CALABASH
SOLUTIONS

SUBMISSION

National Health (Privacy) Rules 2018 review

CONTACT US

W www.calabashsolutions.net

E info@calabashsolutions.net

OVERVIEW

The *National Health (Privacy) Rules 2018* (the **Rules**), a legislative instrument made under section 135AA of the *National Health Act 1953,* requires the Office of the Australian Information Commissioner (**OAIC**) to issue privacy rules for how Services Australian and the Department of Health handle Medicare Benefits Scheme (**MBS**) and Pharmaceutical Benefits Schedule (**PBS**) claims information.

Scheduled to sunset on 1 April 2022, the Rules are being reviewed by the OAIC to ensure that, in their current form, they achieve the intent of section 135AA of the National Health Act and are easy to read, understand and apply in practice.

The OAIC requests input from interested individuals, agencies and organisations on all elements and aspects of the Rules, including, but not limited to, their effect on individuals, the operation of MBS and PBS processes, public sector operations and policy development, open data and associated research initiatives.

This document is Calabash Solutions' submission to the Consultation Paper: National Health (Privacy) Rules 2018 review (**Consultation Paper**). This document details our exclusive focus on Questions 12 – 29 of the Consultation Paper. We do not cover Questions 1 – 11 ('Key Questions for this Review').

Calabash Solutions welcomes the opportunity to contribute to the review of the Rules, and makes ourselves available for further discussion, questions and comments.

Calabash Solutions consents to the publication of all or part of our submission to public fora.

Donna-Leigh Jackson (CIPM, CIPT)

Director, Calabash Solutions

Carey-Ann Jackson

Director, Calabash Solutions

PREAMBLE

The MBS and PBS are critically important health services, providing invaluable, often life-preserving, support to Australian residents and certain categories of visitors to Australia. Through these schemes, funded by the federal government, millions of Australians are able to access affordable, reliable health care.

Calabash Solutions' submission to the Rules recognises the importance of these schemes but also values the importance of protecting the privacy of the schemes' beneficiaries. As our submission will show, we caution against any relaxations that erode or compromise the privacy of claimants.

SPECIFIC QUESTIONS ABOUT THE RULES

Management of claims information 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?

Section 8(2) and Section 8(3) of the Rules provide the requirements for how Services Australia must manage claims information. Specific requirements refer to:

- the separation of the MBS claims database and PBS claims database from enrolment and entitlement databases;
- the exclusion of personal identification components other than the Medicare card number from the MBS claims database; and
- the exclusion of personal identification components other than the Pharmaceutical entitlement number from the PBS claims database.

Calabash Solutions' position is that the current requirements should remain unchanged: the requirements minimise the risk of unintended or unauthorised secondary uses of claims information. In so doing, they reduce the likelihood of unintended negative impacts and reduce the risk of serious harm to claimants whose information is linked.

Calabash Solutions notes the absence of a defined meaning for the expressions '*enrolment database*' and '*entitlement database*'. When these expressions are not defined, there is a risk that agencies may not comply with these requirements by unintentionally misinterpreting their intent. To improve clarity, and for the avoidance of doubt, Calabash Solutions suggests that either the Rules or the Explanatory Statement on the Rules be updated to include the meaning of these two expressions.

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 applying to Services Australia?

14. Should the technical standards cover any other matters?

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

Section 8(4) of the Rules requires Services Australia to establish and maintain standards to ensure a range of technical matters are adequately dealt with in designing a computer system to store claims information.

We believe that this requirement is necessary, and should be retained for the following reasons:

- The nature of the information in scope of the Rules, being sensitive information, is afforded a higher level of protection under the Privacy Act 1988.
- A technical standard is necessary to describe the specific category of data in scope of the Rules, being MBS and PBS claims information. While the Privacy Act makes provisions for sensitive information, MBS and PBS claims information requires specific attention to assure its protection.
- The technical standard should consider holistically all security obligations in relation to MBS and PBS claims information, including any and all information security requirements under Australian Privacy Principle (**APP**) 11 in the Privacy Act, the Australian Government's Protective Security Policy Framework and the Information Security Manual.
- The identification, implementation, management, monitoring and evaluation of security controls is an agency's only defence against unauthorised access, disclosure or loss of information, and in the protection and safekeeping of information.
- As reported by the OAIC, there has been an increase in notifiable data breaches by Australian Government agencies. For the first time since its introduction, Australian Government as a sector is among the top five industry sectors to report notifiable data breaches in the period July to December 2020. The OAIC has recently made the following determinations in relation to privacy complaints against government agencies:
    - See 'WP' and Secretary to the Department of Home Affairs (asylum seeker data breach)
    - See 'WZ' and CEO of Services Australia (Centrelink breached domestic violence victim's privacy by disclosing new address to former partner)
    - See 'WL' and Secretary to the Department of Defence (disclosure of former reservist officer personal information by the Australian Defence Force in relation to the sale of ADF items)
- Media reports have highlighted these additional disclosures of personal information involving federal and state government agencies:
    - See A data bungle put at risk the private health details of millions of Australians
    - See My Health Record system data breaches rise

- See Data breach sees Victorian Government employees' details stolen
- See Family Planning NSW targeted by hackers with ransom demand, data of 8,000 people at risk

The requirements for a technical standard should remain in place, with some notable amendments. It is our view that the scope of the technical standard be updated. The current scope refers to the design of a computer system to store claims information. The scope is too narrow and restrictive; it should be expanded to include the design and implementation of the computer system and solutions, as well as all related support activities required for ongoing management, monitoring and evaluation of computer systems.

The Rules currently provide that the technical standard should specify:

- access controls;
- security procedures and controls to prevent unauthorised linkage of records;
- measures to enable tracing of authorised linkages; and
- destruction schedules for authorised linkages.

The Rules would benefit from being less prescriptive in the matters that need to be covered by the technical standard. The technical standard should cover other matters that more broadly describe all security controls needed to safeguard claims information. The requirement should be amended to refer to the establishment and maintenance of a technical standard that aligns with industry best practice security controls, or that refers to specific Australian Government Security Frameworks.

Section 8(5) of the Rules provide Services Australia must lodge a Variation Report with the Australian Information Commissioner detailing variations to the technical standards. Calabash Solutions believes that this requirement is an overly burdensome one for the Australian Information Commissioner. What is not apparent from the Rules is the action the Australian Information Commissioner is required to take in response to a lodged Variation Report. It would be best placed to amend this requirement, to place the burden of accountability of ensuring their technical standard is current, up to date and adheres with industry best practice, on Services Australia. The Rules may be updated to include provisions on the cadence of reviews; for example, at a minimum, an annual review or a review per major change (technological or information handling practice change) or in response to a privacy impact assessment finding, a data breach or an improvement initiative.

Calabash Solutions believes that each agency that handles sensitive information (as defined under the Privacy Act) should establish and maintain technical standards. Because the risk of serious harm to an affected individual of a data breach is significantly greater when the information is sensitive, we believe that agencies should be accountable for the safekeeping of the information it holds. Federal and state government agencies should not be exempt from this responsibility.

Medicare Personal Identification Numbers (PINs)

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

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

Section 8(6) of the Rules provides that Services Australia may maintain a Medicare PIN to assist in identifying individuals included in the MBS and PBS databases. Medicare PINs may be stored on databases holding records of claims information.

Calabash Solution supports the current provisions for the creation, use and disclosure of Medicare PINs. These provisions appear suitably restrictive in preventing their use as an identifier for other purposes.

Section 8(8) provides that a Medicare PIN must not be based on or derived from a person's name, date of birth, address, telephone number or Medicare card number. Calabash Solution suggests that this requirement be updated. The Australian Government is currently conducting a review of the Privacy Act; part of the review seeks to evaluate the current definition of "*personal information*". In line with the likely expansion of the definition of "*personal information*", Calabash Solution believes that Section 8(8) should be amended as follows:

- remove explicit reference to a person's name, date of birth, address, telephone number of Medicare card number; and
- replace with a reference to any information that identifies an individual or refer to the personal information definition provided in the Privacy Act.

Calabash Solutions cautions against any amendments to the Rules that sees the relaxation of Medicare PIN disclosure requirements. It should not be the case that Medicare PINs be shared with other agencies, unless as permitted by restrictive disclosure requirements.

Disclosures by Services Australia to the Department of Health

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

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

As permitted under Section 9 of the Rules, Services Australia may disclose claims information to the Department of Health provided that such disclosures do not include personal identification components, except as permitted by section 14 of the Rules or where directly connected to the Department of Health assisting the Chief Executive Medicare to perform his or her health provider compliance functions in accordance with these Rules. Services Australia may disclose to the Department of Health claims information that contains a Medicare PIN and/or an encrypted form of an individual's Medicare card number.

Where Services Australia lawfully discloses information to an agency, organisation or individual other than the Department of Health it must not provide both the name and the Medicare PIN unless it is expressly required by or under law (for example, under warrant or subpoena).

It is our view that the current disclosure provisions strike the correct balance between data sharing and protection of privacy. Only in limited circumstances should claims information include personal identification components. The circumstances that permit the disclosure of claims information with personal identification components are explicitly provided by the Rules.

APP 6 of the Privacy Act provides 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**) unless:

> (a) the individual has consented to the use or disclosure of the information; or
>
> (b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

APP 6 provides a range of exceptions for the use or disclosure of personal information for a secondary purpose. We believe that the secondary purpose exceptions provided under APP 6.2 and APP 6.3 of the Privacy Act are suitably adequate for regulating disclosure of claims information to agencies, organisations or individuals other than the Department of Health.

Calabash Solutions cautions against any amendment to the Rules that seeks the relaxation of disclosure requirements. Our position seems to be supported by the findings from the 2020 OAIC Community Attitudes to Privacy Survey which showed that only 36% of Australians are comfortable with Government agencies sharing their personal information with other Australian Government agencies, while 40% are uncomfortable with this. The uptake of COVIDSafe, a government contact tracing app, is relevant here, too. Approximately 6.4 million downloads occurred, suggesting that only 28% of Australians with a mobile phone installed the app after it launched.

Considered together, these cited references suggest a hesitancy by the Australian public towards the collection and sharing of their personal information by agencies.

Linkage of claims information

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?

Section 9 of the Rules makes specific provisions regarding the circumstances in which claims information from the MBS database and the PBS database relating to the same individual may be linked.

While the circumstances provided by the Rules seem reasonable, Calabash Solution notes a news article reporting on the Australian government secretly releasing sensitive medical records to police. As reported, Services Australia was found to be operating under outdated guidelines to decide how and when to respond to requests for PBS and MBS data from state and federal policing agencies. Services Australia confirmed it has granted 2,677 requests (just over 7 requests a day) from police for PBS and MBS data in the 12 months from September 2017. What was not reported on was the number of requests received from police in the reporting period, but not granted by Services Australia.

Calabash Solutions recommends that the guidelines referred to in the article (Guidelines for the release of information where necessary in the public interest) be updated by Services Australia and submitted to the Australian Information Commissioner for evaluation.

Calabash Solutions cautions against any relaxation of linkage provisions in the Rules. The linkage provisions need to be considered in conjunction with the introduction of the *Data Availability and Transparency (Consequential Amendments) Bill 2020* (the **Bill**), a scheme intended to authorise and regulate access to Australian Government data. If enacted, the Bill will authorise public sector data custodians to share data with accredited users in accordance with specific authorisations, purposes, principles and agreements. With the impending introduction of the Bill, Calabash Solution advocates for a rigorous regime that further limits the linkage of claims information, a position that appears to be supported by genuine public interest.

Retention and reporting of linked claims information

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

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

Section 10 of the Rules provides that linked claims information must be destroyed as soon as practicable after meeting the purpose for which it was linked. Services Australia and the Department of Health must also report to the Australian Information Commissioner certain information about their linkage activities including the number of records linked, the purposes of the linkage, the number of linked records that were destroyed, and so on.

Calabash Solutions believes that the current data retention requirements are appropriate. Claims information should only be linked for specific and prescriptive purposes. For this reason, data retention requirements for linked claims information should closely align with the purpose of performing the linkage in the first place. Failure to implement stringent data retention requirements that align with the purpose may result in function creep and unauthorised secondary use or disclosure of linked claims information. The rigorous retention requirements provided under Section 10 of the Rules complement APP 11.2 of the Privacy Act, which states that if an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed, the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

Furthermore, we believe that the current reporting arrangements for linked claims information places unnecessary burden on the Information Privacy Commissioner. The Rules currently do not state what action the Information Privacy Commissioner is required to take upon receiving the report, other than to decide whether to make the report publicly available. Is the intention of the reporting arrangement for the OAIC to monitor and provide oversight on the handling of linked claims information by Services Australia and the Department of Health? If so, an alternate provision should be to hold Services Australia accountable for their adherence to the linked claims information provisions. One method to improve accountability would be for the agencies to publish the report for wider public scrutiny, which would further increase transparency.

Old information

23. Are the provisions applying to old information appropriate?

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 *National Health Act 1953* defines '*old information*' to mean information that has been held by one or more agencies for at least the preceding 5 years. Section 11 of the Rules provides that Services Australia must store old information in separate databases from the MDS and PBS databases claims information, in a form that does not include any personal identification components. Old information may only be linked to personal identification components by use of a Medicare PIN in limited circumstances, as prescribed in Section 11(2). These circumstances include:

(a) taking action on an unresolved compensation matter;
(b) taking action on an investigation or prosecution;
(c) taking action for recovery of a debt;
(d) determining entitlement on a late lodged claim or finalising the processing of a claim;
(e) determining entitlement for a related service rendered more than five years after the service which is the subject of the old information;
(f) fulfilling a request for that information from the individual concerned or from a person acting on behalf of that individual; or
(g) lawfully disclosing identified information in accordance with the secrecy provisions of relevant legislation and this instrument.

Calabash Solutions is of the view that these provisions are appropriate. There should be no expansion to the circumstances in which old information can be linked with personal information components. Old information that is linked with personal information components should be destroyed as soon as practicable after meeting the purpose for which it was linked.

The requirement for Services Australia and the Department of Health to provide to the Australian Information Commissioner an annual report detailing the extent to which old information has been linked to personal identification components places an unnecessary burden on the Information Privacy Commissioner. The Rules do not currently state what action the Information Privacy Commissioner is required to take upon receiving the report, other than to decide whether to make the report publicly available. Is the intent of the reporting arrangement to ensure that the OAIC monitors and provides oversight on the handling of old information by agencies? If so, an alternate provision may be to hold Services Australia accountable for their adherence to the old information provisions. One way to improve accountability is to publish the report for wider public scrutiny, which would further increase transparency.

Disclosure of identifiable claims information for medical research

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?

Section 12 of the Rules provides that identifiable claims information may be disclosed for medical research purposes, if the individual to whom the information relates has given their informed consent to the use of their information in the research project or the disclosure is made for the purposes of medical research to be conducted in accordance with guidelines issued by the *National Health and Medical Research Council* under section 95 of the Privacy Act.

It is the position of Calabash Solution that the requirements should be made mutually inclusive; both requirements should be met (not one or the other) before identifiable claims information is disclosed for medical research purposes. Citing the 2020 OAIC Community Attitudes to Privacy Survey, Australians are far less likely to be comfortable with Government agencies sharing their personal information with businesses in Australia (15% comfortable, 70% uncomfortable). Further, Australians are presented with no privacy choice with respect to what information is collected about them in relation to the MBS and PBS claims information and how their information is managed. What should be presented to individuals as a privacy choice is whether claims information that identifies them is shared for medical research purposes. Individuals may have strongly held views regarding the nature of the research being undertaken, or may wish to be excluded for fear of harm if their information is compromised in some way by the researcher.

Section 12(2) of the Rules provides that Services Australia must obtain a written undertaking from the researcher that the claims information will be securely destroyed at the conclusion of the research project. It is Calabash Solutions' position that this provision does not go far enough to safeguard the identifiable claims information. We believe that Section 12(2) should be strengthen, to seek a written undertaking from researchers that identifiable claims information will be kept safe, and will only be used for the **primary purpose** of conducting research. It should not be the case that researchers are able to use identifiable claims information for a secondary purpose.

It is our position that these provisions be retained under the Rules, and not be deferred to the Privacy Act, to strengthen their efficacy.

Use of claims information

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

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

Section 13 of the Rules states that claims information provided to the Department of Health by Services Australia in accordance with Section 8(9) may be used by the Department of Health as authorised by the Secretary of the Department of Health, or delegate. Claims information may be linked by a Medicare PIN by the Department of Health in certain circumstances, such as where the linkage is necessary for a use authorised by the Secretary of the Department of Health, or delegate and the claims information is used solely as a necessary intermediate step to obtain aggregate or de-identified information.

It is Calabash Solutions' view that the Rules be reviewed, to be made more restrictive on the use and disclosure provisions of claims information by the Department of Health, as well as the linkage provisions by the Department of Health. The Rules should more explicitly list the circumstances under which the Department of Health as authorised by the Secretary of the Department of Health, or delegate, may use or disclose claims information.

Further, the current provisions for the linkage of claims information should remain intact, and not be relaxed in any way.

In relation to the disclosure provision, we believe that all disclosures by the Department of Health be reported publicly, and lodged with the Australian Information Commissioner, to improve transparency and to enhance Department of Health accountability.

Finally, we suggest that the heading of Section 13 of the Rules be amended from "Use of claims information" to "Use and disclosure of claims information by the Department of Health", or similar.

Name linkage

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

The Department of Health may collect from Services Australia the name and other personal identification components corresponding to a Medicare PIN where that is authorised by the Secretary of the Department of Health, or delegate, 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.

Calabash Solutions cautions against any relaxation of requirements to the name linkage provisions by the Department of Health. Citing the 2020 OAIC Community Attitudes to Privacy Survey, only 36% of Australians are comfortable and 40% of Australians are uncomfortable with Government agencies sharing their personal information with other Australian Government agencies. Any attempt to relax the circumstances that allow name linkages should be thwarted, in light of Australians' privacy expectations.

Section 14(6) provides that the Department of Health must advise the Australian Information Commissioner of procedures developed to ensure compliance with Sections 14(2), (4) and (5) and any changes to those procedures.

Calabash Solutions believes this requirement should be strengthened. As noted early in Australian government secretly releasing sensitive medical records to police, Services Australia has been found to operate under outdated guidelines to decide how and when to respond to requests for PBS and MBS data from state and federal policing agencies. We would seek more stringent accountability on procedures being reviewed regularly, with a minimum requirement of an annual review or a review per major change (technological or information handling practice change), or following a privacy impact assessment, data breach or improvement initiative.

Other matters including management of paper copies

29. Are provisions relating to paper copies of claims information appropriate? Why or why not?

Section 15(1) provides for the conditions under which paper copies of claims information may be made.

Calabash Solutions believes that the provision pertaining to paper copies of claims information be expanded, to include any copies of claims information, and not just those recorded in paper form. Besides the expansion of the meaning of '*copies*', all other provision under Section 15(1) should be retained as per current form.

OUR VISION

Healthy. Safe. Respected. Free.

We believe in a world where all people are healthy, safe, free, and respected.

OUR MISSION

Helping Others.

The best versions of ourselves emerge when we help others to be the best versions of themselves.

OUR APPROACH

Listen. Support. Analyse. Discover

- We value patient privacy, and work with health service providers to assure and implement compliant privacy programs.
- We listen to patients and carers as they talk about their journeys through all systems of care.
- We develop and deliver Continuous Professional Development (CPD) for clinicians, support staff, and practice managers.
- We work with small and medium datasets to understand what inhibits or enables treatment compliance within unique patient cohorts.
- We embrace solutions that work, from technology to the creative arts, to cultivate health systems that deliver patient-centred care.

CONTACT

W www.calabashsolutions.net

E info@calabashsolutions.net

M +61 (0) 430 231 184

OUR PRIVACY SERVICE OFFERINGS

Online Privacy Training

Designed specifically for private sector health care workers. Offers a commonsense, practical view of the Australian Privacy Principles. Demonstrates how to apply the Australian Privacy Principles in Australian private health care sector.

Face-to-Face Training

Register for face-to-face training delivered at your practice, for your team.

Face-to-face training lets you and your team discuss your practice-specific privacy questions, concerns.

Privacy Compliance Assessment

Does your practice comply with the Australian Privacy Act? We assess your practice's compliance with the privacy principles using our privacy compliance assessment tools. Onsite visit and review of your privacy systems, processes and practices against the thirteen Australian Privacy Principles contained in the Privacy Act.

Privacy Compliance Heat Map

After the privacy compliance assessment, we produce your unique privacy compliance heat map showing areas of strong and weak compliance against the thirteen Australian Privacy Principles.

Templated Privacy Processes

Use our privacy compliance heat map to uncover your areas of weak compliance. We work with you to strengthen the gaps and create privacy processes for your practice

DISCLAIMER