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 Sharing and Release Legislative Reforms

datalegislation@pmc.gov.au

The AMA welcomes the opportunity to comment on the Data Sharing and Release Legislative Reforms Discussion Paper.

The AMA values the importance of health research and notes the examples of beneficial research outlined in the discussion paper has been conducted under existing patient privacy protections. The pursuit of research using sensitive health data, however, should not be prioritised at the expense of patient privacy. This is not to say the AMA opposes out-right the proposition in the Data Sharing and Release Legislative Reforms Discussion Paper. Rather, we consider the Sharing and Release Framework requires much more work before it provides ***certain*** and *sufficient* privacy protections for health data that is used for secondary purposes.

The AMA notes My Health Record data will be exempt from the Data Sharing and Release legislation. The AMA recommends that, at least while the new framework is being bedded down, the secrecy provisions in the *Health Insurance Act 1973* and the *National Health Act 1953* also be exempted.

The reasons for this are discussed further below.

Current position

Currently section 135A of the *National Health Act* and section 130 of the *Health Insurance Act* prohibit Commonwealth officers from disclosing information collected under that legislation unless expressly authorised by that legislation. Breach of these provisions is a criminal offence.

The Privacy Commissioner has issued *National Health (Privacy) Rules 2018* under section 135AA of the *National Health Act*. Rule 12 provides that:

> *(1) Claims information that identifies an individual may only be disclosed for medical research if:*
>
> *(a) the Department of Human Services is satisfied that the individual to whom the information relates has given their informed consent to the use of that information in the research project; or*

(b) 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 1988.

(2) Before disclosing claims information under section 12(1), the Department of Human Services must obtain a written undertaking from the researcher that the claims information will be securely destroyed at the conclusion of the research project.

Similarly, section 130(3) of the *Health Insurance Act* allows Medicare to disclose information to a third party without the patient's consent:

if the Minister certifies, by instrument in writing, that it is necessary in the public interest

New framework

Under the proposed approach, these statutory secrecy provisions would be overridden by a new principles-based framework that:

- applies the same Data Sharing Principles to the secondary use of all Commonwealth government regardless of its sensitivity; and
- delegates decision making power to Departmental officers.

This means that the degree of privacy protection will vary case by case, according to the skill and knowledge of the departmental officer(s) responsible for developing the data sharing agreement.

For some government data wrong decisions may have no negative consequences, but for health information the consequences are serious.

Five safes principles

A key component of the new framework is 'privacy by design' guided by the five safes principles.

The first safe principle is that the research must be for at least one of the following purposes:

A purpose that is research to advance knowledge, contribute to society and create better public policy;

A purpose that related to planning for government policy and programs in the future;

A purpose related to improved public access to their own data and services the government provides to individuals.

The remaining four safes principles require the data custodian (ie, the department) to assess and design a data sharing agreement that takes account of:

People – *Data is only available to authorised users.*

Setting – *The environment in which the data is shared minimises the risk of authorised use or disclosure.*

Data – *appropriate protections are applied to the data (includes data minimisation where only the minimum amount of data required for the proposed research question is released)*

Output – *outputs are appropriate for further sharing or release*

While the five safes principles have the *potential* to protect sensitive identified 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 safes principles have been met.
- The first five safes (the purpose test) is very broad and the remaining four safes sharing principles are subjective.
- The Data Sharing and Release Framework and the Data Commissioner are intentionally biased in favour of sharing.

This means that, so long as a department had regard to the Data Sharing Principles, it would be difficult in practice to prove that its decision was unlawful. Identified sensitive MBS and PBS data could be shared with any researcher approved by the department for any purpose providing the research applicant is, or becomes accredited, and can demonstrate the research project has an approved purpose.

Comparison with existing health information protections

Under the new framework there is no requirement for individual consent before identified health data is disclosed and shared with researchers or private sector organisations. While the National Data Commissioner can issue guidance and advice about when and how consent should be built into the Data Sharing Principles, there is no requirement this guidance will be binding.

Unlike the guidelines issued under section 95 of the Privacy Act[1], the new framework does not require ethics approval before identified health data is shared and/or integrated with other data sets without the patient's consent.

A comparison with the Data Integration Partnership for Australia (DIPA) indicates privacy protections applied to de-identified data that has been integrated with other data sets will also be reduced under the Data Sharing and Release framework.

[1] Available from https://www.nhmrc.gov.au/about-us/publications/guidelines-under-section-95-privacy-act-1988

Data Integration Partnership for Australia (DIPA)	Data Sharing and Release framework
Integration must be by an authorised data integrating Authorities – the Australian Bureau of Statistics or the Australian Institute of Health and Welfare	Data can be shared with any accredited researchers or private sector organisations approved by the data custodian who enters in a data sharing agreement. Subject to the Rules, data can be integrated with other data sets by any accredited data service provider.
Linked health data must be anonymised using best practice privacy preserving linking methods with the technical assistance of Data61.	The data custodian can undertake de-identification in house unless the data custodian determines that it is a high risk integration.
Linked data must be used in secure environments such as a virtual data centre.	Security arrangements are determined by the data custodian.

Rules and Data Code

The AMA appreciates that, while the new framework is 'one size fits all':

- The Minister will make rules which govern accredited data users and data service organisations.
- The National Data Commissioner will develop a Data Code on handling sensitive information, including identified personal information[2].

However, the Rules and Data Code have not yet been released and will not be finalised until after the proposed Data Sharing and Release bill becomes law.

It is also foreseeable that, after the legislation commences, new issues will come to light that need to be addressed in future iterations of the Rules and Data Code. Preferably these issues would be 'ironed out' before the new scheme is extended to health information.

It is also worth noting that the Rules and Data Code will set out general rules rather than project specific requirements. By contrast, ethics approvals are granted on a case-by-case basis so can include additional protections to mitigate against project specific risks.

Role of the Data Commissioner

As noted above, the new framework devolves decision making to data custodians. This assumes that data custodians will have deep data set knowledge and the technical expertise to deliver best practice privacy protections. The well-publicised privacy breaches involving Medicare

[2] Page 40

provider numbers[3] and MyKi travel information[4] demonstrate well-intentioned officers may not be trained to appropriately anonymise personal information.

While the new framework will be overseen by the Data Commissioner, their remit is to encourage release (open access) of government data as much as possible. The expectation is that adherence to the five safes principles of safely sharing data will be largely achieved via education and ***non-binding*** Guidelines. The Data Commissioner does not have power to:

- overturn decisions to share (so long as the data custodian has applied the Data Sharing Principles);
- require data custodians to engage experts to undertake de-identification; or
- require specific projects to implement a higher standard of compliance with the five safes principles.

Given this, it is not clear how the Data Commissioner will be able to ensure that the framework is:

> *applied in a manner that is a reasonable, necessary and proportionate use of the 'authorised by law' provisions in the Privacy Act 1988*[5].

The AMA is also concerned about the potential conflict between the Data Commissioner's two roles, namely:

- to encourage government agencies to share personal information; and
- to consider whether decisions to share were appropriate.

Penalties

As noted above, breaches of section 135A of the *National Health Act* and section 130 of the *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 in accordance with the purpose test or the Data Sharing Principles" (page 47). However, as discussed above:

- Agencies are responsible for determining whether the five safes principles have been met.
- The first five safes (the purpose test) is very broad and the remaining four safes sharing principles are subjective.

Accordingly, unless an agency had no regard to the Data Sharing Principles, 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.

[3] https://www.oaic.gov.au/privacy/privacy-decisions/investigation-reports/mbspbs-data-publication/
[4] https://ovic.vic.gov.au/wp-content/uploads/2019/08/Report-of-investigation_disclosure-of-myki-travel-information.pdf
[5] Page 32

Similar issues apply to the proposal that the sharing no longer be "authorised by law" (and hence no longer protected by Australian Privacy Principle 6.2(b)) if a data custodian "fails to apply" the Data Sharing Principles (page 32).

More generally, there needs to be greater clarity regarding:

- how any new penalties will be applied to breaches by government agencies;
- what mental and physical elements need to be established; and
- the remedies available to individuals whose privacy has been breached.

Public expectations in relation to health information

The public expect that the Commonwealth will keep their health data confidential and secure. This message was very clear during the passage of the My Health Record opt out legislation. In light of this, the government has recognised the need to exempt My Health Record from the new framework.

MBS and PBS data held under the *Health Insurance Act 1973* and the *National Health Act 1953* is essentially the same data as My Health Record but held in a different data set. It does not make sense to acknowledge the sensitivity of this data when held in My Health Record but to lower the threshold for MBS and PBS data.

While MBS and PBS data is owned by the Commonwealth, it is sensitive information and the public rightly expect that it is used carefully. For example, patients receiving treatment for bi-polar were shocked and angry that the Department used PBS data to send them targeted letters inviting them to participate in research related to their disease. While ethics approval had been obtained, more could have been done to ensure that letters were not inadvertently opened by other household members or third parties (where old addresses were used).

If Australians lose confidence in the privacy protections applied to identified sensitive health information, there is a very real likelihood patients will not seek medical treatment. This is a particular risk for mental conditions where patients still face increased discrimination in seeking employment and insurance.

Conclusion

The proposed Data Sharing and Release legislation provides substantially less protection for MBS and PBS data than the statutory secrecy provisions in the *National Health Act 1953* and the *Health Insurance Act 1973*. The AMA welcomes the exemption of My Health Record information from the proposed Data Sharing and Release Framework because the community does not support it. The same MBS and PBS data stored in a different data set should also be exempt – at least in the interim until protections for health data of a similar standard to current protections have been built into the new Data Sharing and Release Framework. These include:

- the establishment of robust and binding Rules and Data Codes in respect of health information, for ethics approval in relation to release of identified health information;

- the adoption of best practice anonymisation technologies applied to de-identified data prior to release to prevent new privacy breaches via re-identification;
- appropriate training for officials or a requirement all data sharing agreements are approved by data anonymisation and data environment experts such as NHMRC or AIHW;
- appropriate and enforceable penalties and remedies.

Alternatives

The AMA recognises the value of research to improve health policy, service delivery, efficiency. We recognise the urgent need to find affordable solutions to supply patients with the non-admitted health services needed to reduce hospital admissions. However, as demonstrated by the DIPA research and all the other examples of valuable health research mentioned in the discussion paper, this type of health research is already possible within existing privacy laws and statutory secrecy provisions.

Although the Data Sharing and Release Framework, in its current form is not yet suitable to protect patient privacy when sensitive health information is shared for a secondary purpose, while adjustments are made to the Sharing and Release Framework, the AMA is open to a discussion with the Department of Health about how the existing statutory secrecy provisions might be streamlined to facilitate research but retain important patient protections such as consent and/or ethics approval.

OCTOBER 2019

Contact

Leonie Hull
Senior Policy Adviser
Medical Practice
Ph: (02) 6270 5487
lhull@ama.com.au