Response to Request for Comment

ON THE SECONDARY USE OF MY HEALTH RECORD DATA FRAMEWORK PROPOSAL

November 2017

Authored by Fellows and Members of the

Australasian College of Health Informatics

PO Box 125, GLEN IRIS 3145, Australia Secretary@ACHI.org.au www.ACHI.org.au

Index

About the Australasian College of Health Informatics

The Australasian College of Health Informatics (ACHI) [1] is the professional organisation for Digital Health and e-Health in the Asia-Pacific Region. ACHI sets standards for professional practice and education in Health Informatics, provides evidence-based guidance to jurisdictions, supports initiatives, facilitates inter-disciplinary collaboration and mentors the community.

The membership of the Australasian College of Health Informatics is diverse with representation across all fields of Health Informatics activity. Membership and Fellowship are predicated on proven substantial contributions to Health Informatics worldwide in the areas of education, position, achievement, research and development.

Our response

In responding to the Secondary Use of My Health Record Data Framework Proposal, ACHI have collated diverse opinion based on experience within Australia and Internationally. Our aim is to provide opinion that is biased only through demonstrated experience and knowledge in the areas of Health Informatics in general and of secondary uses of data in particular.

The College congratulates the Department of Health and the Australian Digital Health Agency in undertaking an extensive public consultation regarding this important issue and we look forward to the outcomes of this consultation being reflected in the implemented framework. Below are our principal thoughts and recommendations. We offer our services to ADHA and the Department of Health in this area going forward.

Executive Summary

We see the Secondary Use of My Health Record (MHR) data as being a fundamental component of My Health Record with huge opportunity to drive quality assurance, quality improvement, audit, research and surveillance to improve population health outcomes and reduce health system costs.

To drive these health and financial aspirations, the MHR systems must have comprehensive data content, data quality and utilisation. The college recognises that the MHR is at the early adopter stage of implementation and the systems are at an early stage in the product lifecycle. These facts should not detract from taking a long-term view regarding how the secondary uses of data should be accommodated – further – a long view is a necessary foundation for long-term success.

A governance framework will need to be employed at the earliest opportunity. The college recommends that any initial governance model implemented under the framework be implemented as a transition step whilst a comprehensive future-aware model evolves.

Maximising the benefits of My Health Record will require extensive secondary uses of data and extensive data linkage. As a result of trust and agility issues, achieving this to the full extent will be hard to achieve using fully centralised systems of governance, data curation and linkage.

Looking internationally, social values, government and health system structures impact on the approach that can be taken. A model that members have seen as potentially applicable to Australia is that of Canada via the Institute of Clinical Evaluative Sciences (ICES) [2]. ICES is one of the leading and most respected institutes for secondary uses of data with three components to its success being: 1: Independence from Government (subject to oversight and enshrined in legislation) 2: A distributed, accredited nodal structure allowing de-centralisation promoting agility 3: Effective accreditation mechanisms for ICES in general, nodes and users of the data.

With respect to the specific questions asked in this request for feedback, many questions relate to understanding what principles may apply to different components of managing access to My Health

Record data for Secondary uses. We believe Australia already has a well-established set of principles for the use of data for research embodied in the 'National Statement on Ethical Conduct in Human Research' [3] and that these principles can apply to My Health Record across all secondary uses – not just research.

Patient, organisation and provider consent receive little mention in the questions posed and yet we see the issue of management of consent as being an issue of concern. In our responses we have raised the issue of consent management and believe the principles of 'National Statement on Ethical Conduct in Human Research' provide a good foundation.

Recommendations

Our general recommendations are as follows:

1. Thinking for the future: The College advocate avoiding enshrining policies or legislation that inhibit the long-term aspirations for the Secondary Uses of My Health Record.
2. Governance principles that can permit an evolution of data utilisation whilst retaining public confidence are recommended.
3. We recommend an interim governance model be implemented under the framework that will allow harder to achieve long term models of governance that may promote trust and agility to be considered.
4. We recommend evaluating international models where independent governance has been employed as these can be effective in fostering trust and maximising utilisation.
5. Being able to consent patients to allow them to participate in studies evaluating the quality of My Health Record apps and services is required to validate the National Digital Health Strategy and we recommend the approach to consented patients be resolved in the initial framework and governance model.
6. Dynamic consent shows some promise for the management of informed consent but may not be able to be applied in all cases – particularly where data linkage is employed. Dynamic consent research [4] indicates that a very important aspect of achieving trust and acceptance is being fully informed about the uses data is put to. We recommend transparency and feedback regarding the uses of patient data as key principles to the framework and governance going forward.
7. An ability to utilise the Individual Health Identifier as a unique key for secondary uses of data linkage is crucial. We request clarity on the legislation and mechanisms that might be employed in this area.

Responses to Questions

Below are the views of the College to the specific questions asked in relation to proposed Secondary Use of My Health Record Data Framework

Question1: What secondary purposes, if any, should My Health Record data be used for?

ACHI do not recommend prejudging what the data may be used for beyond ensuring principles of what is acceptable be established and implemented robustly through the governance model. The governance model must apply to all potential uses of the data - not just research, for example government use, quality assurance, quality improvement, audit and surveillance activities.

ACHI note the Government response to the Productivity Commission's Report on Data Availability and Use [6] will play a role.

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

ACHI do not recommend adding specific policy or additional legal restrictions on any particular use of the data beyond ensuring the governance mechanisms are robust, transparent and follow appropriate and well established principles (see Question 5 response).

The governance process must be fully accountable as a result of the open nature of our proposed model.

ACHI note the Government response to the Productivity Commission's Report on Data Availability and Use [6] will play a role.

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

Best national outcomes are likely to be served via encouraging many organisations to access data according to governance and procedural protocols. This includes risk management around data release e.g. through systems that manage the access to data, training and accreditation for individuals and organisations. Note that this applies to all secondary uses of data – not just research.

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?

Restricting access to overseas users is from a practical perspective hard to police and would restrict our ability as a nation to be competitive and relevant on an international stage. Use cases do however require careful consideration. Principles internationally around international collaborations using data already exist - for example sharing of data for international genomics research. Best practice should be applied through governance and risk mitigation strategies.

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?

We would recommend that all secondary uses conform to the principles of the National Statement on Ethical Conduct in Human Research [3] including for audit, quality assurance, quality improvement or surveillance purposes. The principles have proven to be effective and are the result of many years' consideration and evolution and hence represent a base set of principles with a track-record of trust and respect. All secondary uses (not just research) should be overseen via an agreed secondary uses governance process. The data access process for non-research applications should not necessarily be bound to the full processes outlined in the National Statement (for example ethics review for an internal departmental audit) but should fully embody the principles of respect, merit and integrity, justice, and beneficence.

Wide access to data is an aspiration – this is only going to happen if the governance mechanism is flexible around the physical mechanisms employed to access the data.

Question 6: What governance model should be adopted to oversee the secondary use of My Health Record data?

Existing national resources such as the AIHW and the ABS may be able to adapt processes and be involved in access mechanisms and linkage however governance should be independent from Gov-

ernment. This is unlikely to be possible initially but we believe this should be a defined goal and potentially expand beyond the remit of the governance of My Health Record alone. Ultimately, independence of governance from Government is crucial to fully realise national trust. Any governance model must also encompass all intended secondary uses of data including government administrative access and non-research uses for example quality assurance, quality improvement, audit and surveillance. Including government access within the governance model is not intended to restrict essential government work but would be designed to ensure there is transparency and mechanisms to ensure appropriate processes are adhered to.

A distributed model of governance is a recommendation to facilitate agility in responding to data use cases via accredited governance nodes. The Government response to the Productivity Commission's Report on Data Availability and Use [5] may play a role in the consideration of what constitutes a 'safe pair of hands'.

The Canadian Institute for Clinical Evaluative Sciences (ICES) [2] model is an exemplar of good independent governance and effective access to data that has the potential to be adapted to an Australian setting. The model allows for the accreditation of nodes and individuals that could be replicated in Australia allowing distributed access and efficiency in the management of data requests via nodes that have satisfied and continue to satisfy accreditation and oversight requirements. The governance model of ICES is specific to research and an Australian model would need to encompass non-research secondary uses.

Question 7: What principles should be adopted, if any, to enable organisations/researchers to request and gain approval for de-identified data from the My Health Record system to be provided for secondary purposes?

As a principal, the application and approval processes must be simple, transparent and independent of physical location. This does not negate a need to ensure applicants (organisations and individuals) have the required certifications and demonstrated mechanisms to protect data they have access to.

There is a grey area with regard to what is considered de-identified data. 'de-identified' is an ambiguous term and its use is not recommended.

This is important here as the principles need to embody how to consider; data where it may have potential for re-identification; it is potentially identifiable in small cell sizes; commonly utilised data linkage keys contain identifying information or may be unencrypted.

Examples of these scenarios are below:

1. Re-identification: On some occasions data that may be anonymous may contain a mapping number that gives the potential for the data to be re-identified. This is termed re-identifiable data rather than de-identified even if the re-identification process may be well controlled.
2. Identity inference & Cell size: The data released contains sufficient information to infer the identity of an individual (for example records containing the home town of patients and patient leg amputations including towns where only one person has a leg amputation)
3. Inadequately anonymised or reversible data linkage keys: use of an SLK581 [6] hash which is commonly shared for data linkage purposes however it contains date of birth, sex and components of surname and forename. As such, it is identifiable information

The principles in relation to questions 7 and 8 must ensure consideration of these common issues is embodied. We recommend that mandating a minimum cell size is NOT embodied as a principal as this will radically impact the ability to undertake key research in rare conditions. Rather, the accredi-

tation mechanisms and processes to secure and protect the use of data in the scenarios above must be defined and be robust.

Transparency of the use of anonymous data is crucial as a principal to ensure trust.

Consideration of mechanisms that allow geospatial analysis whilst minimising the potential for re-identification is important.

Question 8: What principles, if any, should be adopted to enable organisations/researchers to request and gain approval for identified data from the My Health Record system to be provided for secondary purposes?

There should not be a difference in the application process from de-identified uses. The principles outlined in the National Statement on Ethical Conduct in Human Research and privacy legislation already encompass access to identifiable data. This can be applied to all secondary uses of identifiable data.

This is a sensitive issue and we recommend use-cases be presented that allow the public to understand how identifiable data may be handled in certain cases (for example any necessary departmental administration).

As a principal, the mechanism of obtaining consent will need review as part of the application process to ensure the consent obtained and how the consent was obtained is sufficient to balance issues of beneficence and risk.

Dynamic consent [4] is one option for consideration however it is not always possible to implement dynamic consent.

Transparency of the use of identifiable data is crucial as a principal to ensure trust.

The principles should protect health organisation and health provider privacy as well as consumers.

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?

There are no specific requirements to be made beyond ensuring the principals of National Statement on Ethical Conduct in Human Research are complied with for all secondary uses.

There are principals and potential issues that need resolved with regard to data linkage that are important:

1. Cell-size and potential for re-identification becomes an issue when linking data that separately is anonymised. Like any research application, satisfying the governance requirements about how such data will be handled and protected is crucial.
2. Data linkage where person identifiable data is utilised should be undertaken by an accredited data linkage unit. This does not need to be restricted to one data linkage unit – we need mechanisms that are agile.
3. In undertaking data linkage, linkage units should not be party to any information that is not strictly required for the data linkage process (a three-party protocol).
4. Privacy-preserving data linkage keys [7] where the linkage is undertaken using non-reversible and dictionary-protected hashing techniques can impact privacy assessments and can give greater guarantees of anonymity at the potential expense of linkage sensitivity and specificity. A two-party protocol is also possible in this scenario.

5. Consideration should be given to policies regarding the sharing of person identifiers for the purposes of data linkage. It is a common scenario that two organisations by policy to refuse to share identifiers. In this case data linkage is impossible unless the data is further protected by privacy-preserving data linkage key sharing.

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

The processes employed should take a long-term view with regard to where the ADHA see the secondary uses of data going in coming years.

No system is foolproof but this fact should not prevent an open but measured approach to data release.

Different combinations of data released have differing levels of sensitivity. Access processes should take data sensitivity into account when determining what protections are required around a data release. As an example, highly sensitive information may require a research group to perform analysis in a secure research repository environment.

All data users and organisations must meet accreditation requirements unless the data is for public release.

Breach response needs to be an integral part of the framework.

Question 11: What arrangements should be considered for the preparation and release of My Health Record data and who should be responsible for undertaking and overseeing these arrangements?

A National Health Data Custodian [8] as proposed by the Productivity Commission Report on Data Availability [5] in addition to the independent governance mechanisms proposed must have appropriate responsibility and accountability to authorise release. The actual release needs undertaken by the ADHA or delegate (e.g. AIHW / other approved node) under this authorisation.

Question 12: Whose responsibility should it be to make a quality statement about the My Health Record data and to ensure the data are of high quality?

The Australian Digital Health Agency as they are managing the MyHR implementation. Research and validation studies will also build the knowledgebase of the quality of the data in the contexts of research uses of the data, surveillance, audit and quality improvement. It would be good to build a characterisation (metadata) of known limitations of the data.

Question 13: What monitoring and assurance processes, if any, should be considered to ensure My Health Record data secondary users comply with the Framework?

User and organisational accreditation mechanisms should be employed prior to the release of data. Appropriate legal penalties are required for non-compliance with data users and organisations being contractually bound.

Question 14: What risk mitigation strategies should be included in the Framework?

A risk plan is essential and should be employed across the framework. Specific protections and mechanisms have been described above.

Question 15: Should there be a public register which shows which organisations/researchers have requested data, the status of their data request, what they have found by using the data; and any publications that have resulted from using the data?

Yes – evidence from the UK (dynamic consent research [4]) suggests that whether opt-in or opt-out processes are applied, the most important thing for consumers is knowing what their data is used for.

Question 16: Are the existing penalties under the My Health Record Act sufficient?

We are not best-placed to comment on this.

Question 17: What policy changes, if any, need to be considered to support the release of de-identified data for secondary uses from the My Health Record system?

A number of possible approaches have been proposed above. We note that policy is not the law – there needs to be flexibility and understanding that implementing policies to protect data in all cases will not be possible from day one. The policy framework must be able to evolve to itemise what is possible initially and to allow for the eventual further uses of data that may not be able to be considered on day 1.

Note that being able to consent patients to allow them to participate in studies evaluating the quality of My Health Record apps and services is required to validate the National Digital Health Strategy and we recommend the approach to consented patients be resolved in the initial framework.

Question 18: What policy or legislative changes, if any, need to be considered to support the release of identified data (bearing in mind that such release is only possible with the informed consent of the person) for secondary uses from the My Health Record system?

The College cannot comment definitively on the legislation. Release where consent has been granted should not be prevented.

Legal clarity regarding the secondary uses of the Individual Health Identifier for research is required. We suggest that permitting this to be utilised for secondary uses is crucial. The use of fingerprinting / hashing / dictionary attack prevention mechanisms could be proposed if the use in its original form is problematic.

Contributors

Lead Author: Douglas IR Boyle

Contributors: David Bunker, Evelyn Hovenga, Teng Liaw, Peter MacIsaac, David More, Jon Patrick, Leon Heffer, Peter Williams

Review and other contributions: Fellows and Members of ACHI

☐ **I do not consent to my submission being published on the website**

☐ **I wish to remain anonymous**

References

1. The Australasian College of Health Informatics http://www.achi.org.au/
2. The Institute for Clinical Evaluative Sciences (ICES) https://www.ices.on.ca/About-ICES
3. The National Statement on Ethical Conduct in Human Research https://www.nhmrc.gov.au/guidelines-publications/e72
4. Kaye J; Whitley EA; Lund D; Morrison M; Teare H; Melham K, Dynamic consent: a patient interface for twenty-first century research networks *European Journal Of Human Genetics*: EJHG [Eur J Hum Genet], ISSN: 1476-5438, 2015 Feb; Vol. 23 (2), pp. 141-6;
5. Australian Government Productivity Commission Report on Data Availability and Use 8 May 2017 https://www.pc.gov.au/inquiries/completed/data-access#report
6. Randall, Sean M; Ferrante, Anna M; Boyd, James H; Brown, Adrian P; Semmens, James B. Limited privacy protection and poor sensitivity: Is it time to move on from the statistical linkage key-581? *Health Information Management Journal*, August 2016, Vol. 45 Issue: 2 p71-79
7. Vatsalan, Dinusha; Christen, Peter; Verykios, Vassilios S. A taxonomy of privacy-preserving record linkage techniques *Information Systems.* Sep2013, Vol. 38 Issue 6, p946-969. 24p. DOI: 10.1016/j.is.2012.11.005
8. A National Data Custodian http://dataavailability.pmc.gov.au/national-data-custodian