

4 June 2021

Ms Angeline Falk
Australian Information Commissioner
Office of the Australian Information Commissioner
GPO Box 5218

Consultation on National Health Privacy Rules 2018 Review

Dear Ms Falk,

NPS MedicineWise is an independent, not-for-profit, evidence-based and consumer-centred organisation, working to improve the way health technologies, medicines and medical tests are prescribed and used.

NPS MedicineWise welcomes the opportunity to comment on the Consultation on the National Health Privacy Rules (Rules) 2018 Review. The Review is a necessary step towards unlocking the potential of the Medicare Benefits Schedule (MBS) and Pharmaceutical Benefits Schedule (PBS) claims information, and its use for medical research purposes which serve the public good.

Disclosure of claims information for medical research

The current Rules permit disclosure of claims information to researchers for the purpose of medical research in certain circumstances. They include provisions for when claims information identifies an individual. The relevant provisions state that such information 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.

NPS MedicineWise is of the view these provisions are unnecessary as the position is governed appropriately under the Privacy Act 1988. To avoid duplication and inefficiency in data release decision-making, a clearer delineation of the roles and responsibilities of Human Research Ethics Committees (HRECs) and data custodians is required¹. Unfortunately, the Rules do not provide delineation of this authority, and in their current form appear to offer little meaningful basis (beyond referencing the existing ethical requirements under s95 of the Privacy Act) upon which the Commonwealth data custodians may base decisions.

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

Yes. NPS MedicineWise is uniquely placed to comment on this issue having deep experience with the Australian health research community through the MedicineInsight program. For background, NPS MedicineWise is the custodian of a large dataset which is collected pursuant to the MedicineInsight Program. MedicineInsight was established by NPS MedicineWise in 2011, with core funding from the Australian Government Department of Health, to support quality improvement in Australian primary care and the post-market surveillance of medicines.

¹ See for example advocacy by the Australian Health Research Community and a [suggested division](#) of HREC and data custodian roles to avoid duplication

In our view the current Rules are incorrectly focused on linkage *between* the MBS and PBS and on circumstances involving *disclosure of personal information* for medical research.

The more pressing regulatory issue is circumstances where de-identified claims information may be linked to de-identified external datasets for medical research. In addition to our direct experience with the Australian health research community, NPS MedicineWise note successive Government Reviews² and Senate Committee Reports³ over the past ten years which describe frustration at the overly cautious, cumbersome, costly and opaque processes which apply to the release of claims information. This is despite MBS and PBS data being the fourth most requested government dataset⁴.

The lack of medical research involving data linkage of claims information further suggests the Rules do not achieve the policy intent of section 135AA of the National Health Act; which is to recognise the sensitivity of health information and restrict the linkage of claims information, *while also allowing* for the use of such information for health policy and medical research purposes in certain circumstances.

Consistency with the Data Availability and Transparency Bill 2020

NPS MedicineWise notes the Commonwealth's proposed Data Access and Transparency Act provides a legislative framework which may override the existing Rules⁵ and the use and disclosure provisions of the Privacy Act 1988 (Cth)⁶. It is recommended the revised Rules provide greater clarity about how these legislative frameworks interact, and how data custodians may act should they be contemplating the disclosure of claims information for medical research.

Should the requirements about separation of claims information from enrolments and entitlements and exclusion of personal identification components remain?

NPS MedicineWise agrees with the Office of the Australian Information Commissioner that the requirement of the Rules to store data in 'separate databases' may no longer be meaningful in the current digital environment⁷. For example, NPS MedicineWise implements privacy preserving linkage methods which provide lower risk solutions for record linkage than the separation requirements of the current Rules. These methods do not require third parties to see personal identifiers and provide more robust privacy protections by engaging in record linkage on encrypted information.

Importantly, these requirements of the Rules have been made redundant in recent years as data access and release principles endorsed by the Commonwealth require data custodians to look beyond 'Safe Storage' as a single criterion⁸. Similarly, data deidentification by simple exclusion of personal information is no longer considered an effective or contemporary method to manage the ongoing risks of reidentification⁹.

² See the [Prime Minister and Cabinet Public Sector Data Management Project](#)

³ See the [Senate Committee Sixth Interim Report \(Big health data: Australia's big potential\)](#)

⁴ See survey results from the [Open Data 500 initiative](#)

⁵ See the [Australian Medical Association submission to the National Data Commissioner](#)

⁶ See [NPS MedicineWise submission to the National Data Commissioner](#)

⁷ See [OAIC consultation paper on the on National Health \(Privacy\) Rules 2018 Review](#)

⁸ See [National Data Commissioner data access and release principles](#)

⁹ See the [CSIRO deidentification decision making framework](#).

NHRMC ethical guidelines thoroughly support the deidentification of data for medical research purposes and NPS MedicineWise accordingly seek advice from properly constituted Human Ethics Research Committees to guide data access use and disclosure decisions for MedicineInsight and PBS data use proposals.

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?

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. However, NPS MedicineWise note that 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 (PSPF), and the Information Security Manual (ISM).

NPS MedicineWise currently receive and securely store PBS claims information for research purposes. This data is stored and processed in an environment hosted within an Australia based Amazon Web Services and iRAP¹⁰ certified cloud offering.

NPS MedicineWise have maintained a productive, and longstanding contractual relationship with Services Australia. As a trusted third-party user of PBS claims data, we are of the view that detailed technical standards for claims data are unnecessary. The Rules in their current form have little bearing on the Secure Storage Security Plan, and NPS MedicineWise's Information Security Policy. Alternatively, our detailed technical frameworks, similar to Services Australia, are guided by the PSPF and ISM. These provide more detailed assurance than the Rules provide in their current form¹¹.

NPS MedicineWise would welcome the opportunity to discuss these views further with the Office of the Australian Information Commissioner.

We thank you for the opportunity to contribute.

Andrew McAlister

**Research Ethics and Data Governance Specialist
NPS MedicineWise**

¹⁰ See <https://aws.amazon.com/compliance/irap/>

¹¹ Key Controls include a multilayered security architecture implementing the Defence in Depth principle. Multifactor authentication is required to gain access to the environment, or to the relevant administrative functions; The environment is separated into multiple network zones, with traffic flow controlled by Security Groups in such way that network communication to/from the components with the most critical information assets are explicitly controlled (white listed). No communications are permitted between zones that are exposed to unauthenticated traffic. Further exfiltration of information requires actions from two segregated roles. Role based access control ensures that users have the least privilege required to perform their duty. Need to principle is applied for all access requests before granting access.