**Introduction**

The Health Information Management Association of Australia (HIMAA) has had over 70 years strong association with the protection of health information and data. We are invested in the protection of privacy and confidentiality of all forms of sensitive information.

We are a member-based organisation that includes qualified Health Information Managers’ and other associated qualifications in this area. Our members are the data custodians of health information in their respective areas. We feel that we are well placed to be consulted on matters such as the review of the National Health (Privacy) Rules 2018 proposed by the OAIC and present our collective thoughts in this paper.

**General Feedback**

When reviewing this consultation paper, we also considered the question- ‘Does there need to be consideration for any impacts or relationship to the My Health Record (or My *Health Record Act*)?’ The My Health Record contains an individual’s MBS and PBS information.  The My Health Record has been one of the changing technologies with the Australian e-gov model and supporting health care. This has not been discussed in detail however we feel it is an important inclusion in any future privacy reviews.

1. **What provisions in the Rules are no longer fit for purpose? Why?**

Separate storage of MBS/PBS claims data –is an inefficient privacy practice that impedes claims process and visibility of entitlements. Improved efficiency for claims, research and planning if they are stored in one place, and privacy adherence can be realised by new technological advancements.

The prohibition on co-located MBS/PBS data is outmoded:

* inhibits the streamlining of data collection, and
* increases the effort of data linkage for the uses allowed under the rules
* decreases ability to leverage data for secondary and tertiary uses
* compromises the principle of reusable data collections

1. **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?**

Most of the rules do get the balance right between privacy and use claims information in that the technical specifications clearly describe access, the provisions for use have clearly defined boundaries and conditions for de-identification and identification.

Exceptions:

* The use of identifiable claims information for medical research purposes. It is advised that there be additional prescriptive rules around satisfying that “the individual to who the information relates has given their informed consent to the use of that information in the research project”.
* The restriction of the use of claims information to enable the Chief Executive Medicare to perform provider compliance functions in accordance with these rules. Expanding the use of claims information to inform clinical research and inform future funding of health care is

essential. Expanded use of claims data can be used to identify patient cohorts with similar interventions and medications, and to track their outcomes or inform risk profiling for readmission. Similarly expanding use to inform research in future funding of health care will enable better identification of all initial and ongoing costs for care bundling and programs such NDIS.

1. **Which provisions in the Rules are too prescriptive / not prescriptive enough? – see table below**
2. **Which Rules would benefit from being more principles based? Why? – see table below**

|  |  |  |  |
| --- | --- | --- | --- |
| Too Prescription or Not prescriptive Enough | Rule | Why | Benefits of being more principles based |
| Too Prescriptive | 7 (1) Handling of claims information claims information obtained under the MBS must be stored in a separate data base to claims information stored obtained under the PBS | * + - * No clear benefit to privacy       * Confusing for patients and providers       * Obstructs reasonable use of data for claims processing       * Technological advances in data storage, linkage, identification and encryption presents an opportunity to keep data safer and therefore removes the need prevent co-location of MBS and PBS data       * The prescriptive rules around storage inhibit efficiency and may result in claims delays and poor data for research       * rules inhibit interoperability       * rules increase burden of administrative and data management       * Medicare numbers are stored on both MBS/PBS databases .As data in both of these databases informs claims management and uses the Medicare number for linkage it makes sense to have them stored together.       * The rule appears to be obstructive in terms of Rule 9 Linkage of claims information(c ) | * + - * More principles-based rules for storage of data obtained for PBS/MBS data would improve opportunity for efficiencies in claims management and improve visibility of PBS/MBS usage and thresholds. Improve efficiency of reporting on these.       * Create opportunities for multi-provider management, has implications for bundled care for complex chronic conditions and aged care.       * It is a fair assumption to make that many Australians’ would already expect that this information is held in a centralised, accessible location to support streamlined claims management.       * Improved utility for My Health Record/ My Gov and a patient dashboard for how they are tracking with their MBS/PBS usage.       * Storage in the same system may create an opportunity for greater visibility of patients and their families who are reaching or close to their MBS, PBS thresholds.       * Improved ability to leverage data for equitable care and understanding where/whom resources are being used by |
| Not prescriptive enough | Rule 12 (1 a) the department of human services is satisfied that the individual to whom the information relates has given their informed consent to the use of that information in the research project | * + - * This rule appears to have grey areas in terms how individual informed consent is obtained and recorded       * Some additional points are recommended for method of obtaining informed consent       * In which circumstances would informed consent not be obtained – i.e. deceased persons or       * are there situations where a provider has obtained individual informed consent from the person to share this information and has obtained organisational ethics committee approval to share information through a data sharing platform. | Some of the suggestions regarding prescriptive rules for obtaining consent could work better as in principle rules to cover situations such as deceased patients and where informed consent for research has previously been obtained at a provider level and/or via an ethics committee or data sharing platform |

**Interaction with the APPs (Australian Privacy Principles)**

The rules under 135AA of the National Act apply to public sector agencies such as the Department of Health and Services Australia and must follow these rules.

The Commissioner issues privacy Rules on handling MBS and PBS claims information. The requirements of the rules can change but the matters of the rules cannot change under the section 135AA.

The rules are more prescriptive in contrast to the APPs as a primary legislation and these are maintained to allow officers to deal with information to mitigate privacy risks.

There are aspects in the Rules that are already covered in APPs but there may also be some gaps or rules that have to be adjusted in light of the APPs.

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

**APP 1 Open and transparent management of personal information**

Any entity or government agency has to have a clear and up to date policy about management of personal information. Sufficient information is available on MBS privacy online. This policy is made freely available to consumers and to other organizations.

Rules applicable to other agencies may include additional information in relation to legislative framework and current national information standards. Data governance of digital records, storage, security, retention, and disposal need to be more specifically aimed at agencies using MBS and PBS claims information.

**APP 2 anonymity and pseudonyms**

This matter is an option in relation to disclosure of personal health information.

Claims information concerning sensitive information must be dealt with to maintain the option of not being identified such as the use of government identifiers, pins and other security measures as stated in App 10.

**APP 3 Collection of solicited information**

An entity may be the department of health; government agencies must not collect information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity’s functions or activities. Provisions under the rules are already covered under these APPs. For example, researchers must obtain individual consents and the rules must specify to the researchers of their obligations to use de-identified information and follow retention and disposal under NHMRC guidelines.

The need for sharing or directly linking health information using aged care identifiers for example, to investigate unlawful activities or improve the quality of care is an important step to monitor the aged care systems activities; however, the data sets shared must only be obtained for the necessary function and activities of the government agencies investigating or dealing with the claims.

The rules on sharing and linking sensitive information for government business purposes to offer new kinds of products and services must be clearly prescribed in the rules. Privacy Impact Assessments must be conducted in undertaking major projects. Information can be de-identified and solicited information must be destroyed only if it's lawful to do so and not necessary.

The emerging digital technology such as the use of cloud computing poses a challenge to government agencies linking data for the benefit of multiple providers. The rules need to be more precise to control the use of data sets that are only related to their functions and activities. The rules must apply to Government agencies such as the Australian Digital Agency that stores and manage My Health Records.

**APP 5 Notification of collection of personal information.**

Currently some stakeholders can access information via My Health record and My Gov website. Notification of Information to consumers automatically may be used pertaining to organizations that would access MBS and PBS claims in relation to their activities online can be included as a requirement in the rules.

**APP 6 Disclosure of personal information**

Disclosure of personal information is permitted if authorised by law or a court tribunal. There is also disclosure for general situation 16A and health reasons 16B. The APPs states that a written note of use or disclosure of personal information is required under sub clause 6.2e.

Situations may arise when using Medicare ID that can identify a person's sensitive information, therefore, in such situations rules for notifying individuals should be added.

**APP 10 Security measures** to avoid loss, misuse, threats of cyberattack of personal information including de identified personal information.

Additional information for layers of security for all agencies in the delivery, distribution and access may include authentication certificates, pins and key security access.

* [APP11](https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information/) Security of personal information provides sufficient guidance and regulation on the disposal of personal information. AP11 also addresses if the information is used in a Commonwealth record and implications for disposal. Therefore, the National Health (Privacy) Rules no longer requires disposal to be addressed separately within the rules.

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

These rules below have the right balance between privacy and use of claims information except those points where noted.

* The technical standards for management of claims information (4) a- f (5) *(except that which pertains to the need to store MBS/PBS in separate databases)*
* Medicare Personal Identification Numbers (6), (7) (8)
* Disclosures (9) (10) (11) (12) (13) (14) (15)
* Linkage for claims - all points all sections *except* (1c)
* Retention and reporting of linked claims information all sections
* Linking old information with personal identification components all sections
* Disclosure of Identifiable claims information for medical research purpose all sections except (1a)
* National Health Privacy (Rules) 13. Use of claims information point 5 discusses the use of claims information for policy and research purposes if the information does not include personal identification components.   But the Rules don’t describe what ‘personal identification components’ are.  Should there be a reference to the Privacy Act definition, or a definition included in these National Health Privacy Rules?

* [APP9](https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-9-app-9-adoption-use-or-disclosure-of-government-related-identifiers/) discusses government related identifiers. The National Health (Privacy) Rules also discuss the Medicare Personal Identification Number. There should be a reference to APP9 due to rules around the adoption, use and disclosure of these identifiers.

**Modernisation and trends in government information policy**

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

* The rules could be modernised to allow for the MBS/PBS claims information to be stored in virtual locations, cloud data hubs appropriately secured – in line with the Secure Cloud strategy. The prohibition on linking claims data to Services Australia could be amended to enable greater transparency of service use by vulnerable or at-risk populations to deliver equitable access to the right number and mix of services for this population.
  + We have the frameworks of the My Health Record and My Gov which allow for data linkage and sharing between providers and agencies as well as providing an important method of improving consumer engagement with their health information. It is important to continue to leverage the frameworks for improving patient engagement in their care, and collecting consistent, linkable data that informs where and why new services are needed, and care delivery in a community setting.
* These rules could remove the rules that were created for the protection of privacy and to prevent fraudulent claims under the online pharmacist reimbursement claim system. As this scheme did not proceed, the amendments to the privacy rules may not be relevant and in fact inhibit the use of the MBS/PBS claims data for legitimate research and data linkage projects that inform future funding and care delivery improvements.
* These rules could be made more effective by clearly describing exceptions to informed consent – such as consent for research obtained at the point of care when patients are admitted.

**Management of claims by Services Australia**

***12. Should these requirements (about separation of claims information from enrolments and entitlements and exclusion of personal identification components) stay the same or be changed? Why?***

Storage of MBS/PBS data in accordance with the Secure Cloud Strategy and the technical provisions with the rules and the Privacy Act protect against inappropriate access, disclosure and unauthorised secondary use such as marketing. The requirements for separation from enrolments and entitlements and exclusion of personal identification should be amended. It is important for the future of bundled care, effective functioning of schemes such as NDIS, improvements to Aged Care delivery and Mental Health care delivery. Amending these requirements will improve service planning, resource allocation and improve our ability to provide care to patients across multiple settings, improve visibility of patient outcomes, the types of services they access, identify risk and factors influencing readmission.

**Technology specificity vs Technology neutrality**

***6.How could the Rules be updated to better accommodate current information technologies and modern data practices in a way that continues to protect privacy?***

Where possible the Rules should remain technology neutral in order to allow the Department of Health and Services Australia to select the best way in which to meet their responsibilities under the Rules. References to specific systems provided by one company or another should be avoided, however references to common key ways of managing information (e.g. database) are okay as there are many different structures or ways of managing a database.

**Requirement for Services Australia to maintain technical standards**

***13. Is having dedicated detailed technical standards for MBS and PBS claims databases necessary given the range of other information security requirements apply to Services Australia?***

* The technical standards are very prescriptive which is both useful for maintaining governance but also restrictive in that changes/adaptations take time.  While there are security requirements documented in other legislation, policies and frameworks they are not to this level of detail. Potentially these technical standards could state these items are minimum requirements. Strict controls do not require approval or relaxing the requirements or changing the intent details requiring the lodgement of a Variation Report as per point 5 in this section of the Rule.

***14. Should the technical standards cover any other matters?***

Not evident at this stage.

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

It is not clear why the Services Australia require these standards but not the Department of Health.

**Medicare PINS**

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

Current regulatory provisions are still relevant to everyday practical use of Medicare PINs. That said, with the increasing use of electronic healthcare records across Australia. There is the need to ensure the integrity and uniqueness of the PIN is protected and maintained.

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

There should not be additional permissive use of Medicare PINs to protect patient confidentiality and identity theft. Where there is the need to increase permissive use of the Medicare PIN, this should be backed and enforced by law. It is also important to keep a history of the access and release of Medicare PINs as part of the custodianship of Medicare PINs.Could there be an example or explanation of ‘in some circumstances’ that Services Australia may disclose Medicare PINS?

**Disclosure to the Department of Health**

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

Disclosure provisions seem to be quite rigorous in relation to data sharing, however this is dependent on the type of data sharing that is undertaken. Considering the 2016 MBS/PBS data breach (OAIC 2018) it is right to be very protective, but at what cost to agencies or entities seeking information? Would the restrictions limit further investigations into identity/claiming fraud or overclaiming of prescription drugs for example? Would the further restriction on release of linked data limit research capability?

It is difficult to see whether the disclosure provisions get the balance right without running some test cases or analysis on ‘what if’ scenarios. Further review of the provisions needs to occur before we can confidently comment on this section.

1. ***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 appears to be adequate for regulating disclosure of claims information in several ways. Additional requirements that could be reviewed or spelt out, include the addition of greater consent or open disclosure if claims information is disclosed.

**Linkage of Claims Information**

1. ***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?***

Linkage of MBS and PBS claims information should be available for several other uses, including research. Linkage of data is very useful for research purposes, however as this data may be re-identifiable it is very important to separate identifiable information (addresses etc) from the clinical data prior to being linked. Having a data steward role or custodian of data would ensure that this information is managed appropriately. Have a clear set of mandated guidelines prior to any information release. There are technologies that generate non-reversible linkage signatures, meaning that there is no chance of identifiable information (RACGP 2017). Health Information Managers have a very good understanding of data protection requirements and should be considered as a major player in developing data custodian requirements and protecting patient data. Further consultation needs to continue in this area.

Of note, Western Australia has a well-developed data linkage department that links many different sensitive databases. Further information is available here: [Home - Data Linkage WA (datalinkage-wa.org.au)](https://www.datalinkage-wa.org.au/#:~:text=Enabling%20Health%20%26%20Medical%20Research%20in%20Western%20Australia,research%2C%20develop%20policies%2C%20plan%20services%20and%20evaluate%20services.).

Further education on the potential use of health information and data needs to be provided to the public, particularly in relation to what it means to have de-identified data linked and used. Strict rules related to potentially identifiable óutliers’ need to be in place prior to the release of any linked information.

**Old information**

***23. Are the provisions applying to old information appropriate?***

Yes

***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 Rules discuss if this information can be relinked for investigation or prosecution. Does a Royal Commission, or a legal class action fit within this definition? Or investigation or prosecution related to an individual prescriber/patient?

**Disclosure of claims information for medical research**

1. ***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?***

Yes, this provision should remain a part of the Rules to provide clarity and reduce confusion around the how claims information may be used. Keeping this provision within the Rules will make clear to new users or readers of the Rules for what uses they can obtain data for.

Identifying data should always be obfuscated to maintain confidentiality of the patient. To achieve this, it may be necessary to have a function with the data linkage unit to obfuscate research data and release this to researchers. Otherwise the data should remain as close to possible as its original state.

Use of claims information should not be limited to medical research. Accessing claims information could be used to review systems, processes and functions for opportunities for improvement. The same principles should be applied to maintain patient confidentiality.

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

The Department of Health should be able to link claims information in a wider range of circumstances. The circumstances could be related to the development of a very good evidenced-based dataset that could allow researchers to more appropriately examine the burden of disease, review social impacts in all aspects of community life across Australia and review specific health interventions (Research Australia, 2015).

Again, there needs to be rigorous management of the control in the release of information. Ethical standards need to be applied in a greater manner to all aspects of data release, and there should be a greater collaboration with ethical entities being involved, as well as data custodians.

The bioethical principle of nonmaleficence needs to be applied. In circumstances where it is not it can cause potential harm to a patient if information is disclosed in some way through mismanagement of linked health information or other personal information. We need to remember that the data refers to human experiences and should be treated with respect and dignity. Ethical principles need to feature more prominently in the Act.

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

It is difficult to comment on this question without being aware of test cases or attempts to disclose information.

**Name Linkage**

1. ***Are name linkage provisions appropriate? Should name linkage be allowed in any other circumstances?***

If they are released under the guidance of law, this linkage can continue to occur. It is crucial to add Emergency or disaster situations to the condition of name linkage. This will allow the easy identification of patients under these scenarios.

**Other matters including management of paper copies.**

29. Yes appropriate, paper copies are high risk for breaches.

**Authors**

**Sharon Campbell (WA)**

Health Information Manager/Claims Specialist

**Dreda Heard (VIC)**

Health Information Manager/CDS

**Meleah Herbert (QLD)**

Health Information Manager

**Trixie Kemp (TAS)**

Health Information Manager

**Dwayne Richards (VIC)**

Health Information Manager/IT Product Manager

**Elijah Mahama**

Health Information Specialist

**Wendel Tolete (QLD)**

Senior Clinical Coder

Reviewers

**Melissa Clowes (VIC)**

Health Information Manager

**Nadine Ghassibe (NSW)**

Health Information Manager

**Kirstie Mountain (TAS)**

Health Information Manager/Client Record Adviser

**Glenda Wyatt (VIC)**

Health Information Manager

**References**

RACGP., 2017. Data Linkage. Research Article. Available at: [RACGP - Data linkage](https://www.racgp.org.au/afp/2017/august/data-linkage/#:~:text=The%20first%20studies%20to%20link%20MBS%20and%20PBS,data%20linkage%20%28ie%20linking%20federal-held%20and%20state-held%20datasets%29.)

Research Australia., 2015. Improving access to and linkage between health data sets held by Commonwealth entities. Available at: <https://researchaustralia.org/wp-content/uploads/2015/11/Health-Data-Linkage-and-Access.pdf>