New South Wales
Council for Civil Liberties

NSWCCL SUBMISSION

OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER

NATIONAL HEALTH (PRIVACY) RULES 2018 REVIEW

3 June 2021

About NSW Council for Civil Liberties

NSWCCL is one of Australia's leading human rights and civil liberties organisations, founded in 1963. We are a non-political, non-religious and non-sectarian organisation that champions the rights of all to express their views and beliefs without suppression. We also listen to individual complaints and, through volunteer efforts, attempt to help members of the public with civil liberties problems. We prepare submissions to government, conduct court cases defending infringements of civil liberties, engage regularly in public debates, produce publications, and conduct many other activities.

CCL is a Non-Government Organisation in Special Consultative Status with the Economic and Social Council of the United Nations, by resolution 2006/221 (21 July 2006).

Contact NSW Council for Civil Liberties

http://www.nswccl.org.au
office@nswccl.org.au
Correspondence to: PO Box A1386, Sydney South, NSW 1235

The NSW Council for Civil Liberties (NSWCCL) welcomes the opportunity to make a submission to the Office of the Australian Information Commissioner in regard to the Review of the National Health (Privacy) Rules 2018 (Review).

Introduction

1. The Review has been prompted by the sunsetting of the National Health Privacy Rules 2018 (Rules), a legislative instrument under section 135AA of the *National Health Act 1953* (Act). The Rules apply to the processing and storage of Medicare Benefits Schedule (MBS) and Pharmaceutical Benefits Schedule (PBS) claims information by Services Australia and the Department of Health. The Review will determine whether and how the Rules should be updated.

2. NSWCCL considers that the Rules adequately protect the privacy of individuals and that to the extent that privacy safeguards are eroded the Rules should not be amended. The Consultation Paper that accompanies the Review makes it clear that there is an emerging public policy approach "favouring data use and reuse in research, evidence-based decision making and the provision of government services generally."[1]

   NSWCCL does not accept that a technocratic approach to more convenient or efficient service-delivery and research policy warrants eroding the privacy safeguards in the Rules.

3. Within the last 5 years public perceptions of how data should be used and shared have changed. The expectations of a majority of Australians are in favour of more privacy protections over their information, not less. The latest Government survey of Australians' privacy concerns shows 84% of Australians consider it to be a misuse of their information when supplied to an organisation for a specific purpose and then used for another purpose.[2]

4. Public policy is served, under the Rules, by recognising that the information provided to the Department of Health and Services Australia is for the purpose of dealing with MBS and PBS claims and for no other secondary purpose. Public policy is served by recognising that the information provided by individuals is provided because they have to, if they wish to avail themselves of Medicare or PBS services. Public policy should sufficiently acknowledge the interests of individuals in their own data and that government is the custodian of that data. If there is any sensitive personal information provided to government that should not be used for secondary purposes, then, surely, this is that information.

[1] OAIC Consultation Paper: National Health (Privacy) Rules 2018 review. https://www.oaic.gov.au/engage-with-us/consultations/national-health-privacy-rules-2018-review/consultation-paper-national-health-privacy-rules-2018-review/

[2] OAIC 2020 Australian Community Attitudes to Privacy Survey https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey/

5. In order to assist the Commissioner, further commentary in this submission refers as much as possible to the headings of the key issues and general questions in the Consultation Paper.

Are provisions in the Rules fit for purpose? Is the balance between protection of privacy and use of claims information achieved?

6. NSWCCL considers that the Rules get a great deal right. Databases for PBS and MBS claims information are to be kept separate and are kept separate from enrolment and entitlement databases. Claims information between the MBS and PBS and old information can only be linked in certain limited circumstances. Old information must not include identifiers. These are matters prescribed in S135AA of the Act.

7. The purpose of the S135AA and the Rules is to "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."[3] Though, "provision remains for the use of such information for health policy and medical research purposes in certain circumstances."[4] NSWCCL emphasises the strict purposes that must inform the activities of Services Australia and the Department of Health.

8. Community expectations of the handling of sensitive health information are that it will not be repurposed. The government and its agencies are the custodians of its citizens' data and the interests of those conducting projects or research do not outweigh the risk of a breach of the private information of those citizens. Simply because that database exists does not mean that it should or needs to be exploited.

9. NSWCCL opposes any change to the Rules which would increase accessibility to data information for secondary purposes. The results of any authorised secondary use must benefit the public overall, not the priorities of researchers or the public service. Sharing more data will not necessarily lead to better outcomes and represents a technocratic approach to managing policy outcomes. Drives for efficiency and data-driven results can lead to unfairness and discrimination.

10. The purpose for which data is proposed to be used should be independently assessed as appropriate having regard to its necessity, use and value to the public.

11. Opting out of digital interactions, of this kind, is not a realistic option for most people. When individuals share their personal information with government, it is generally because they have to. Government agencies typically collect personal information because its citizens want or need to access some kind of government service. Balancing interests therefore amounts to having to agree to terms of access.

[3] National Health (privacy) Rules Explanatory Statement, Policy intent of the legislation and Rules https://www.legislation.gov.au/Details/F2018L01427/Explanatory%20Statement/Text
[4] ibid

NSWCCL therefore considers that the default position should be that any disclosure of our personal information should only occur in very limited circumstances. The Rules in their current form allow for this.

12. Balancing or leveraging of technological options should not mean sacrificing personal privacy. The Rules should continue, and enhance, minimisation of the social implications of privacy violations in order to maintain the public's trust and government accountability.

13. The Rules need to continue to set high standards for the limitation of data sharing. They permit linkage of claims information and disclosure, amongst other circumstances, for the enforcement of criminal law, a category which can widen with the introduction of new legislation. In this regard, the Consultation Paper flagged the Review of the *Privacy Act 1988* and the introduction of the *Data Availability and Transparency Bill*, both of which encompass significant changes to privacy regulation and data sharing policy.

Prescription, technological specificity and interaction with the APPS

14. It is appropriate for the Rules to be prescriptive. One of the purpose of Rules is to contain technical information rather than that information being set out in the Act.

15. The Consultation Paper makes reference to the latest rapidly changing information technology and the possible redundancy of some privacy safeguards. NSWCCL does not consider, for example, that the use of separate databases is a requirement that is inefficient or inappropriate. It accords with GDPR principles of data protection and storage limitation.

16. NSWCCL considers that it would be prudent for government entities to also revert to the other GDPR data privacy principles of lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; integrity and confidentiality (security) and accountability. Modern data practices that accommodate or enhance these principles and don't undermine or erode privacy safeguards are appropriate.

17. The *Privacy Act 1988* provides minimum privacy safeguard compliance for government entities. Australian Privacy Principle (APP) 6 deals with the use or disclosure of personal information and states that "If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose)."

18. The Rules should continue to exceed the minimum requirements of the *Privacy Act* not least because other legislation may be exempt from that Act with unintended consequences for the use of claims information.

Detailed Technical Standards & Retention and reporting of linked claims information

19. Rule 8(4) requires Services Australia to maintain detailed technical standards in relation to the MBS and PBS databases. Rules 10(3) and 11(5) require the Department of Health and Services Australia to provide an annual report to the OAIC of the extent to which new and old claims information is linked. If these standards and reports are public, they are not readily available to the public. If they are not public, they should be. The publication of technical standards and reports relating to data use are a function of appropriate transparency and accountability.

20. Rule 14(3) requires the Department of Health to maintain and make public a policy statement outlining its practices of disclosure. This statement is not easily accessible or available to the public.

21. Reporting should include details of who has requested and been provided with linked information.

22. Technical standards should be over and above the existing information security requirements applying to Services Australia. Services Australia reported a total of 20 cybersecurity incidents to the Australian Cyber Security Centre (ACSC) in 2019-20.[5] There is no information about how many individuals were affected by those incidents.

23. Other agencies handling claims information should be subject to the same technical standards as the Department of Health and have the relevant skills in data security.

24. Relinking claims information risks reidentification. Any relinking and storage of information without strict data destruction policies is dangerous and counter to the purposes of the Rules. Advances in technology which can claim to assist in efficiencies for the Department of Health also create increased risk of breach of privacy safeguards and reidentification, in particular.

Disclosure of claims information for medical research

25. In the interests of data minimisation, provisions for medical research disclosures, should be framed narrowly with strict data destruction terms (as currently existing or narrower). Keeping claims information long term in other databases defeats the purpose of the Rules and enables increased likelihood of exploitation by technological threat.

Statutory tort for serious invasions of privacy

26. Breach of privacy provisions may have terrible consequences for the individual. An individual can have limited compensation options [6] for a breach but should be able to sue for breach of privacy.

Recommendations

[5] https://www.zdnet.com/article/services-australia-reported-20-security-incidents-to-the-acsc-in-2019-20/
[6] S52(1)(b)(iii) privacy Act 1988

27. NSWCCL opposes any change to the Rules which would increase accessibility to data information for secondary purposes.

28. NSWCCL opposes any erosion of the privacy safeguards in the Rules and recommends strict adherence to data privacy principles, as set out in the GDPR. Privacy safeguards must continue to be more robust than those set out in the *Privacy Act 1988*.

29. NSWCCL recommends that all technical standards, linkage reports and policy statements be made public and easily accessible. Linkage reports should include the source of the linkage/data request.

30. NSWCCL supports the introduction of a statutory tort for serious invasions of privacy to control excessive collections of data and to provide a remedy for unauthorised access to and breach of that data.

This submission was prepared by Michelle Falstein on behalf of the New South Wales Council for Civil Liberties.

Yours sincerely,

Michelle Falstein
Secretary
NSW Council for Civil Liberties

Contact in relation to this submission- Michelle Falstein:
email michelle.falstein@nswccl.org.au;
Tel 0412980540