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 Framework for the secondary use of My Health Record Data

The AMA welcomes the opportunity to comment on the secondary use of My Health Record data. The AMA is a strong supporter of the shift to digital health records. The consolidation of patient information in digital form will allow treating doctors to access clinically relevant data at the time of diagnosis or treatment. This creates an opportunity to improve the safety and quality of medical care and maximise the efficient use of resources.

The AMA recognises the My Health Record data set will be useful for purposes other than direct patient treatment. The data set will become an important and valuable asset because it will give a single source, clear line of sight into the health service utilisation of each patient across the primary and tertiary sectors. It will offer opportunities to see patterns and trends in health conditions and service utilisation. It will create opportunities to quickly identify patients who might benefit from participation in approved new drug trials, or patients who might be adversely affected by TGA initiated drug or prostheses recalls. The data set will be of equal interest to health researchers, government and commercial entities with a vested interest in the health sector.

Our clinician members recognise the positive opportunities the new My Health Record data set will create. However, clinicians are also acutely aware of their role in protecting the privacy of their patient's health data – a large part of which is created by our members in the process of providing their patients with high quality healthcare.

Our reading of the My Health Record Act 2012[1] [2] and its intersection with privacy law, suggests the Framework document bears the full responsibility for setting the parameters and circumstances in which the disclosure of de-identified My Health Record data for secondary purposes can occur. This confers on the Framework, a substantial responsibility to strike the right balance between secondary disclosure for public good on the one hand, and protecting patient privacy and integrity of the My Health Record system on the other hand.

Given the complexity of the laws affecting the use and disclosure of very sensitive health data, it is the AMA's firm belief the Framework document must be a disallowable instrument to ensure appropriate parliamentary oversight.

[1] *My Health Records Act 2012*, Division 1 Part 2, s17(ma)
[2] *My Health Records Act 2012*, Division 2 Part 4 s67

Failure to strike the right balance will undermine patient and medical practitioner confidence in the My Health Record and negatively impact their willingness to participate. This outcome will be counter to the logic of shifting to opt out and will undermine the primary purpose of the My Health Record – to improve patient outcomes via access to the right clinical information at the right time to inform patient diagnosis and treatment.

Australians are equal stakeholders in the My Health Record system – it is the management and secondary disclosure of their sensitive health data under discussion in this consultation paper. Notwithstanding decisions individuals may make about the type of personal information they decide to post on social media, or share publically, Australians are likely to expect their health data collected by Government in the process of using a health service will not be shared with a third party - unless they know about it and they have consented to it. Or if they have not consented, they know their data will not be released as open data but only when de-identified and only in controlled situations so there is no probability their health data could become re-identified if linked with other publicly available data. Over-riding all this is that the information would only be used for public good. The AMA considers it is vital that de-identified health data is protected from re-identification, misuse or personal gain by individuals or organisations with vested interests – commercial or criminal.

If the government wants to build community trust in the My Health Record system and the intended use of data for secondary purposes, the AMA questions the timing of this consultation process so soon after the media coverage of the fraudulent access to Medicare information that was made available illegally on the 'dark web'.

The AMA also queries why stakeholders are being asked for their views on the secondary use and disclosure of My Health Record data ***before*** the release of the revised My Health Record Rules and the Privacy Impact Assessment on opt out arrangements. Any details in these two documents that substantially impact stakeholders views of the use and disclosure of My Health Record data would seriously compromise the validity and authority of this consultation process.

It is the AMA's strong view the Office of the Australian Information Commissioner (OAIC) is given the opportunity to comment on a draft Framework before it is finalized to ensure only entities who are subject to the My Health Record Act and Australian privacy laws can access My Health Record data for secondary purposes. Indeed a full privacy impact assessment on a draft final framework should be conducted as part of due diligence.

The AMA recommends that once the final Framework is decided, but before it takes effect, a separate additional communication campaign is undertaken to ensure all Australians understand the effect of the government's intended secondary data disclosure. This is especially important for the early adopters into My Health Record who agreed to participate on the basis their data would not be used for secondary purposes.

The AMA recognises communicating this message en-masse will be difficult. But it will be vital to maintain the social contract needed to underpin wide spread participation in the My Health Record – patients and health providers. All Australians will need to be reassured their My Health Record data will be kept secure and their privacy will *not* be breached and the purposes for

which the data will be disclosed will not serve vested commercial interests but instead used only for the public good.

The AMA also recommends participants in the My Health Record should have a choice to opt out of disclosing their sensitive health data for the purpose of secondary research – at any point in time. An individual's sensitivity to participation could change with the unanticipated onset of a health condition(s) or other social factors. This means the My Health Record data custodian will need to keep Australians informed whenever the parameters or principles of the Framework change.

The AMA response to specific consultation questions follows.

Question 1: What secondary purposes if any, should My Health Record data be used for?

The AMA considers the use, disclosure and linkage of data held in the My Health Record database must be limited to research that exclusively aims to improve the health of patients - health policy analysis, health service program development and delivery, best practice health care, public health initiatives and the identification of unmet health service demand. The AMA is opposed to using My Health Record data for the purpose of improved 'safety and quality' of healthcare while-ever this label continues to be used by the Commonwealth to justify funding cuts to our already chronically underfunded public hospitals. Overall, My Health Record data should only be disclosed if the privacy risk has been minimized.

It should not be used for compliance or audit purposes – the Professional Services Review is the appropriate mechanism for this.

Question 2: What secondary purposes if any, should My Health Record data not be used for?

My Health Record data should never be used:

i. To monitor, interfere with or control doctor's clinical decision making;
ii. To limit or determine doctor's remuneration;
iii. To enable performance management of individual doctors;
iv. To establish pay-for-performance systems;
v. To serve vested commercial interests - including health insurers, pharmaceutical companies, and device manufacturers;
vi. In a way that allows sensitive health data that has been de-identified and disclosed in one setting to become re-identifiable in a different data environment.

Question 3: What types of organisations/individuals should be able to access My Health Record data for secondary purposes?

The AMA is not sure if a fully defined list of organisations/individuals can be identified in advance as 'safe users' of sensitive My Health Record data but should be limited to governments and university researchers who are working on their behalf for public benefit. My Health Record data should never be released for commercial purposes either immediate or

downstream. Each application should be exposed to a rigorous assessment of their research purpose and design, plus where relevant, checks on reputation and criminal history.

Question 4: Should access to My Health Record data for secondary uses be restricted to Australian users only or could overseas users be allowed access?

The AMA does not support the disclosure of My Health Record data to an overseas user. Overseas entities are not subject to Australian law, there is no way Australia could monitor the secure storage of the data, whether the data user complies with the conditions of data release and destroys the data after use. There is also no realistic way to prevent the data recipient from passing the data to other parties. This restriction would not necessarily limit collaboration between highly regarded Australian and international health and medical research teams. But it does mean My Health Record data should not be downloaded by an off-shore entity/ researcher.

Question 5 – What principles, if any, should be included in the Framework to guide the release of data for secondary purposes from the My Health Record system?

The principles need careful consideration. Health data is personal and sensitive. Each disclosure decision must consider the data situation and be assessed against the public interest purpose to be served by disclosure. Data 61 describe a *data situation* as the relationship between data and its environment[3]. The authors identify 4 components to each data situation: (i) **Other data** in the data environment – overlap and connection to My Health Record data. (ii) **Agency**: who is capable of acting on the data in the data environment? (iii) **Governance processes**: How will the users' relationship with the data be managed? (iv) **Infrastructure**: How do infrastructure and wider social and economic structures shape the data environment?

Given the high risk and high complexity of assessing these criteria for each disclosure decision, the AMA considers it would be prudent and efficient if the disclosure principles had the following characteristics:

1. A single decision making body that:
    i. Is a health data expert, with demonstrated experience and knowledge of Australian privacy law, health legislation and experience managing decisions about the disclosure of sensitive Australian health data sets.
    ii. Reports to the Australian Parliament and subject to senate estimates scrutiny.
    iii. Is required to publicly list all disclosure decisions.

2. Each disclosure request is assessed on its merits and only granted if there is a clear public interest.

[3] CM O'Keefe, S Otorepec, M Elliot, E Mackey, and K O'Hara (2017) The De-Identification Decision-Making Framework. CSIRO Reports EP173122 and EPI75702.

3. De-identified data is only released if it complies with existing laws that govern the disclosure of government held health data or according to the Five Safes Principles with the following modifications:

   De-identified data is only released:
   i. to 'safe' people (data applicant is assessed as trusted to use the data in an appropriate manner.)
   ii. for a 'safe project' (data will be used for a lawful/public interest purpose)
   iii. in a 'safe setting';
   iv. for a single defined use;
   v. only if the permitted disclosure is time limited;
   vi. only if there is a mechanism to guarantee disclosed data is destroyed after use.

4. Identified data is only released:
   i. with the same caveats as (2) & (3) above; and
   ii. with express, fully informed consent of affected patients;
   iii. following approval by an Australian human ethics committee;
   iv. in a way that does not allow the identification of individual medical practitioners.

A 'safe setting' may be either:

a) Permitted data interrogation of de-identified My Health Record data sets in a controlled premise –all outputs checked to protect against privacy breach prior to release; or
b) release of My Health Record data to accredited researchers via a Secure Unified Research Environment (SURE) – after it has been de-identified. The AMA understands this approach does not allow researchers to download My Health Record data so it removes the risk de-identified data becomes identifiable in this other data environment.

It may be appropriate to consider enforcement penalties if data access is granted and conditions of access are breached. The development of a robust, practicable and implementable compliance process should form part of this Framework paper. The development of a Framework will have little effect if conditions of access are breached without repercussions.

Our overall position may seem cautious but our comments recognise the sensitivity of the data held in the My Health Record and the technical difficulty of de-identifying health data in a way that removes virtually all risk the data, in a new environment, becomes re-identifiable. The AMA notes the Information Commissioner reached a similar conclusion in his submission on the Productivity Commission Draft Report on Data Availability and Use[4].

> *It is very unlikely high value datasets containing sensitive health information can be sufficiently de-identified to enable general, open publication (in a manner that also preserves the integrity of that data).*

[4] 'Data Availability and Use – OAIC submission to Productivity Commission Draft Report', p4 OAIC, December 2016

Disclosure in a controlled, safe setting would maximise the use of My Health Record data for public good and reassure Australians and medical practitioners that participation in the My Health Record does not expose them to security or privacy risk.

Question 6: Which of the governance models described in the Framework paper should be adopted to oversee the secondary use of My Health Record data?

The sensitivity of health data, combined with the complexity of privacy legislation, health legislation and the large number of separate health data sets held by governments (Commonwealth and State) and health insurers, suggests the most appropriate governance option is a single governing body. This body must be accountable to the Australian Parliament.

This would give a single authority a clear line of sight into all My Health Record data disclosure decisions and add to the transparency and accountability for these. It goes without saying the single governing body must be of high integrity and a health data expert organisation with expertise in health data disclosure management – eg the Australian Institute of Health and Welfare (AIHW).

It is paramount the secondary use and disclosure guidelines that apply to My Health Record data are consistent with existing legislation that applies to various data subsets within the My Health Record. For example, the National Health Act 1953 Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs[5] that govern the use, disclosure and linkage of MBS and PBS data. Failure to implement a consistent approach across all My Health Record data subset custodians would mean a request to access My Health Record data that is rejected by the My Health Record data custodian, could be circumvented if the data subsets are separately available via subset data custodian release processes – or vice versa.

Questions 7 & 8 What principles, if any, should be included in the Framework to guide the release of de-identified and identified data for secondary purposes from the My Health Record System?

As per our response to Q5, the AMA considers the My Health Record data to be high risk and in need of maximum disclosure protection. This offers the greatest potential to capture the research insights from My Health Record data without compromising My Health Record data security/privacy.

The process to manage requests and approvals for data release need to be equally rigorous. The AMA is inclined to support a disclosure request process like the AIHW model described on page 11 of the Framework paper. Data requests are made via a custom web-based form. This has the advantage of allowing the AIHW, or similar government body, to specify the information

[5] National Health Act 1953 - Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs in force 13 November 2017 https://www.legislation.gov.au/Details/F2008l00706

needed to understand the research design parameters and assess risk to patient privacy and the public benefit of the proposal. Conversely, the email application process used by DHS for access to MBS or PBS data seems open to inefficiency and potential errors of judgment according to the detail a researcher/applicant happens to include in their initial email request.

The AMA also supports the use of an internal data committee to assess My Health Record data requests. Consultation with the data subset custodians is important because each disclosure decision will need to be considered in the context of the relevant legislated release/disclosure conditions that apply to the data subsets within the My Health Record.

If patient consent to release identified or identifiable data is requested this must be subject to human ethics committee approval. If approval is granted, the AMA recommends the appointed governing body [eg AIHW] oversees the patient consent process. Patient consent cannot be valid unless it is explicit, and given by the patient after a full, transparent explanation of how their identified health data will be used, stored, accessed and destroyed after use. Assigning oversight responsibility to the governing body will ensure the consent process remains accountable/transparent. This is as much a protection to the integrity and confidence in the My Health Record system as it is a protection for individuals.

The entity who requests patient consent to access identified health data should never be provided with the patient's contact details. Instead, the data custodians should write to the patient to invite them to contact the researcher if they wish to participate or find out more. Similarly, ethics approval should only be considered valid if it is granted by a known, respected ethics committee arms-length of the research team/requesting entity.

Question 9: Should there be specific requirements if researchers/organisations make a request that needs the My Health Record data to be linked to another dataset? If so, what should these requirements be?

Requests to link My Health Record data to another data set should always be subject to human ethics approval and only released to the data applicant in de-identified format after the data is securely linked by one of the three accredited integrating authorities. Use of the de-identified linked data should be subject to the same restrictions as identified data. That is access occurs using a secure on-site data laboratory or within the secure unified research environment (SURE) under a binding agreement of use.

Linked de-identified data should never be released as 'take away' data because it could become identifiable data in a different data environment. The AMA recognises there may be circumstances where linking My Health Record data to a database of clinical trial participants could prevent a foreseeable patient harm even though the data linkage exposes patient identity. Approval in these circumstances is a question for the relevant human ethics committees and should be considered case by case.

Question 10: What processes should be used to ensure the My Health Record data released for secondary purposes protects the privacy of an individual?

Covered in earlier responses.

Question 11: What precautions should be taken to reduce the risk of de-identified data from the My Health Record data base being re-identified after release?

Covered in earlier responses.

Question 12 & 13: What arrangements should be considered for the preparation and release of My Health Record data? Who should be responsible for assessing the quality of My Health Record data?

In line with our view that the My Health Record data is both sensitive and high risk, it would seem appropriate if the preparation and de-identification of the data was undertaken by a single health data expert entity such as the AHIW who is also responsible for all disclosure processes/decisions. Our view on the arrangements for the release of My Health Record data are covered in our earlier responses. We strongly prefer the options that limit release to a strictly secure, controlled environment such as a safe haven or restricted data platforms. The exact mechanism to guarantee data security/privacy is a technology question that should be informed by consultation with trusted ICT experts.

Consideration of questions 14-17 would become redundant if the cautious strictly controlled disclosure recommended by the AMA in this submission is adopted. On balance, in AMA's view it is likely more cost effective to completely control the data disclosure environment to remove all risk of privacy/security breach – than to adopt a 'take away' disclosure model that is open to misuse and is resource intensive to monitor/regulate post release.

The full cost of privacy/security breach is not only the possible harm to individuals who become identifiable, but a reduction in participation due to a loss of confidence in the My Health Record system – consumers and clinicians.