AUSTRALIAN MEDICAL ASSOCIATION
ABN 37 008 426 793
T | 61 2 6270 5400
F | 61 2 6270 5499
E | info@ama.com.au
W | www.ama.com.au
42 Macquarie St Barton ACT 2600
PO Box 6090 Kingston ACT 2604

AMA submission on the Data Availability and Transparency Bill 2020

[redacted]

The AMA welcomes the opportunity to comment on the exposure draft of the Data Availability and Transparency Bill 2020. Our submission in October 2019, highlighted AMA concerns with a number of the key concepts underpinning the earlier Data Share and Release framework. As explained below, a close examination of the Data Availability and Transparency Exposure Bill (the **Bill**), reveals most of these concerns have not been fully addressed.

It is impossible to overstate the importance of this Bill because it creates an alternative pathway for the sharing and release of public sector "data lawfully collected, created or held by or on behalf of a Commonwealth body". Unless stated otherwise, the Bill is intended to override all existing statutory secrecy provisions and overrides all restrictions on disclosure in the Privacy Act 1988 Cth (the **Privacy Act**). 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

Lack of certainty in the application of the five data sharing principles to individual projects

As noted in our October 2019 submission, the AMA's main concern with the fundamental structure of the proposed new data sharing powers is that, although the five data sharing principles have the potential to protect sensitive identified or potential re-identifiable health data, there is no guarantee that individuals' privacy will be protected in all circumstances. This is because:

- Data custodians (ie, generalist agency bureaucrats) are responsible for determining whether the five data sharing principles have been met.

- The data sharing purposes are very broad.
- Except for the outputs principle (which simply requires that outputs have been agreed), the sharing principles are subjective. In each case, they require that something be "appropriate".
- The data sharing scheme and the Data Commissioner are intentionally biased in favour of sharing.

This means that, so long as an agency (or the accredited user) had completed and lodged the template data sharing agreement with the Data Commissioner, it would be difficult in practice to prove that the decision to share was not consistent with the data sharing scheme. This means that identified or identifiable sensitive MBS and PBS data could be shared with any accredited user so long as the agency is satisfied that the research project is for a "data sharing purpose". While the data sharing agreement must set out "how the public interest is served by the sharing" (section 16(1)), there is no ability for the Data Commissioner (or OAIC) to query or second guess this either before or after sharing occurs.

Ethics

It is positive to see the latest draft Exposure Bill now generally requires consent of the individual before personal information is shared under the data sharing scheme. However, sharing can still proceed without consent, if it is unreasonable or impracticable to obtain this. In practice the difficulty of obtaining individuals' consent prior to the disclosure of large datasets of identified or identifiable data will mean this protection, as currently worded, is extremely weak. For example, it will be unworkable to contact every patient, or every health practitioner who has claimed an MBS or PBS item number to request their consent prior to the release of identified data in these datasets. In comparison, 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.

The AMA remains of the view, that unless there is an enforceable requirement on data custodians to obtain ethics approval prior to the release of identified or identifiable health data under a data sharing agreement, this data should be exempt from the data sharing framework. While section 16(1)(a) 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. In our view, some form of ethics approval should apply whenever health data is being used without individuals' consent. As discussed at the teleconference, there may also be circumstances where ethics approvals is best practice notwithstanding that individuals have provided consent.

The privacy protections that apply to de-identified data that has been integrated with other data sets will also be substantially reduced by the data sharing scheme. In our earlier submission we compared the proposed standards with the current requirements in the Data Integration

Partnership (DIPA). As noted in the table below, all the comparative weaknesses still apply in the Data Availability and Transparency Exposure Bill.

Data Integration Partnership for Australia (DIPA)	**Data Availability and Transparency Bill**
Integration must be by an authorised data integrating Authorities – the Australian Bureau of Statistics or the Australian Institute of Health and Welfare Linked health data must be anonymised using best practice privacy preserving linking methods with the technical assistance of Data61.	The **data principle** requires that "appropriate protections are applied to the data". Unless this is specified in rules made under section 28 (Engage ADSP for prescribed data services), data custodians can choose to undertake integration or de-identification in-house. While the Data Commissioner can make recommendations under section 97, 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 entity to outsource, but only where the Data Commissioner is satisfied that this is "necessary to properly address an emergency or high-risk situation" (section 98). This is a high bar.
Linked data must be used in secure environments such as a virtual data centre.	The **setting principle** requires that "data is shared in an appropriately controlled environment". There are no minimum requirements for specific types of data, such as linked data or health data. While the Bill includes provision for data codes, there is no requirement for these codes to be in place prior to the commencement date. The AMA notes also that section 8(e) specifically contemplates that data may be "shared with or through accredited entities by means of electronic communications". Paragraph 28 of the draft Explanatory Memorandum defines this as "transfer of information via the internet or a telecommunications network". It suggests that "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". This appears to be encouraging the sharing of data by email, Dropbox and other unsecure means where the sharing would not otherwise fall within a Constitutional head of power.

Role 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.

This conflict will be most apparent if an agency seeks advice from the Data Commissioner prior to entering into a data sharing agreement. Paragraph 46 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."*

There is the potential for a conflict between the two roles both:

- At the time the Data Commissioner is advising the agency – as the Data Commissioner is tasked with both promoting sharing and promoting safety.
- If data is subsequently re-identified or a complaint is made – the Data Commissioner will be investigating a data sharing agreement that they advised on.

We note also that section 41(1)(e) contemplates that the rules may confer additional functions on the Data Commissioner. What kind of additional functions are contemplated and what assurances are there that these will not detract from the Data Commissioner's responsibilities for ensuring that data security is maintained?

Data sharing agreements not subject to review before finalised

As noted above, the data sharing scheme devolves decision making to data custodians. While section 18 requires that data sharing agreement include mandatory terms and that data sharing agreements be lodged with the Data Commissioner (section 32), there is no power for the Data Commissioner to:

- Approve data sharing agreements prior to finalisation; or
- Require amendments to data sharing agreements in order to improve privacy protections.

As noted above, the Data Commissioner also has very limited power to require that agencies engage external expertise.

This assumes that data custodians will have deep data set knowledge and the technical expertise to deliver best practice privacy protections. As noted in our previous submission, 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.

Complaints, redress and merits review

The complaint mechanism in Part 5.3 of the Bill is restricted to current data scheme entities (or entities that ceased to be data scheme entities in the previous 12 months). This means individuals about whom the data relates cannot complain to the Data Commissioner if information about them was released in an identified form without their consent, or in a more likely scenario the terms of the data sharing agreement (particularly Item 7) were inadequate, and an individual became identifiable after the data was released. Paragraph 54 of the draft Explanatory Memorandum notes that a person "may also complain about government activities to the Commonwealth Ombudsman, or to the Australian Information Commissioner 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 (unless there was a breach under another APP like APP 11) and they will have no grounds for complaint (including under the proposed new tort). They will also have 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, and members of the public are unlikely to understand them or utilise them.

Paragraph 55 of the Explanatory Memorandum also states that the "Bill also supports a 'no wrong door' approach by empowering the Commissioner to transfer matters and information to other regulatory bodies, such as the Australian Information Commissioner." However, as noted above, there is no ability for individuals to lodge complaints with the Data Commissioner and, subject to whistle-blower legislation, they will have no statutory protections if they do so.

More generally we are concerned that the process for data scheme entities to make complaints is highly regulated. In particular:

- The complainant must "reasonably believe" that another entity has breached the Act. 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 397 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. 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

88(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.

Penalties

Breaches of section 135A of the *National Health Act 1953* (**National Health Act**) and section 130 of the *Health Insurance Act 1973 (***Health Insurance Act***)* are currently criminal offences. The AMA appreciates that under the 'rebound provisions' these provisions would be reinstated if data custodians share health information in a way that is not authorised by section 13(1). However:

- Agencies are responsible for determining whether the five sharing principles have been met.
- Except for the outputs principle (which simply requires that outputs have been agreed), the sharing principles are subjective. In each case, they require that something be "appropriate".
- There is no provision in the data sharing scheme for merits review of an agency's decision to share or the terms of the data sharing agreement.

Accordingly, unless an agency had no regard to the data sharing principles or failed to complete and lodge the template data sharing agreement, 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 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.

Definition of release

The AMA's understanding was that the focus of the legislation would be on sharing. However, there are a number of references to release. In particular:

- Section 9 defines release as providing open access to data.
- Item 10 of the data release agreement allows the accredited user to release the output in specified circumstances that meet the requirements set out in section 20(3).
- Section 20(3) allows an accredited user to release output in circumstances specified in the data release agreement if releasing the output in those circumstances does not contravene a law of the Commonwealth or a State or Territory.
- Section 113(2)(b) contemplates that the guidelines issued by the Data Commissioner may include principles and processes relating to data release.

Output released by an accredited user in accordance with subsection 13(3) exits the data sharing scheme at the time it is released (section 20(4)).

We understand that this provision is intended to refer to release under existing schemes, particularly the Privacy Act or the information publication scheme in the *Freedom of Information Act 1982*. For example, a researcher may publish a paper that includes charts based on de-identified data.

We note that the Bill does not introduce any additional penalties for unauthorised release. This is on the basis that any penalties would be under the authorising legislation (ie, the Privacy Act etc).

Sharing of identified data with individuals or businesses (pre fill)

We note also that, while the previous consultations focused on de-identified data, the Explanatory Memorandum contains a number of references to highly identifiable data. In particular:

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 48	The definition of output is "an inclusive term to cover a range of results and products that incorporate or are founded upon the shared data such as an integrated dataset, tables or graphs of statistical information, an algorithm, a pre-filled form compiled using shared data, and a research paper or policy proposal. Outputs are subject to ongoing controls under the data sharing scheme, unless they exit the data sharing scheme under clause 20."
Paragraph 77	"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 107	"Data sharing under [section 15(1)(a)] 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 details like a tax return. This purpose supports sharing for services delivered by or on behalf of government, such as through contractors."
Paragraphs 181 and 182	"The exit mechanism in subclause 20(1) is intended to support the use of outputs created for permitted purposes in clause 15 – particularly government service delivery for which accurate, up-to-date information is essential. 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. The focus of subclause 20(1)(b) on individuals' and businesses' control and active validation of

	their data is consistent with the privacy-positive approach of this Bill, and supports a user-centric model of service delivery. Where the output relates to an individual, the accredited user may alternatively provide access to the individual's responsible person (e.g. parent or guardian), within the meaning of the Privacy Act, for validation or correction (refer subclause 20(1)(b)(ii)). This approach maintains processes and safeguards in existing frameworks to facilitate efficient government service delivery, while ensuring personal information is not provided in a manner that jeopardises the safety or welfare of the individual."

We understand that these provisions have been included to facilitate the use of public data for government service delivery. In line with this section 20(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 and query whether the agencies concerned are prosecuting this inclusion.

One option would be for the data sharing scheme to specify types of data (eg MBS and PBS) that cannot be released under the pre-fill mechanism.

Regulations

We note that aspects of the PSR scheme and provisions of the *My Health Record Act* have been listed in the Regulations. As noted above, 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.

Data Code

Previously data codes were expected to be a key part of the scheme. However, data codes are only referred to in:

- clause 34(b)(iii) – prescribed event which constitutes a data breach;
- clause 37(1) – prescribed requirements for notifying data breaches; and
- clause 75(3)(c) – prescribed requirements for complaints

Paragraph 569 of the Explanatory Memorandum says that the data codes could include:

> *"prescribing how to apply the Data Sharing Principles in different situations, such as when sharing via an ADSP, or assess requests against the data sharing purposes. Use of data*

codes in this manner will clarify core requirements for sharing, and standardise their application by data scheme entities."

Is the Data Commissioner intending on issuing a data code and, if so, when will a draft be circulated to stakeholders?

Guidelines

The Data Commissioner may also issue guidelines (section 113). Data scheme entities must comply with the rules and data codes (section 25) and "have regard to" the guidelines when sharing data (section 26). As noted in our teleconference discussion on 22 October, we are concerned that that there is no requirement to comply with Guidelines or keep a record of the reason why Guidelines were not complied with.

The only provision of the Bill referring to the content of the Guidelines is section 113 itself. It provides that:

"(1) The Commissioner may make written guidelines in relation to matters for which the Commissioner has functions under this Act.

(2) The guidelines may include principles and processes relating to:

(a) any aspect of the data sharing scheme; and

(b) any matters incidental to the data sharing scheme, including:

(i) data release; and

(ii) data management and curation; and

(iii) technical matters and standards; and

(iv) emerging technologies."

According to paragraphs 213 and 576 of the Explanatory Memorandum

"The guidelines will explain expectations and best practice for how the data sharing scheme should operate. Requiring entities to have regard to these guidelines is important to build data management capacity and enhance voluntary compliance with this scheme.

The Commissioner will use guidelines to support best practice and to provide information about how the data sharing scheme operates.

Guidelines will help to build capacity in the data sharing scheme and data system more broadly."

Is the Data Commissioner intending on issuing guidelines and, if so, when will a draft be circulated to stakeholders?

Other issues

Section 8 – The AMA has real concerns about how this provision is intended to operate in practice given that it means that the entire Act will not apply unless the data sharing falls within one of the paragraphs. Will educational resources or guidance be available to data custodians to explain the operation of this Clause?

Section 8(c) – Is a university a constitutional corporation (ie, a corporation to which paragraph 51(xx) of the Constitution applies? If not, it appears to us that the only way an Australian university researcher could be authorised to receive data (other statistical data) from a data custodian under the data sharing scheme for a non-Commonwealth government purpose (other than a statistical purpose), is if the data is sent via an electronic communication (eg email or Drop-box). This is complex for data custodians to understand and creates absurd results. In particular, it applies different sharing pathways depending on the identity of the recipient and the purpose of the sharing.

Section 8(e) – As noted above, particularly where data sharing is not for a Commonwealth purpose or is not with a Constitutional corporation, there appears to be a strong incentive to use email or the internet to share the data. This is because nothing in the Act prohibits this and a data custodian that shares outside section 8 of the Act may find themselves committing a criminal offence under the original legislation. The AMA suggests that either section 8(e) be deleted (to remove this incentive) or the data sharing scheme set out situations where sharing by email or via the internet is not permitted. 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.

Section 15 – As noted above, the definition of data sharing purposes is very broad. Paragraph 110 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 health information (particularly MBS and PBS data) to be shared with health funds outside the existing statutory schemes. The AMA recommends that this be prescribed in the rules as a precluded purpose (section 15(2)(c)).

Sections 16(1)(d) – This section requires that the data custodian "considers" using an ADSP to perform data services in relation to the sharing. We understand that this decision is subject to judicial review. We suggest that it also be subject to merits review.

Section 20(1)(b)(iii) – This provision allows the Rules to specify additional circumstances where the output may be shared. What kind of circumstances are contemplated here? Paragraph 183 of the Explanatory Memorandum says that this is to "ensure the Bill can respond to future needs while maintaining data custodian oversight of the process".

Section 22 – Paragraph 203 of the Explanatory Memorandum states that this "clause ensures that custodians follow due process to consider requests that appear appropriate and made in good faith, before accepting or rejecting those requests". We understand that these decisions – particularly any decisions not to share – are subject to judicial review.

Section 27 – We note that data sharing with small businesses and government entities from Western Australia and South Australia is prohibited unless those entities agree to comply with the Privacy Act in accordance with the statutory process set out in the Privacy Act. We understand that sections 73 and 74 will be amended so that this is part of the accreditation process (ie, these entities will not be able to be accredited unless and until they opt in.)

Section 28 – As noted above, the AMA recommends that the rules require that all data custodians (other than ABS, AIHW and other specified bodies) be required to outsource de-identification and other high-risk activities.

Section 30(2) – This subsection allows the rules to prescribe circumstances where an event or change in circumstances that affects the entity's accreditation does not need to be reported. What kind of rules are contemplated here? No examples are given in the Explanatory Memorandum and no explanation has been given as to why the obligation to report would be watered down.

Sections 73 and 74 – We understand that these provisions will be amended to incorporate the minimum requirements for accreditation into the Act. We agree with this approach.

Sections 18 and 123 – Section 18 requires that a data sharing agreement be entered into by an authorised officer. There is no requirement in the Bill for an authorised officer to hold a minimum level of seniority (eg SES or equivalent). Given the risks to the public, we recommend that the data sharing scheme require a minimum seniority for sharing of health information, particularly MBS and PBS data.

Conclusion

After a close examination of the detail in the Bill, the AMA considers it does not afford a level of privacy protection for personal data and, in particular sensitive health data that is equivalent to the protections in the Privacy Act and, for MBS and PBS data, the *National Health Act* and the *Health Insurance Act.* The AMA continues to recommend that, at least in the short term, the Regulations exclude health data. The most significant reasons for this conclusion are detailed throughout this submission. In particular:

Section 8(e) – There is the real potential for email or internet to be favoured as a sharing mechanism in order to ensure the data sharing scheme will apply where data is being shared with a State entity or a university. This introduces an unacceptably high risk that personal/and or health data will be intercepted or stolen by a third-party during transmission.

a. **Weak consent protections** – While consent provisions have been added, consent is not required where it would be impracticable. In a large dataset it is impractical to obtain the consent of every person about whom the data relates prior to sharing this data. In our view, ethics approval should be mandated prior to the release of identified or identifiable sensitive health data whenever consent is not obtained.
b. **Sharing with private sector entities for non-public purposes** - The Bill allows sharing with a wide range of entities for a wide range of purposes. As currently drafted, it would allow 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, the Health Insurance Act 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.

8 December 2020

[redacted]