AUSTRALIAN MEDICAL ASSOCIATION
ABN 37 008 426 793

# AMA submission to the Senate Finance and Public Administration Committees - Data Availability and Transparency Bill 2020

**Senate Finance and Public Administration Committees**
**PO Box 6100**
**Parliament House**
**Canberra ACT 2600**
**E:** fpa.sen@aph.gov.au

The AMA welcomes the opportunity to comment on the Bill.

## Introduction

It is impossible to overstate the importance of this Bill and the level of concern that the AMA holds regarding significant elements of the proposed legislation given that it:

- applies to any "data lawfully collected, created or held by or on behalf of a Commonwealth body"[1];
- overrides existing Commonwealth, State and Territory statutory secrecy provisions[2];
- overrides the restrictions on disclosure in the *Privacy Act 1988* Cth (the **Privacy Act**); and
- provides no minimum privacy protections – a standard of privacy governance well below community expectations expressed during the 2018 Senate Review of the My Health Record System.

In the health space, this will include data held by:

- The Department of Health
- Services Australia
- Hearing Australia
- National Disability Insurance Agency
- Independent Hospital Pricing Authority
- National Blood Authority
- Organ and Tissue Authority
- Australian Institute of Health and Welfare
- Australian Institute of Family Studies

[1] See definition of ***Public sector data*** in section 10(2).
[2] Section 23 (Authorisation to share override other prohibitions)

**Recommendations**

The Government has proposed that the Regulations exclude aspects of the PSR scheme and provisions of the *My Health Record Act 2012* from the scheme. The AMA **strongly recommends** that the Regulations also list sensitive health data, particularly MBS and PBS data. This is because:

- this data is subject to existing statutory secrecy obligations and is a core component of the information held in My Health Record; and
- the Bill does not afford a level of privacy protection for health data that is equivalent to the protections in the Privacy Act, the *National Health Act 1953* and the *Health Insurance Act 1973.*[3]

There is scope for the Regulations to be updated in the future once agencies demonstrate that they have the capacity and capability to appropriately de-identify this data.

The AMA has also included other recommendations throughout our submission.

**No minimum privacy protections**

Agencies can determine their own privacy settings

The AMA's main concern with the Bill is that it provides no minimum privacy protections. Section 16(11) requires that agencies be:

> *satisfied that each [data sharing] principle is applied to the sharing in such a way that, when viewed as a whole, the risks associated with the sharing are appropriately mitigated.*

In other words:

- Agencies are responsible for determining whether the data sharing principles have been met; and
- There is no requirement for all the data principles to be satisfied in full.

It is also important to acknowledge that the data sharing principles (in section 16) themselves are inherently subjective: sharing must be with "appropriate persons" (people principle) for an "appropriate" project (project principle) in an "appropriately controlled environment" (setting principle) for an "appropriate protection" (data principle).

This means that, unless an agency had no regard to the data sharing principles or failed to comply with other procedural requirements, it would be difficult to 'second guess' their decision. This leaves the public with little comfort that they will have redress – or that the officials and/or

[3] Breaches of section 135A of the *National Health Act 1953* and section 130 of the *Health Insurance Act 1973* are criminal offences.

agency will be penalised – if decisions are made recklessly or negligently. While section 14 includes criminal offences for recklessness, this only applies where a person is reckless as to whether or not sharing was authorised by section 13(1). It will not be triggered where an agency applies the sharing principles in a way that would be considered by third parties to show a reckless disregard for the risk of re-identification or misuse.

While section 19 requires that data sharing agreement include mandatory terms and that data sharing agreements be lodged with the Data Commissioner (section 33), there is no power for the Data Commissioner to:

- Approve data sharing agreements prior to finalisation; or
- Require amendments to data sharing agreements to enhance privacy protections.

**Recommendations:** The AMA recommends that:

- section 16(11) be amended to require that each data principle has been satisfied;
- decisions to share and the conditions imposed on sharing be subject to merits review by the Administrative Appeals Tribunal (**AAT**), with the Data Commissioner, OAIC and individuals' whose data is being shared having standing;
- decisions to share not take effect until 28 days after the key details of the data sharing agreement have been published by the Data Commissioner in accordance with section 116 (in order to provide an opportunity for review);
- if review is sought, sharing be suspended while the matter is being while the matter is being considered by the AAT;
- the Data Commissioner have greater powers to intervene prior to sharing or release, including the capacity to require that data not be shared until the agency has demonstrated that risks have been adequately addressed.

<u>No Data Codes and Guidelines</u>

The Data Commissioner may issue a data code (section 126) that:

- sets out "how the data definitions in section 10, and provisions of Chapters 2 (including section 13) and 3, are to be applied or complied with"; and
- imposes "additional requirements to those imposed by Chapters 2 and 3".

However, these data codes have not been circulated and there is no obligation on the Data Commissioner to establish data codes prior to the commencement date.

By contrast, under the previous Data Integration Partnership for Australia (DIPA)[4]:

- Integration had to be undertaken by an authorised data integrating Authorities – the Australian Bureau of Statistics or the Australian Institute of Health and Welfare

[4] https://pmc.gov.au/public-data/data-integration-partnership-australia

- Linked health data had to be anonymised using best practice privacy preserving linking methods with the technical assistance of Data61.
- Linked data had to be used in secure environments such as a virtual data centre.

**Recommendation:** The AMA recommends that either:

- the data sharing principles include minimum privacy requirements for specific types of data, such as linked data or health data that are at least as robust as the requirements that were required by Data Integration Partnership for Australia (DIPA); or
- the Data Commissioner be required to issue data codes prior to the commencement of the Act, to allow these issues to be addressed.

Section 27 (Guidelines)

While the Data Commissioner may issue guidelines (section 127), data scheme entities are not required to comply with Guidelines or keep a record of why the Guidelines were not complied with.[5] By contrast agencies are required to provide written reasons for rejecting a request to share data (section 24).

**Recommendation:** The AMA recommends that agencies be required to keep a record of why they chose not to comply with any Guidelines.

Sections 18 and 137 (Authorised officers)

Section 18 requires that a data sharing agreement be entered into by an authorised officer. There is no statutory requirement for an authorised officer to hold a minimum level of seniority (eg SES or equivalent).

**Recommendation:** The AMA recommends that only senior officers be able to sign off on a decision to share individuals' health information, particularly MBS and PBS data.

No requirement to obtain ethics approvals before using health data without individuals' consent

Section 16(2)(c) (project principle) recommends that "any sharing of the personal information of individuals is done with the consent of the individuals, **unless it is unreasonable or impracticable to seek their consent**". It is entirely foreseeable that this exception will be used to justify the disclosure of MBS and PBS data large datasets of identified or identifiable sensitive health information without patient consent. We note also that this exception has been included as a standard justification for not obtaining patient consent in the Draft Data Sharing Agreement Template issued by the Data Commissioner.[6]

[5] Section 27 provides that agencies must "have regard to the guidelines".
[6] https://www.datacommissioner.gov.au/resources/draft-data-sharing-agreement-template

By contrast, section 16B(3) of the Privacy Act allows the collection, use and disclosure of health information without the individual's consent where, amongst other things, the use or disclosure is conducted in accordance with guidelines approved under section 95A of the Privacy Act. These guidelines are maintained by the NHMRC.[7]

While section 16(2)(b) of the Bill requires that any "applicable processes relating to ethics are observed", unlike section 95A of the Privacy Act, it does not contain any mechanisms for specifying what those processes are. This means that, unless the entity is already required to comply with the NHRMC Guidelines or other ethical guidelines, it will have no legal obligation to do so.

**Recommendation:** The AMA recommends that ethics approval be mandatory whenever identified or identifiable health data is being shared or released without individuals' consent. The AMA acknowledges that there may also be circumstances where obtaining ethics approvals is best practice notwithstanding that individuals have provided consent.

No obligation to use accredited data service providers (ADSP) to undertake de-identification

While the Bill includes provision for public or private organisations to be accredited as accredited data service providers:

- agencies are only required to "consider" whether to use an ADSP (section 16(2)(d));
- agencies may choose to undertake de-identification in-house; and
- the Data Commissioner has limited power to direct agencies to engage external expertise.

While the Data Commissioner can make recommendations under section 111, this provision only applies where the Data Commissioner has completed an assessment or investigation under Part 5.4. These are both formal processes. Recommendations are not enforceable. The Data Commissioner could direct an agency to outsource, but only where the Data Commissioner is satisfied that this is "necessary to properly address an emergency or high-risk situation" (section 112). This is a high bar.

The well-publicised privacy breaches involving Medicare provider numbers and MyKi travel information demonstrate well-intentioned officers may not be trained to appropriately anonymise personal information.[8]

**Recommendation:** The AMA recommends that:

- rules be issued under section 29 (Engage ADSP for prescribed data services) that require that all data custodians (other than ABS, AIHW and other specified bodies) be required to outsource de-identification and other high-risk activities; and

[7] https://www.nhmrc.gov.au/about-us/publications/guidelines-approved-under-section-95a-privacy-act-1988
[8] Culnane C et al (2019) *Stop the open data bus, we want to get off* University of Melbourne 15 August 2019 https://arxiv.org/pdf/1908.05004.pdf

- decisions not to engage an ASDP be subject to merits review by the Administrative Appeals Tribunal, with OAIC, the Data Commissioner and the individuals' whose data is being shared having standing; and
- sharing be suspended while the matter is being considered by the AAT.

No mechanisms for affected individuals to make complaints

Part 5.3 of the Bill only allows complaints to be made by current data scheme entities (or entities that ceased to be data scheme entities in the previous 12 months)[9]. This means individuals cannot complain to the Data Commissioner if their health information is released or inappropriately shared without their consent.

Paragraph 56 of the draft Explanatory Memorandum states that a person may complain to the Commonwealth Ombudsman, or OAIC about suspected mishandling of their personal information". However, so long as the data custodian has complied with this Act, there will be no interference with their privacy. This means that they will have no grounds for complaint and no right to seek compensation, regardless of how poor the agencies' processes were or the inadequacies of their risk assessment processes. While there may be some scope of individuals to seek judicial review or make claims under Compensation for Detriment caused by Defective Administration (CDDA) procedures, both these processes are complex.

More generally the AMA considers that the complaints mechanism has the potential to discourage complaints. In particular:

- The complainant must "reasonably believe" that another entity has breached the Act (section 88). This is a high bar given that a failure to apply industry standard protections is not a breach unless those standards were specified in the data sharing agreement.
- In most cases "complainants should have first raised their complaint with the respondent directly. This minimises the burden on the Commissioner and respondents when dealing with vexatious or unsubstantiated complaints" (Paragraph 467 of the Explanatory Memorandum).
- There is no provision for anonymous complaints and all complaints must be notified to the respondent if they are to proceed.
- The complaint must be in an approved form and must meet any additional requirements set out in a data code. Paragraph 655 of the Explanatory Memorandum suggests that this could be used to minimise the submission of vexatious or frivolous complaints.

While the Data Commissioner can commence investigations of their own initiative, this only applies if "the Commissioner reasonably suspects that the entity has breached [the] Act" (section 101(2)). This is a high standard and will be difficult for the Data Commissioner to satisfy without a complaint being made. Moreover, there will be no breach if a data scheme entity has followed the steps in the data sharing scheme.

[9] Section 88

These requirements are substantially more onerous than the requirements that apply under the whistleblowing amendments that were made to the Corporations Act.

**Recommendation:** The AMA recommends that:

- the mechanism for complaints be made less legalistic;
- individuals affected by decisions to share their personal information be empowered to lodge complaints with the Data Commissioner;
- the complaints process include provision for anonymous complaints;
- the Data Commissioner have the capacity to remove the complainant's name when notifying a complaint to the respondent; and
- the Data Commissioner to have greater powers to consider issues or complaints that do not comply with the procedural requirements (eg, they are not in the approved form or have not been previously raised with the respondent).

Conflict in the dual responsibilities of the Data Commissioner

The AMA continues to be concerned about the potential conflict between the Data Commissioner's two roles, namely:

- to advocate greater sharing by data custodians; and
- to act as regulator.

Paragraph 48 of the Explanatory Memorandum states that:

> *"As champion of the data sharing scheme, the Commissioner will provide advice, advocacy and guidance to ensure the scheme operates as intended. The Commissioner will also work with data scheme entities to build data capability, promote best practice data sharing and use, and address cultural barriers to sharing."*

If an agency seeks advice from the Data Commissioner prior to entering into a data sharing agreement, there is a potential conflict at the point of providing advice between the Data Commissioner's role of promoting safety and their role of promoting sharing. Moreover, if the data is subsequently re-identified or a complaint is made, the Data Commissioner will be investigating a data sharing agreement that they advised on.

**Recommendation:** The AMA recommends that OAIC be provided with a greater role, particularly where there is the potential for a conflict of interest.

Blanket authorisation to share identified data with individuals or businesses

While the initial consultations focused on de-identified data, the Explanatory Memorandum clearly contemplates sharing and release of identified data. For example:

| | |
|---|---|
| Paragraph 29 | "Sharing data [could improve] user experiences through simplified or automated systems like pre-filled forms and reminders to submit or verify details." |
| Paragraph 103 | "Data sharing ... could improve design of systems, engagement, and processes involved in delivery of government services, including improving user experiences through simplified or automated systems like pre-filled forms and reminders to submit or verify information like a tax return. This purpose supports sharing to undertake services delivered by or on behalf of government, including through contractors." |
| Paragraph 131 | "sharing a certain amount of identifiable data, like street addresses, may be reasonably necessary to pre-fill government forms or to create an integrated dataset for use by researchers." |
| Paragraph 191 | "This clause supports pre-filling forms (to be validated by the individual or business) and a single point-of-contact to engage with multiple government agencies." |

We understand that these provisions have been included to facilitate the use of public data for government service delivery. In line with this section 21(1)(b) provides for this data to be actively validated by the end user.

These provisions and concepts appear to be an 'after thought' and the AMA is concerned that they may dilute the emphasis on robust de-identification of data, data minimisation and only sharing with accredited users. We note also that pre-fill already exists outside this legislation.

**Recommendation:** The AMA recommends that the Bill specify types of data (eg MBS and PBS) that cannot be released under the pre-fill mechanism.

Perverse incentive to share data by email and other unsafe means

Section 8 (Application of the Act) provides that the Act will not apply unless the data sharing falls within one of the Constitutional heads of power in section 8. This means that, for example, unless an Australian university or not-for-profit will only be authorised by the Bill to use non-statistical data for a non-Commonwealth government purpose if:

- It is a "trading or financial corporation" for the purposes of the Constitution[10]; or
- The data "shared with or through accredited entities by means of electronic communication" (eg email or Drop-box).

Paragraph 28 of the draft Explanatory Memorandum defines "electronic communication" as "transfer of information via the internet or a telecommunications network". It suggests that:

[10] Section 51(xx) of the Australian Constitution. See also https://www.fwc.gov.au/anti-bullying-benchbook/who-covered-workplace-bullying-laws/definition-constitutionally-covered-0 and Williams, G., & Pillai, S. (2011). Commonwealth power over higher education. *U. Queensland LJ*, *30*, 287.

> *a data custodian could rely on this subclause to transfer data from its computer or server to that of a State government authority for the recipient's own policies, programs and services, or for research and development, as the application is not restricted to Commonwealth government purposes.*

The AMA is concerned that this creates a perverse incentive for data to be shared by email, Dropbox and other unsecure means where the sharing would not otherwise fall within a Constitutional head of power. The AMA is particularly concerned about sharing health information (particularly MBS and PBS data) via insecure channels where that information is identifiable or could be re-identified.

**Recommendation:** The AMA recommends that:

- section 8(e) be deleted;
- the Bill set out situations where sharing by email or via the internet is not permitted; or
- the Bill set out minimum standards for sharing by email or via the internet.

<u>Ability for individuals' health information to be shared with for profit organisations</u>

Section 15 (Data sharing purposes) allows data to be shared for:

> *(a) delivery of government services;*
> *(b) informing government policy and programs;*
> *(c) research and development.*

As drafted, section 15 allows individuals' health information (including PBS and MBS data) to be shared with private sector organisations for profit. Paragraph 107 of the Explanatory Memorandum states that:

> *Sharing for purposes that are consistent with clause 15(1) but have other applications may be permissible. For instance, a research project to improve pharmaceutical treatments for heart disease may deliver both profit for the researcher as well as serving the public interest. The mere fact of private sector involvement or profit does not infringe clause 15, provided sharing is for a permitted purpose, is not for a precluded purpose, and is otherwise consistent with this Chapter.*

The AMA is concerned about the potential for non-admitted primary healthcare data (including MBS and PBS data) to be shared with health funds for their own purposes. Currently this is prohibited by the *National Health Act 1953, the Health Insurance Act* 1973 *and the My Heath Records Act 2012*. It makes no sense to preclude My Health Record data from the data sharing scheme, but then permit the same MBS/PBS data to be directly shared with private health insurers. This is not consistent with the public's expectations and has the potential to undermine the community-rated private health insurance system.

While the data sharing agreement must describe "how the public interest is served by the sharing" (section 19(7)), there is no ability for the Data Commissioner (or OAIC) to query or second guess this either before or after sharing occurs.

As noted above, agencies must give reasons for refusing to share data (section 24) and health funds may seek judicial review of any decision:

- By the Data Commissioner – not to accredit them as an accredited user an ADSP or both; or
- By an agency – not to share data with them.

**Recommendation:** The AMA recommends that the rules specify that use of MBS data and PBS data by health funds is a precluded purpose (section 15(2)(c)).

Unclear criteria for accreditation

We note that the criteria for accreditation now appear in section 77 of the Bill. We are surprised that the same criteria apply to applications to be an accredited user and to be an ADSP. We would have expected more stringent criteria to applications to be an ASDP.

We had also understood that section 77 would expressly state that entities cannot be accredited unless they are subject to the Privacy Act or equivalent legislation or have opted into the Privacy Act. This is particularly relevant where agencies propose to share with small business or government entities from Western Australia and South Australia (as these entities are prohibited by section 28 from participating).

**Recommendation:** The AMA recommends that more stringent criteria be specified for accreditation as an ASDP and that section 77 expressly state that entities cannot be accredited unless they are subject to the Privacy Act or equivalent legislation or have opted into the Privacy Act.

**11 MARCH 2021**