AIDH Submission | National Health (Privacy) Rules 2018 review

Background

Submission details

Submitted via email to privacy.rules@oaic.gov.au by Heather Hunt, Corporate Communications Director. Any enquiries arising from this submission should be directed to Heather Hunt.

Members of the Australasian Institute of Digital Health who contributed to this were:

- Dr Greg Adamson FAIDH MCommrclLaw, Chief Risk and Security Officer Medikey Australia
- Dr Densearn Seo, CHIA MBBS, Medical Director at Drop Bio, Royal Australasian College of Physicians Trainee and Honorary Researcher, Cabrini Health & Cabrini Institute
- Richard Rendell, Managing Director, Applied Precision Medicine

The consultation paper for this review can be found on the OAIC website.

Summary

Personal health data, including MBS and PBS data, is the subject of significant privacy protection, including in the *National Health Act 1953*, which in Section 135AA requires the issuing of rules as a privacy function. Since the last major review of the Rules we have seen a significant shift in the ability of technology to de-anonymise data, and researchers now generally agree that per-record anonymisation is not achievable. Therefore, other privacy measures, such as avoiding large data set aggregation as described in the separation of MBS and PBS data, has increased importance.

In addition to recommending the reasserting and strengthening of privacy provisions provided in Rules, this submission proposes that the Rules should consider whether new types of health data, particularly genomic data, require special consideration.

While there are many reviews and possible changes to the privacy and data policy environments in Australia today, the submission recommends that any change to the requirement for the Rules should take place in a review of the National Health Act 1953, and that the purpose of the Rules should remain consistent with the Act, rather than seek to modify the intention of the Act.

Key questions for this review

This review is aimed at understanding how the rules are currently operating, whether their provisions remain fit-for-purpose and what revision or updates may be needed.

1. What provisions in the rules work well and should remain as they are or with minimal changes?

We believe that the provisions should all remain but require (minor-major) edits as will be detailed further in this submission. This will ensure that privacy is maintained and where possible, more specified to be more inclusive.

2. What provisions in the rules are no longer fit for purpose? Why?

Understandably the Rules were made to be generic. The Rules are potentially losing relevance and must be reviewed as concerns exist in the following domains:
Data governance: Existence of a relevant and tailored framework in the data ecosystem
Inclusion of genomic (and other biometric) data
Prescribed circumstances to be detailed further
Protection of consumer data rights (i.e. autonomy, privacy/anonymity)
Application and implementation in industry and research setting
Technical standards for linkage/data-matching
Regulating and re-linking 'old information' especially with identifiable components
Considerations for future
Clarity regarding compliance of standards within the Rules

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?

The balance could exist but it is still currently rather murky. There needs to be better transparency to support the Australian Privacy Principles (APP). We believe that in order to achieve a balance, a step-wise approach is necessary, beginning with building confidence amongst all stakeholders that privacy is protected, then ensuring efficient data governance structure/policies exist in regards to data linkage.

Form and function of the rules

Prescriptive versus principles-based

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. A prescriptive approach can have the positive effect of eliminating known privacy risks that would otherwise confront an officer 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.

4. Which provisions in the Rules are too prescriptive / not prescriptive enough?

The major technology change since the Rules were issued in 2018 is the increased capacity to link data which was previously considered to be anonymised, in order to de-anonymise it. It is now widely accepted that per-record anonymisation is not possible. Therefore, any assumption that this is possible should be made more prescriptive. For example, 13(5) states that "Claims information may be held indefinitely for policy and research purposes by the Department of Health provided that such claims information does not include person identification components." Given the current capacity to link, this would need to be extended, eg, "that such claims information does not include any components related to individuals."

5. Would any parts of the Rules benefit from being made more principles-based? Why?

Potential areas for inclusion of the underlying principle are:

The term "database" throughout the Rules could benefit from examination of the underlying legislation. In 135AA of the National Health Act 1953, "database means a discrete body of information stored by means of a computer". The concept of a "discrete body of information" provides a more nuanced summary of the goal of the Act than the term "database".
The reference in 15(1) to "Paper copies" is anachronistic. Rather than update this to current technology, a replacement by "working copies" would preserve the principle that the need for temporary working copies of information should not be used to undermine the privacy principle incorporated in the Rules.

Technological specificity versus technological neutrality

A side-effect of more prescriptive regulations is that they may struggle to accommodate rapidly changing information technology. In the context of these Rules, this can have two effects:

- The Rules contain requirements that have been overtaken by changes to technology and are therefore difficult to apply in practice or require inefficient workarounds to enable compliance.
- The Rules obstruct or limit reasonable use cases for claims information that have been enabled by changes to technology and digitisation of government operations.

While the Rules minimise the use of technologically specific language, there are some provisions where this is unavoidable. For example, the National Health Act says that the Rules must prohibit the storage of MBS and PBS information in the same 'database.' Therefore, the Rules refer to separation of 'databases'. Other provisions, while not necessarily being technologically specific, impose requirements that may operate counter to modern data practices. For example, very short retention times for linked claims information may make use of the information difficult or discourage legitimate linkage activities.

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?

We suggest firstly keeping first principles in mind. The purpose of the Rules is to govern and protect privacy. That requirement needs to be met in a rapidly changing and fluid environment of technological progress and in turn data management practices. Some technologies have higher risk associated with their use (including for privacy) while at the same time may offer valuable insights and benefits to society. For example, the power of AI and Machine learning has delivered many benefits across society but can also cause harm through unintended consequences and misunderstanding of the full semantics of the data used to train models. Privacy may be broken rapidly and unintentionally. It is difficult and potentially remiss to abstract the use of powerful technologies from the Rules and be confident that the evolving worst case risks to privacy are being mitigated. It suggests that the Rules be more fluid and subject to more regular updates more towards a living document rather than what is apparently a set and forget approach. It would be useful for the OAIC to develop its positions on the uses of new technologies with respect to privacy and in particular AI/ML. We note that the Human Rights Commission has produced technical papers on Ethical AI. In turn this raises the question as to whether the OAIC is appropriately funded to effectively carry out the first principles mandate of protecting privacy in the modern age.

7. Which parts of the rules are no longer fit for purpose due to technological change or need adjustment?

Simply referring to 'databases' and data separation is no longer fit for purpose. The rules should provide guidance on various technologies starting with those that have the highest potential impact on privacy risk, while meeting the needs of the agencies requiring data access. Again, this requires effort and funding of the OAIC to deliver more effective rules.

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 and 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. 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. For example, the Rules contain strict disposal provisions for claims information (particularly linked claims information). This made sense prior to the introduction of the APPs because the earlier IPPs did not contain any information disposal requirements so the Rules filled a gap. However, that changed with the APPs which now impose data disposal requirements. Therefore, a question arises as to whether certain APPs should 'cover the field' for health information (including MBS and PBS information) or whether the nature of MBS and PBS information demands additional controls set down in the Rules.

8. What additional requirements should apply to MBS and PBS information over and above the APPs? Why?

While the APPs as a set of *principles* consider health data in some detail, the specific privacy threat related to aggregation of data is an instance, which requires specific consideration.

9. Which provisions in the rules (if any) should be removed or adjusted in light of the APPs?

The APPs provide additional consideration of genomic data, which may also require specific consideration in the Rules. It would be premature to remove protections designated in Act unless the Act itself is modified in light of the APPs. The field of protection of health data is highly nuanced, and the risk of losing an existing privacy-preserving control should not be contemplated lightly.

The rules in practice

Modernisation and trends in government information policy

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.
For example, 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'.
Recent developments outlined above illustrate opportunities for alignment of the Rules with new currents in government information policy.

10. How can the rules be modernised or made more effective, while remaining within the parameters of the primary legislation?

The purpose of the Rules is guided by the intent of the Act: 135AA(3A) states "The issuing of rules under this section is a privacy function for the purposes of the Australian Information Commissioner Act 2010." It would

therefore be inappropriate to use the Rules as a mechanism for undermining the privacy protecting principles of the Act, for example in order to facilitate the creation of privacy-undermining practices in the health data industry.

11. How might the rules better align with current government policies pertaining to information use, re-use and sharing while still protecting privacy?

The principles of Consumer Data Rights legislation regarding the availability of data to an individual "for use as they see fit" is not reflected in the Rules (Competition and Consumer Act 2010, 56AA(a)(i)). The ability for individuals to hold their personal health data and share it requires appropriate safeguards, but the approach is consistent with the Act. For example, Australian Immunisation Register records while available to individuals don't allow the individual to display a single record (eg evidence of a COVID-19 vaccination), as all past vaccinations are displayed in one list.

Specific questions about the Rules

Storing claims information in separate databases

What the Rules say

The Rules require agencies to store MBS claims information in a separate database to PBS claims information. The National Health Act itself requires the Rules to prohibit storage of this information in the same database and the Information Commissioner has no discretion to alter or moderate this requirement. 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.'

The requirement to store data in 'separate databases' may no longer be meaningful in the current digital environment. However, until the National Health Act is changed, this requirement will have to remain a feature of the Rules.

Management of claims information by Services Australia

What the Rules say

The Rules specify how Services Australia must manage claims information. This includes requirements 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.

The Rules ensure that claims information in the MBS and PBS databases is stripped of personal identification components, such as name and address information, apart from a Medicare card number, or a pharmaceutical entitlements number.

These requirements apply to claims information that is not 'old information'. Information that is more than five years old is considered 'old information', and this information must not be stored with any personal identification components at all, including the Medicare card number or the Pharmaceutical entitlements number.

The effect of these requirements is to lessen the privacy impact of these databases and reduce privacy risks. This could include risks that the claims information is inappropriately accessed or disclosed, or risks of function creep such as where claims information is used for unintended or unauthorised secondary uses.

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?

We believe this separation does not need to be changed. Modern interoperability between database and information technologies is capable of providing integrations for data-sources. Merging MBS & PBS information into a 'single' database should not be necessary for the enabling of analysis or 'digital economy' reasons. Amalgamation of databases increases risk for unintended uses of the combined data especially with the growth of new data analysis technologies that will depend on the availability of the merged information. It is worth noting that in a monolithic database system it is difficult, expensive, and time-consuming to affect remedial activities should adverse privacy events occur. This also becomes a single point of failure from a systems and privacy standpoint.

Requirement for Services Australia to maintain technical standards

What the Rules say

The Rules require Services Australia to establish and maintain detailed technical standards in relation to the MBS claims database and PBS claims database which cover matters including:

- Access controls
- Security measures, including measures to prevent unauthorised linkages
- Measures to enable tracing of authorised linkages
- Destruction schedules for authorised linkages.

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. If Services Australia changes the standards, it must inform the OAIC.

Services Australia is subject to other security obligations in relation to MBS and PBS claims information. These include information security requirements under APP 11 in the Privacy Act, the Australian Government's Protective Security Policy Framework, and the Information Security Manual. This could raise a question as to whether dedicated technical standards for MBS and PBS information is necessary in view of those other security obligations. On the other hand, dedicated technical standards enable more specific requirements particularly in managing data linkage and safeguarding the data from unauthorised linking.

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?

Yes.

It must be noted that Services Australia covers a broad range of services, and these include personal and sensitive information which are ultimately identifiable. The notion of having further linkage, especially without detailed technical standards would not be reasonable even with the current information security requirements. For example, the Privacy Policy statement on the Services Australia site (https://www.servicesaustralia.gov.au/organisations/about-us/corporate-publications-and-resources/privacy-policy) clearly states that personal information is collected via engagements done through social networking services. This is potentially a (backdoor) channel of concern.

MBS and PBS are separate entities and as such have separate database to begin with. We would like to emphasise that we do not believe that it is necessary to merge MBS and PBS into a single database. First principles prior to any data linkage program would lean towards preparing and developing detailed technical standards for both databases. The standards should be developed in consultation with both agencies. Inclusion and exclusion criterion which includes considerations for future technological advancements is not only crucial but is also practical. Furthermore, OAIC considers that best practice is to have clearly expressed and detailed

technical standards, which are in keeping with the *Improving the Integrity of Identity Data: Data Matching Better Practice Guidelines*. If done well, it is highly possible that in the future, it could be matched into a single technical standards guideline/report.
The above comments would be in keeping with the requirements under APP, especially APP 11 in upholding the security of personal information.

14. Should the technical standards cover any other matters?

Apart from the standard framework, the standards must include (to name a few):

- More clarity on the nature of the *prescribed purposes* and its limitations
- The intended data matching and analytics that will be undertaken with linked data
- Clear statement(s) on how claims information would be managed or integrated if linkage is to be made further to agencies like ATO or Centrelink via Services Australia
- Third party information and specific clause about data gained from social networking services given the rise in usage and engagement with the public via these channels
- Data storage and (hierarchy of) authorised access including tracing, duration and "destruction schedules" [Data Governance]
- For future purposes: what constitutes a change in the agreed standards and processes for agencies to inform OAIC
- Public accountability: a public record of each linkage including agencies, purpose of linkage, data that was linked – for example a table on a web site.

15. Should any other agencies be required to have technical standards of this sort? Which agencies and why?

Unable to ascertain further at the moment. However, the comments above should pave way for having detailed technical standards as part of the framework for any agencies who are considering or being considered for data linkage (with Services Australia) in the future.

Medicare PINs

What the Rules say
The Rules 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.

The Rules contain provisions on the creation of a Medicare PIN that is unique for each individual, and the purposes for which a Medicare PIN may be used or disclosed. 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. That said, Services Australia may disclose Medicare PINs in some circumstances, though usually not with the individual's name.

16. Are the provisions regulating the creation, use and disclosure of Medicare PINs fit for purpose?

No. This is largely because of the multiple unknowns that exist. Responses in Q13 and Q14 will also be relevant here. Some of the concerns and known unknowns are:

- What is not covered in these *prescribed* purposes/circumstances for disclosure?
- Detailed data governance framework for each participating agency
- Future agencies participating in data matching with Services Australia and the detailed safeguard measures currently in place. Therefore, the rules regarding provisions of Medicare PINs should include current agencies only and the clause must be reviewed regularly at a stipulated time frame and pre-determined clauses in reference to change(s) in technical standards or agency agreements.

For these reasons, the list of exclusions in s8(8) of the rules should be expanded.

17. Should there be more permissive or more restrictive use of Medicare PINs? Why?

There is a fine balance but leaning more towards restrictive - refer to Q16. This would ensure integrity and upholding of APP principles as Australia works towards a more secure and seamless data governance structure.

Disclosure to the Department of Health

What the Rules say

The Rules allow Services Australia to disclose claims information to the Department of Health to enable Medicare to perform 'health provider compliance functions.'

Services Australia may disclose claims information to the Department of Health in other circumstances but generally such information must not include personal identification components – though Medicare PINs and encrypted Medicare card numbers are able to be shared.

If lawfully sharing claims information with an agency, organisation or individual other than the Department of Health, Services Australia must not provide both the Medicare PIN and name unless a law requires specifically requires it.

The disclosure provisions in the Rules mostly relate to how Services Australia and the Department of Health interact to enable the Department of Health to carry out delegated Medicare functions and activities. For example, the Department of Health monitors health providers and makes sure they are doing the right thing when they claim MBS and PBS benefits on behalf of their patients or customers. To carry out this function and take enforcement action, the Department of Health needs to collect and use claims information.

Disclosure of claims information to other entities other than the Department of Health must be 'lawful'. This means that it must not be prohibited by another law and, if the information includes personal information, would need to comply with APP 6.

A later section of the Rules enables disclosure of claims information for medical research.

18. Do disclosure provisions get the balance right between data sharing and protection of privacy? Why or why not?

At present the balance is not well made, as individual records can be de-anonymised. This was not feasible in 2008 when the last major revision of the Rules took place. To address this technology development, any sharing for purposes that don't relate to an individual should be undertaken using appropriately reviewed data aggregation or data obfuscation processes.

19. Is APP 6 adequate for regulating disclosure of claims information? What additional requirements, if any, need to be spelt out in the Rules?

APP 6 considers data reuse for purposes other than for which it was collected. This is considered in the Act, 135AA(5)(b), which requires the rules to "specify the uses to which agencies may put information". In that sense the two are aligned. However, the Rules have a further function, to enforce a separation of databases to address the potential threat to privacy through data aggregation. This is beyond APP 6 and requires specific consideration in the Rules.

Linkage of claims information

What the Rules say

The Rules allow Services Australia and the Department of Health to link claims information held in the MBS and PBS databases but only in prescribed circumstances. These include where the linkage is:

- necessary to enforce a law
- required by law
- for the protection of the public revenue

- 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 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.

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?

This would have been covered to some detail in Q13-15. We agree that data-matching is essential for monitoring claims, excessive services, over-prescribing and enables better research and statistical/modelling measures. However, before determining other circumstances, the prescribed circumstances such as 'protection of public revenue' and 'determining individual's eligibility for benefits' could be better delineated here bearing in mind that no two individuals are similar despite having some similarity in claims data. What are the discriminatory factors used? Where possible, trigger factors and clause for data-matching in prescribed circumstances should also be specified. Usage for medical research will be covered in detail in Q25.

Having more clarity in the prescribed circumstances that allow linkage of claims information should be the first step. It would be worthwhile understanding how linkage of claims information in MBS and PBS databases in a de-identified manner will be utilised alongside specific circumstances for inclusion of Medicare PIN (identifiable information).

Lastly, will there be:

- Clause for future integration with new(er) agencies within Services Australia and Department of Health?
- A waiver system for high claims consumers such as those affected by genetic disorders or chronic diseases (who naturally have higher claims over time – for example in relation to medical research purposes), in order to avoid them being the repeated subject of investigation. Transparency in relation to the degree of consumer autonomy might be worthwhile.

Retention and reporting of linked claims information

What the Rules say

The Rules say that Services Australia and the Department of Health must destroy linked claims information as soon as practicable after meeting the purpose for which it was linked. They must also make special arrangements for the security of records of linked claims information.

Services Australia and the Department of Health 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.

The destruction requirements in the Rules act as a form of protection against function creep and unauthorised secondary use or disclosure of linked claims information. However, the strictness of the destruction requirements may reduce the utility of data linkage and curtail use of the linked information for reasonable and lawful purposes. Data linkage conducted in conjunction with other programs – for example, by the ABS for the Multi-Agency Data Integration Project (MADIP) – is not subject to the same strict destruction requirements.

21. Are the data retention requirements appropriate? Should linked claims information be able to be retained for longer?

Once linkages have been destroyed, what prevents Services Australia or the Department of Health from holding a copy of the linked data? To minimise the potential for privacy breaches and unauthorised secondary use, we do not believe that linked claims information should be retained for longer.

22. Are reporting arrangements appropriate? Should reporting categories be changed in any way?

Linkage reporting should be a matter of public record. Linkage activities including the number of records linked, the purposes of the linkage, number of linked records that were destroyed. Reporting should also include whether the purpose of the linkage was to facilitate the building of AI or Machine Learning models to predict outcomes within health or population contexts. Such reporting should provide an auditable trail for investigation of AI/ML implementations should they demonstrate unethical outcomes once implemented.

Old information

What the Rules say

'Old information' (meaning claims information that is five or more years old) is treated differently under the Rules. It must be stored separately from other claims information and with personal identification components removed. Old information may only be linked with personal identification components in certain circumstances prescribed in the Rules.

As with other forms of linkage, old information linked to personal identification components must be subject to additional security requirements, destroyed as soon as practicable after it has achieved its purpose, and be reported to the OAIC.

The National Health Act states that the Rules must regulate the handling of 'old information'. In particular, they must require old information to be stored without personal identification components and specify the circumstances in which old information may be re-linked with those components. Therefore, the OAIC cannot revise the Rules to change this storage requirement for old information. However, the OAIC can vary the circumstances in which old information may be re-linked.

23. Are the provisions applying to old information appropriate?

One would wonder if the definition of 'old information' should be revisited. Should the retention time be re-defined? Is five years a good cut-off? Health information or medical records are generally stored for seven years from last entry.

The counterargument would be – by extending the duration of storage of data then data governance policies must be reviewed more routinely and revamped where possible to ensure maintenance of security and privacy. However, that is not the true purpose here.

The regulating and handling of 'old information' is part of a continuum in health information management. The Rule states that once data is classified as 'old information' then it must be stored separately from claims information and personal identification components removed. This must be maintained.

The concern would be in reference to the next statement whereby the Rule states that 'old information' may only be linked with personal identification components in certain prescribed circumstances. These circumstances ought to be specified in further detail alongside information on the additional security requirements in these instances, if possible. This would be in keeping with the National Health Act.

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?

The way to ensure appropriate handling of 'old information' is as discussed in Q23 and ultimately by ensuring that they are destroyed completely at the end of the stipulated time frame OR when they have achieved their intended purposes, whichever occurs later. This should include any linkage to potentially identifiable components.

However, the concept of re-linking 'old information' with personal identification components suggests that there is a possibility of data breach even when 'old information' is considered destroyed. Hence, policies and framework surrounding destruction of 'old information' ought to be specified. We do not suggest adding more circumstances at the first instance. It would be ideal to understand the prescribed circumstances in further detail prior to making more recommendations for now/in the future.

Disclosure of claims information for medical research

What the Rules say

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.

These arrangements reflect obligations that would apply under the Privacy Act and related laws regardless. However, the inclusion of this provision relating to medical research is to clarify and provide certainty regarding how claims information may be used for medical research purposes.

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?

This question is actually four questions.

a) Is this provision necessary given it already applies under the Privacy Act?

The provision should remain.

b) If yes, does it need to be modified in any way?

Modification should be considered to ensure that privacy relating to claims data for genomic testing or treatment be heavily reinforced. The emerging MBS support for genetic testing as evidenced for example by MSAC Application 1599 Genomic testing for the diagnosis of heritable cardiomyopathies, supports cascade testing reimbursement from which claims data may potentially enable easier pathways for family clusters to be identified.

c) Should claims data be able to be used for other forms of research?

Claims data has been used elsewhere in the world to inform analyses such as those likely to return or to be readmitted to hospital for given diseases/drugs/circumstances. Physicians may find it valuable to know which patient types are predicted to deteriorate or get better. There are no doubt many more insights that can be found either through or with the addition of claims data to the research models. So yes we should encourage the use of claims data in other forms of research – subject to the nature of the research and the potential of privacy exposures through connection/linkage to other datasets accessible within the research project.

d) If yes should there be any limitation on this use?

A carve-out protection covering the availability and use of data regarding genetic tests and disease treatments should be considered. Linkage to other datasets possibly MyHealth records should be heavily restricted and

possibly covering other databases and registries such as those for rare disease where low numbers may potentially breach privacy.

Use of claims information

What the Rules say

The Rules say that the Department of Health may store claims information indefinitely as long as personal identification components are removed. The Secretary to the Department may authorise other uses of MBS and PBS information but a use involving linkage is subject to certain conditions. For example, the linkage (other than linkage permitted in other parts of the Rules) using the Medicare PIN may only occur where:

- claims information (identified by the PIN or any personal identification components) is used solely as a necessary intermediate step to obtain aggregate or de-identified information; and
- such linked records are destroyed within one month of their creation.
- The Department of Health may only disclose claims information if the recipient cannot identify the subjects of the information (unless an exception in the Rules applies).

The Rules enable linkage by the Department of Health but only in a temporary manner with a short retention period. Moreover, MBS and PBS claims information may only be linked in this temporary manner in conjunction with the Medicare PIN where there is no practical alternative.

26. Should the Department of Health be able to link claims information in a wider range of circumstances? What circumstances?

It is reasonable to assume that requests for linkage of MBS and PBS claims data will increase especially given there is growing adoption of complex downstream analytic and predictive technologies especially AI and Machine Learning, leading to new and valuable insights of benefit to patients and populations which are desirable circumstances. We note that use of these technologies as tools to inform future government policy using the PBS and/or MBS data should give consideration to unintended consequences which can occur for certain ethnic, population, disease or treatment cohorts. Inherent biases in claims data should also be considered for the same reasons and potential marginalisation of specific groups.

27. Are provisions enabling disclosure of claims information by the Department of Health appropriate?

Additional specific focus and potentially a carve-out set of rules protecting any information relating to genetic testing or genetic treatments (likely in future) should be considered.

Name linkage

What the Rules say

The Department of Health may obtain the personal identification components that belong to a particular Medicare PIN from Services Australia where it is authorised by the Secretary of the Department of Health and is necessary:

- 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 or
- 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.

There are circumstances in which it may be necessary for the Department of Health to have access to identified claims information. The Rules enable this and set restrictions on how this may occur.

28. Are name linkage provisions appropriate? Should name linkage be allowed in any other circumstances?
No, they are not sufficient, as they are based on the assumption that separation is achieved through removal of explicit identifiers. As previous described, there is now general agreement among researchers that per record anonymisation is not possible. Therefore, the name linkage provisions should be restricted to those circumstances in which a legitimate and approved requirement exists, and in other circumstances additional controls to achieve anonymisation, such as appropriate aggregation, should be applied.

Other matters including management of paper copies

What the Rules say
The Rules say that while paper copies of information may be made of MBS and PBS information, paper copies may not be made of the complete or a major proportion of either the MBS or the PBS claims databases. Services Australia and the Department of Health must make staff aware of the need to protect privacy in relation to claims information. They must also tell the OAIC of what delegations and authorisations they have in place under the Rules.

29. Are provisions relating to paper copies of claims information appropriate? Why or why not?
Given the Australian government goal to eliminate many categories of paper records in health by 2022, as currently described this is an anachronism. However, the principle involved, that temporary copies of records "must not be made the purpose of circumventing the requirements of this instrument", can be achieved by renaming "paper copies" to "working copies".