescribed permitted purposes and subject to the requirements for destruction, tracing and security assists in the overall objectives of the Rules to protect and acknowledge the sensitive nature of claims information.

Section 20 Requirements relating to reporting—old information

Section 20 places reporting obligations on agencies under which they must report annually to the Information Commissioner on how they have handled old information that has been re-linked with personal identification components.

Such reports must include details similar to those required for the linkage of claims information under section 17. Section 20 of the Rules is based on subsection 10(5) of the old rules and is in materially similar terms.

This section has been expanded to apply to all agencies, now that all agencies are subject to uniform regulation under the Rules. This implements a key recommendation and finding of the IIS Report which highlighted the inconsistent application of the old rules. Previously, multiple obligations in the old rules applied only to Services Australia and the Department of Health and Aged Care despite other agencies' use and handling of claims information.

Part 8—Application and transitional provisions

Section 21 Agency may comply with certain provisions of the *National Health (Privacy) Rules 2021* during the grace period

This section provides that during the six month period commencing on the day that the Rules commence, an agency may store or use certain claims information in accordance with the Rules or the old rules as if the old rules had not been repealed. The six month 'grace period' begins when the Rules commence – see section 2 – and not when the Rules are made.

Schedule 1—Data sharing agreements

Clause 1 Requirements for data sharing agreements

This clause sets out the requirements of data sharing agreements (as defined by section 5 of the Rules), which are required for certain disclosures of claims information by primary agencies under section 11 of the Rules. A data sharing agreement must be in writing and must include the provisions

specified in the relevant clause of Schedule 1. Provisions relating to data sharing agreements are a new addition to the Rules.

Clause 2 Data sharing agreements—disclosure under subsection 11(6)

This clause sets out the particular requirements of data sharing agreements where the recipient of the data to be shared is an agency, and where the disclosure is under subsection 11(6) of the Rules (that is, where the claims information is not disclosed for the purposes of medical research).

Subclauses (1) and (2) of clause 2 provide for data sharing agreements to deal with how disclosed claims information can be used. A data sharing agreement must be for only the certain purpose specified in the agreement. The recipient may only use the information disclosed under the agreement for one or more of the following purposes:

- use for research (other than medical research – medical research is dealt with under clause 3)
- statistical analysis
- development of government policies and programs
- consulting under subsection 11(8)
- linking claims information under section 14.

Subclauses (3) and (4) of clause 2 provide for data sharing agreements to deal with re-identification of de-identified claims information. Data sharing agreements must include a requirement that, if de-identified claims information is disclosed to the recipient in accordance with the agreement, the recipient is not to re-identify the information other than in accordance with the agreement. Where the recipient re-identifies claims information contrary to the agreement, a data sharing agreement must also require the recipient to notify the disclosing agency, as well as notifying of certain actions taken in response.

De-identification is a process which involves the removal or alteration of personal identifiers, followed by the application of any additional techniques or controls required to remove, obscure, aggregate, alter and/or protect data in some way so that it is no longer about an identifiable (or reasonably identifiable) individual.

In line with this, a de-identification process generally includes two steps. The first is the removal of direct identifiers, such as an individual's name, address or other directly identifying information. The second is taking one or both of the following additional steps:

- removing or altering other information that may allow an individual to be identified (for example, because of a rare characteristic of the individual or a combination of unique or remarkable characteristics that enable identification), and/or
- putting controls and safeguards in place in the data access environment, which will appropriately manage the risk of re-identification.

Subclause (5) requires a data sharing agreement to prevent the recipient from on-disclosing the claims information that was disclosed under the agreement. A legislative note appearing below subclause (5) provides that a data sharing agreement will not prevent a recipient from disclosing information such as de-identified or aggregated information which was derived from, but no longer is, claims information.

The introduction of data sharing agreements is a recommendation from the IIS report which has been implemented with minor adjustments to balance practicability concerns raised by stakeholders.

The new Rules provide that a data sharing agreement:

- deal with re-identification of de identified claims information

- deal with how disclosed claims information can be used; and
- not permit on-disclosure of claims information.

The Rules permit disclosure of claims information in a broader number of circumstances, where compared with the old rules. To ensure the protection of disclosed claims information, data sharing agreements must provide that additional privacy measures will be put in place. The OAIC expects that data sharing agreements will formalise existing agreements between agencies and mandate the inclusion of privacy protective measures in any such agreement.

Clause 3 Data sharing agreements—disclosure under subsection 11(7)

This clause sets out the particular requirements of data sharing agreements where the disclosure is for the purposes of medical research under subsection 11(7).

Subclause (1) of clause 3 provides that a data sharing agreement made under clause 3 must limit the purpose for the use of disclosed information to use for medical research, which must be specified in the agreement.

Subclauses (2) and (3) of clause 3 provide for data sharing agreements to deal with re-identification of de-identified claims information in terms identical to subclauses (3) and (4) of clause 2.

Subclause (4) of clause 3 and the legislative note that appears below it are in identical terms to subclause (5) of clause 2 and the legislative note that appears below it.

Subclause (5) of clause 3 provides that, where the recipient is not covered by the Privacy Act or a State or Territory privacy law, a data sharing agreement must require the recipient to comply with the Australian Privacy Principles in relation to claims information that is personal information as if the recipient were an organisation. The Australian Privacy Principles are contained within Schedule 1 to the Privacy Act. Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not (subsection 6(1) of the Privacy Act). 'Organisation' is defined in section 6C of the Privacy Act as an individual or a certain specified entity that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory. Section 6C also contains other related definitions.

Subclause (6) of clause 3 provides that a data sharing agreement must specify the storage and security requirements for disclosed claims information which the recipient must comply with if the recipient is not an agency.

Subclause (7) of clause 3 provides for data sharing agreements to deal with disposal or destruction of claims information if the recipient is not an agency. In particular, data sharing agreements must require the recipient to dispose of or destroy the disclosed information by a specified date, provide for the recipient to apply to the disclosing agency, in an approved form, for an extension of that date, and permit the agency to extend the date if satisfied that it is needed in order to achieve the purpose for which the recipient may use the information (i.e., medical research).

Where the recipient is not an agency covered by the Rules, the new draft Rules require the data sharing agreement to also deal with:

- compliance with Australian Privacy Principles in appropriate cases
- storage and security requirements; and
- disposal or destruction of claims information

These are obligations that already apply to agencies under the Rules so this section is aimed at ensuring consistent obligations if the recipient is not an agency.

Schedule 2—Repeals

Schedule 2 specifies the old rules as the instrument that is repealed by section 4 of the Rules.

ATTACHMENT B

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011.

National Health (Privacy) Rules 2025

This Disallowable Legislative Instrument is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the *National Health (Privacy) Rules 2025*

The *National Health (Privacy) Rules 2025* (the Rules) are binding rules concerning the handling, by agencies, of information relating to an individual obtained by any agency in connection with a claim for a payment or benefit under the Medicare Benefits Program and the Pharmaceutical Benefits Program. Such information is referred to in the Rules as ‘claims information’. The purpose of the Rules is to give effect to section 135AA of the *National Health Act 1953* (the National Health Act). The Information Commissioner is authorised, and required, to make rules under section 135AA.

The policy intent of section 135AA of the National Health Act is to recognise the sensitivity of health information and restrict the linkage of claims information. Provision remains for the use of claims information in certain circumstances, including for the performance of health provider compliance functions and research and statistical analysis purposes. Provision is also made for the permissible disclosure and linkage of claims information in limited circumstances.

The Rules set out specific standards and safeguards that apply to the handling of individuals’ claims information by agencies when stored in computer databases.

The key objectives of the Rules are to ensure that claims information collected under the Medicare Benefits Program and the Pharmaceutical Benefits Program are held on separate databases, as well as to establish the circumstances under which this information may be linked and retained in linked form. In addition, the Rules prescribe the circumstances in which claims information may be retained in various forms, such as where the claims information is separated from personal identification components. The Rules also put in place regular reporting requirements and a framework for limited retention periods.

The Rules do not replace any requirements that may be imposed by the Australian Privacy Principles (‘APPs’) contained in Schedule 1 to the *Privacy Act 1988* (Privacy Act) but operate in addition to these requirements. In some instances, the Rules set a higher standard of protection for claims information than that required under the Privacy Act and deal with issues not covered by the APPs, including by specifying obligations concerning the retention, de-identification and destruction of claims information. A breach of the Rules constitutes an interference with privacy under section 13 of the Privacy Act.

The Rules replace and substantially revise the *National Health (Privacy) Rules 2021* to address recommendations made in a 2021 independent review carried out by Information Integrity Solutions Pty Ltd. The updated Rules include:

- a simplified structure and improved clarity, including in relation to the Rules’ application to government agencies

- new provisions to expressly authorise the use of claims information
- new requirements for data-sharing agreements to govern the disclosure of claims information to government agencies
- expanded coverage to all government agencies which handle claims information, to ensure that consistent obligations and privacy protections apply
- the introduction of the principle of data minimisation to apply to most authorised uses and disclosures and all authorised linkages of claims information
- amendments to ensure the traceability of all linkages conducted in accordance with the Rules.

Human rights implications

This Disallowable Legislative Instrument engages the following right:

- the right to privacy in Article 17 of the *International Covenant on Civil and Political Rights* (the ICCPR).

Article 17 of the ICCPR states, ‘No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation’ and that ‘Everyone has the right to the protection of the law against such interference or attacks’.

The term ‘arbitrary’ in Article 17(1) of the ICCPR means that any interference with privacy must be in accordance with the provisions, aims and objectives of the ICCPR and should be reasonable in the particular circumstances. The United Nations Human Rights Committee has interpreted ‘reasonableness’ to mean that any limitation must be proportionate and necessary in the circumstances.

The Rules engage and limit the right to privacy by authorising the use and disclosure of claims information, which includes sensitive health information, by government agencies in specified circumstances set out in section 10 (use of claims information) and section 11 (disclosure of claims information). These circumstances include for the performance of the health provider compliance functions (discussed further below) as well as uses for the purposes of research (including medical research), statistical analysis and the development of government policies and programs. The Rules also clarify that disclosures are permitted where they are otherwise required or authorised by law, in recognition of the fact that the Rules are delegated legislation and cannot override authorisations in primary legislation.

The Rules also engage and limit the right to privacy by authorising government agencies to link and store claims information collected under the Medicare Benefits Program and the Pharmaceutical Benefits Program in circumstances set out in sections 14 and 15, and by permitting agencies to re-link old claims information with personal identification components in accordance with section 19. Agencies may link or re-link claims information where necessary for a use authorised by the Rules, where specific privacy-related conditions are met. Primary agencies may link claims information for additional purposes set out at subsection 15(2), including where reasonably necessary for the enforcement of the criminal law or protection of public revenue, to determine an individual’s eligibility for a benefit, or to prevent or lessen a serious or imminent threat to life or health.

The Rules authorise the use, disclosure, linkage and re-linkage of claims information broadly to enable government agencies to undertake functions relating to the development and evaluation of health policy and government programs and the carrying out of research, including public health and medical research.

The Rules also authorise the Department of Health and Aged Care (the Health Department) to use claims information in relation to its functions in overseeing the regulatory compliance of health service providers. Health provider compliance encompasses a broad range of activities aimed at identifying various forms of non-compliance, including incorrect claiming, inappropriate practice, and fraud in

relation to Medicare programs. These functions may relate to a variety of practitioners, non-practitioner individuals, administrators, practices, businesses, and other entities. Consistent with the recommendations made by the IIS Report, this is not intended to facilitate individuated intervention and the Rules prohibit primary agencies from creating a data matching program between an MBS and PBS database.

The Health Department's submission to the public consultation on the review of the old rules highlighted that data held by the Australian Government is a strategic national resource. The Capability Review of the Health Department emphasises the importance of using data to lift the Department's strategic capability to deliver integrated policy addressing the interactions between the various parts of the health and aged care system.

The use of claims information in policy and program development and public health and medical research activities is important for providing information to help the government make decisions and develop programs and policies that positively impact on the health of individuals and the community. The limitation on the right to privacy in this regard pursues the legitimate objective of supporting and improving public health outcomes.

The use of claims information for compliance functions is also critical for ensuring that the Medicare Benefits Program and Pharmaceutical Benefits Program are operating effectively to benefit the Australian community, by improving efficiencies and detecting waste, inappropriate practice and fraud. This pursues the legitimate objectives of protecting public revenue and improving public health.

Provisions in the Rules which authorise the use, disclosure and linkage of claims information are rationally connected to achieving the objectives of improving public health outcomes and protecting public revenue. Linked data assets, the creation of which is facilitated by the Rules, consist of a broad range of data from multiple sources. The integration of these sources enhances the evidence base for research providing insights that are not available from a single data source, and answers to complex questions. The ability to link key health datasets is critical to understanding patient pathways through the health system, and implications for patient health outcomes.

For example, health and aged care data linked with data from other portfolios enabled detailed analysis of vaccination coverage rates among priority groups during the COVID-19 response. This resulted in improved targeting of communications campaigns during the COVID-19 vaccine rollout and boosted the vaccination coverage rate for culturally and linguistically diverse groups.

The linkage of Medicare Benefits Schedule and Pharmaceutical Benefits Schedule (MBS and PBS) data with other datasets can also be used to assist in improving clinical care and access to services ultimately improving the quality and safety of health care.

The Information Commissioner's power to make rules under s 135AA is tightly prescribed. The changes that have been made through the Rules as compared to the old rules enhance the effectiveness of the Rules in achieving the intent of s 135AA, by ensuring strong privacy protections apply to sensitive MBS and PBS data, including data-sharing agreements between agencies, data minimisation obligations and enhanced traceability requirements. The changes also improve the efficient operation of the Rules by enhancing their usability by Australian Government agencies. This is achieved through changes including simplification of the structure of the Rules and enhanced clarity for Australian Government agencies regarding their obligations when handling MBS and PBS claims information, as well as a broadening of the Rules in recognition that agencies other than the Health Department and Services Australia use claims information in connection with government data integration activities.

The Rules include a number of important restrictions and safeguards to ensure that claims information is appropriately managed and protected by government agencies. Claims information reveals health information about individuals who generally do not have a choice about when and how they interact with the health system. The Rules therefore seek to ensure that the use of that information, and

particularly secondary use, remains carefully controlled and subject to additional protections to those that already exist under the Privacy Act. Importantly, a breach of the Rules is enforceable by the Information Commissioner as an interference with privacy for the purposes of the Privacy Act.

In particular, the Rules:

- a) ensure that claims information obtained under the Medicare Benefits Program and the Pharmaceutical Benefits Program are held on separate databases
- b) ensure that Medicare Benefits Program and Pharmaceutical Benefits Program claims information is linked only for specified purposes in the public interest and for limited periods of time, and expressly prohibit linkages for any other purposes
- c) specify agencies' obligations concerning the retention, disclosure, de-identification and destruction of claims information, including a new requirement for data sharing agreements be in place before Services Australia or the Health Department (as primary agencies) disclose claims information
- d) enhance the accountability of agencies by imposing specific rules concerning the handling of claims information, including rules to ensure adequate security of claims information and that linkages of claims information can be traced
- e) limit access to databases holding claims information and require agencies to make adequate security arrangements, including in relation to the destruction and tracing of linked claims information
- f) promote oversight and transparency in how claims information is linked by requiring all agencies provide annual reports to the Information Commissioner detailing linkage activities.

The Rules apply to all government agencies which handle claims information. In doing so, they significantly improve the consistency of the privacy protections that apply to this information and reduce the risk of gaps in protection that was identified by the 2021 independent review.

The inclusion of these safeguards ensures that limits on the right to privacy in the Rules are reasonable, necessary and proportionate measures to improve public health outcomes and protect public revenue by ensuring the efficient functioning of the Medicare Benefits Program and Pharmaceutical Benefits Program.

Conclusion

This Disallowable Legislative Instrument is compatible with human rights. Although the Rules engage and limit the right to privacy by authorising the use, disclosure and linkage of claims information by government agencies, the limitation pursues a legitimate objective of improving public health by permitting agencies to use the information to undertake research and develop and improve public health programs and policies, and to ensure the Medicare Benefits Program and Pharmaceutical Benefits Program are working effectively.

The Rules contain significant privacy safeguards which apply to all agencies handling claims information and ensure that sensitive health information is subject to robust protections. These safeguards operate on top of protections under the Privacy Act which also apply to claims information. A breach of the Rules is enforceable by the Information Commissioner as an interference with privacy for the purposes of the Privacy Act. These safeguards ensure that the limitation on the right to privacy is reasonable, necessary and proportionate.