THE LAW SOCIETY
OF NEW SOUTH WALES

Our Ref: PDL:JWap040621

4 June 2021

National Health (Privacy) Rules 2018 review
GPO Box 5218
Sydney NSW 2001

By email: privacy.rules@oaic.gov.au

Dear sir / madam,

National Health (Privacy) Rules 2018 review

Thank you for the opportunity to contribute to a submission on the National Health (Privacy) Rules 2018 (the Rules) review, currently being conducted by the Office of the Australian Information Commissioner (OAIC). The Law Society's Privacy and Data Law Committee has contributed to this submission.

This letter responds to some of the questions posed in the consultation paper for the review.

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

The Law Society notes that Part 3 of the Rules deals with how the Department of Human Services and the Department of Health are required to manage, disclose, link and retain claims information. This Part is significantly more comprehensive than Part 2, which applies to Government Agencies and prescribes that claims information under the Medicare Benefits Schedule (MBS) must be stored in a separate database to claims information obtained under the Pharmaceutical Benefits Schedule (PBS).

We are aware that at least one Government Agency – the Australian Digital Health Agency (ADHA) – now handles MBS and PBS data (noting subsection 135(5AA) of the *National Health Act 1953* (the Act) was inserted to enable the flow of MBS and PBS data to the My Health Record (MHR) system). We consider that if a prescriptive approach to the Rules is maintained, then Part 2 of the Rules should also adopt a more prescriptive approach in relation to the disclosure, linkage, and retention requirements of MBS and PBS information by any Government Agency that deals with such data.

We note the Pharmaceutical Benefits Unit of the NSW Ministry of Health receives, at the least, PBS data, while the Medical Council of NSW also receives such data on request. While conscious the OAIC would not have jurisdiction over those agencies, we query whether there is scope for greater compliance requirements, in the Rules or elsewhere, for State Agencies handling that data.

THE LAW SOCIETY OF NEW SOUTH WALES
170 Phillip Street, Sydney NSW 2000, DX 362 Sydney
ACN 000 000 699 ABN 98 696 304 966
lawsociety.com.au
T +61 2 9926 0333 F +61 2 9231 5809
E lawsociety@lawsociety.com.au
Law Council OF AUSTRALIA
CONSTITUENT BODY

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

The Law Society considers it appropriate that the Rules themselves remain prescriptive, as they provide clarity around the requirements attached to specific datasets. However, we consider the Rules require update and amendment, particularly in relation to data storage requirements, and greater clarity in relation to how data can be tagged, accessed and used by people analysing it.

In our view, overarching 'principles' are better placed in legislation, where they can be overseen by a regulator such as the OAIC who can issue guidance, fact sheets, and suggest reforms.

We therefore support the development of a principles-based framework implemented in legislation, with the associated Rules updated to provide for prescriptive data sharing rights and obligations between agencies.

Question 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?

While the Law Society generally supports the development of technology neutral concepts in primary legislation, we consider that the benefit of subordinate legislation is its ability to be updated relatively easily to reflect changes in technology and practices. We consider that, where possible, the Rules should retain a degree of flexibility, but also be appropriately targeted, to enhance clarity and ensure current best practice processes.

We note the examples provided in the consultation paper focus on the data storage and retention requirements currently contained in the Rules. Without further information, we are not aware of any modern data practice which suggests that MBS and PBS data should not be stored in their own databases. We would welcome advice about whether there are specific considerations behind any suggestion to amend requirements for the separate storage of such data (we note, for example, that the concept of vendor agnostic systems within government to ensure interoperability of technology has been suggested previously). If the suggestion is centred around the language used, we have no in-principle objections to the adoption of a technology neutral term that encompasses a broader range of storage systems.

In relation to the short retention period for linked data, we note that the time taken to achieve the data linkage purpose is not limited by time. We query the necessity of an agency retaining such data after the relevant purpose (i.e. data linkage) has been achieved.

We would support an amendment to the Rules to insert a requirement for agencies to tag data sets better so that personal and sensitive information can be identified, anonymised and then destroyed at an appropriate time.

Questions 8 and 9: What additional requirements should apply to MBS and PBS information over and above the APPs; Which provisions in the Rules (if any) should be removed or adjusted in light of the APPs?

The Law Society considers that the APPs provide limited privacy protections in practice, and there are limited consequences for an agency's failure to comply with relevant requirements. Recognising the sensitivity of the data to which it relates, we note that section 135AA of the Act requires development of Rules over and above the APPs.

We note the Data Availability and Transparency Bill 2020 has been introduced into the Commonwealth Parliament, and query how the interaction between that scheme and the Rules (noting the restrictions contained in section 135AA of the Act) will work in practice.

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

We note that access to MBS and PBS datasets is controlled because of the highly sensitive nature of the information involved. For example, the datasets include information in relation to a person's mental health, or whether they have a sexually transmitted disease or a rare disease. In our view, it is appropriate that access to, and use of, that data is heavily constrained, to ensure public confidence in providing it.

The Law Society recognises that there are benefits to appropriately controlled and safeguarded use and sharing of data, particularly where such use and sharing enables the better delivery of government services and benefits to citizens. However, initiatives that rely on the provision and use of data largely depend on high levels of citizen trust that governments will ensure that uses of data about them are fair, proportionate and consistent with expectations about how that data will be used and shared. This is particularly relevant in the context of the limited role that an affected individual's consent can play in relation to the collection, use and sharing by governments of data about them.

We note that there are currently deficiencies in the existing combination of data privacy laws and administrative law remedies, both in NSW and Commonwealth legislation, in relation to potential outcomes enabled by data outputs from data sharing. Many forms of data sharing (such as through data linkage of disparate data sets using a pseudonymised transactor key) are not closely regulated by data privacy law, yet may still enable the creation of outputs that can be used to impose individuated (differentiated) outcomes upon individuals or small cohorts of individuals. That outcome might be any of the denial of offer of a service, a different price for a service, withdrawal of a service, a demand for payment or reimbursement, an investigation or enforcement action.

In this context, we remain concerned about the lack of control over such algorithmic individuation, and the absence of appropriate legislative regulation of algorithmic individuation. We are also concerned about the absence of legislative requirements to ensure that inferences made by Government Agencies using data about individual citizens are fair and reasonable.

Further, we note there are ongoing issues with the way in which government agencies handle sensitive data, at both the Commonwealth and State level. We are concerned that government agencies have not necessarily demonstrated that they are model data custodians. Noting the increased risks associated with expanded sharing and use, we consider careful consideration should be given to enabling a broader category of agencies to handle such data.

Question 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?

The Law Society supports mechanisms to ensure that PBS and MBS data is devoid of identifying information.

If there is a need for an agency to know whether a person is entitled to a benefit, we support the development of a system similar to the NSW Digital Driving Licence system, which could

simply indicate whether or not someone is so entitled without giving agencies access to unnecessary additional information.

Questions 13/14/15: 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? Should the technical standards cover any other matters? Should any other agencies be required to have technical standards of this sort? Which agencies and why?

As indicated above, the Law Society considers that all agencies that receive this data should be accredited and required to comply with clear rules. In our view, agencies should be required to adhere to stringent technical standards and to be competent in data security and management.

The Law Society has supported a statutory cause of action in relation to serious breaches of privacy. While beyond the scope of this consultation, we consider that, at the least, clear standards should be applied to all agencies with access to this data, and consideration should be given to attaching penalties for a breach of those standards, with independent oversight by the OAIC to monitor compliance.

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

The Law Society considers that data minimisation and purpose limitation are important principles. As currently drafted, we consider the Rules have been effective in establishing prescriptive measures that restrict the use of claims information. Ensuring information is not disclosed for purposes other than those for which it was collected has enhanced confidence in the system.

We consider that this is an aspect of the Rules that is not sufficiently replicated in APP 6. In our view, the disclosure of claims information more broadly than to the agencies that oversee the system devised for public healthcare and payments would expose data to additional risks, including of misuse, and would be beyond the purpose for which it was collected.

Question 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?

As outlined above, the Law Society considers that until the outcomes enabled by data outputs from data sharing, including data linkage, are better regulated, such activity should be constrained and not further expanded without a clear purpose for further linkage. This is particularly relevant in the case of MBS and PBS data, which is highly sensitive and from which many conclusions can be drawn.

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

The Law Society considers that normal retention principles should apply (see for example, APP 11.3), particularly noting the sensitive nature of the data involved.

As outlined above, we query the necessity of retaining linked claims data once the purpose for which it was retained has been achieved.

Question 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?

The Law Society is strongly in favour of limiting the use of claims information, particularly for identified data. In our view, the Rules do not go far enough in controlling such use, or in prescribing appropriate oversight mechanisms or disincentives for data misuse.

As outlined above, the Law Society suggests there should be clear requirements attached to how such data may be stored, used and destroyed by all government agencies. There should also be consequences for failing to adhere to these standards and disciplinary repercussions for breaching those standards.

We note that the data contained in those datasets include information pertaining to all Australians, including Indigenous Australians. We consider careful consideration should be given to developing a mechanism to consider Indigenous Data Sovereignty principles when considering research applications for access to and use of data that relates to Indigenous Australians.

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

As outlined above, we consider that the sensitivity of the data contained in these systems necessitates the implementation of stringent controls to ensure that this data is not accessed, retained, analysed, linked or used for purposes beyond the scope for which it was provided, or shared with or used by, entities that those providing the data would not have contemplated at the time.

Further to our comments in relation to question 11, we consider that purpose limitation must be a key principle in any data access and use system of this kind. Further, while the concept of 'consent' is largely nebulous, we note that, usually, consent is required when sensitive personal information is collected. We query the appropriateness of data being provided to entities that do not have the authority to collect it without the consent of the individual to whom it relates.

Thank you again for the opportunity to comment on this consultation. Should you have any questions in relation to this submission, please contact Adi Prigan, Policy Lawyer, on 9926 0285 or email adi.prigan@lawsociety.com.au.

Yours sincerely,

Juliana Warner
President