Secondary use of Health Roundtable Data – Policy

Version History		
Draft	Rohan Cattell	12 Nov 2020
For approval	Rohan Cattell	10 Feb 2021
Approved by board	Rohan Cattell	22 Mar 2021
Corrected references	Rohan Cattell	24 May 2021
Corrected references	Rohan Cattell	6 Jul 2021

Contents

1 Introduction

The Health Roundtable (HRT) data asset is a significant collection of hospital operational activity, adding over 4.5 million records per year for more than 250 public and private hospital facilities across Australia and New Zealand.

The HRT datasets contains a wealth of diagnosis, procedure, and demographic data linked to a range of sources such as hospital admissions, emergency presentations and outpatient contacts. It is also possible to track the same patient over time where consistent identifiers exist (usually within a single health organisation). However, identifiers for patients are encrypted by member organisations prior to submission and cannot be directly linked to any other datasets.

The primary use of this data is to provide benchmarking reports and analytics to member organisations.

As the value of the datasets has become more widely known, an increasing number of requests are being received for a variety of research and health system interests. This policy has been updated to assist both applicants and the Board of the HRT in assessing and approving data access and use.

1.1 The purpose of this policy

The 'secondary use' of HRT data refers to the use of data for research, analysis, publication, and other purposes that are not generally available as part of core HRT services provided to members.

The purpose of this policy is to provide clear guidance on:

1. The principles on which access to data for secondary use will be based.
2. The governance framework for data access.
3. The approval process for data access.
4. The manner in which such access takes place.

1.2 The purpose of providing access to data for secondary use

The intent of providing HRT data for secondary use is to assist projects that do one or more of:

1. Develop a better understanding of issues that will help improve the quality and safety of patient care in member hospitals and health services;
2. Develop solutions that support improved and more comprehensive data and benchmarks;
3. Improve the general advancement of knowledge about patient disease, patient management and hospital and health service improvement.
4. Are likely to generate public health benefits

1.2.1 Who can access HRT data for secondary use?

This policy does not limit who may access HRT data, other than through assessment of the likelihood that they will:

1. Adhere to the requirements of this policy.
2. Have the appropriate level of knowledge and training to handle the data appropriately
3. Complete the project for which the use is requested.
4. Not act in a way that might damage the reputation of the Health Roundtable or which might be against the public interest.

1.2.2 What data can be accessed through this policy?

This policy only covers datasets derived from health service data provided by member services through their subscription agreements. The Health Roundtable does not provide access to other types of data that we collect unless covered under another agreement or policy, or where required by law.

The Health Roundtable may decide, on a case by case basis, and in accordance with this policy, which subsets of these datasets may be accessed for secondary use.

2 Personal information and privacy

2.1 Privacy by Design

The Health Roundtable has established *Privacy by Design* as the basis on which information is handled.

The 7 key principles of privacy by design are (Privacy by Design (PbD), 2020):

1. Proactive not reactive, preventative not remedial
2. Privacy as a default setting
3. Privacy embedded into design
4. Full Functionality
5. End-to-end security
6. Visibility and Transparency
7. Respect for User Privacy

For more information about Privacy by Design, see *https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/manage-a-privacy-programme/privacy-by-design-pbd/*.

The key ways in which this policy embeds privacy by design is by ensuring that:

1. Datasets shared for secondary purposes do not contain data that identifies individuals. Where there is a risk of reidentification, that risk is balanced against other requirements and restrictions.
2. Organisations and individuals who access the data provide security appropriate to the nature of the data.

2.2 Information Privacy Principles

The Health Roundtable abides by the privacy principles outlined by the OAIC in Australia0 and the Office of the Privacy Commissioner in New Zealand (Privacy Act 2020, 2020). In most cases, datasets provided by the Health Roundtable in response to applications for data for secondary use will not contain personal information, but where they do, or where there is a reasonable risk of reidentification of individuals, both the Health Roundtable and successful applicants are required to adhere to these principles when handling the data.

In Australia there are also state based privacy laws which may apply to both private and public health service providers, such as hospitals, that may override or apply in addition to the national privacy laws. In order to assist members with complying with these laws, The Health Roundtable also commits to adhering to these requirements when considering any request for data which may contain personal information, or any other information governed by these laws.

The policy positions taken throughout this document have been taken with consideration given to each of these laws.

Australian privacy principles

In Australia, the privacy principles apply to *personal information,* which is information:

- *about an identified individual; or*
- *about an individual who is reasonably identifiable*.

For more information about Australia's privacy principles, see https://www.oaic.gov.au/privacy/australian-privacy-principles/

New Zealand privacy principles

In New Zealand, the privacy principles also apply to *personal information*, which the office of the privacy commissioner defines as:

…any information which tells us something about a specific individual. The information does not need to name the individual, as long as they are identifiable in other ways… (NZ Privacy Principles, 2020)

For more information on New Zealand's privacy principles, see *https://www.privacy.org.nz/your-rights/your-privacy-rights/the-privacy-principles/*

Privacy laws for Australian states and territories

While the National Privacy Act applies to all private sector health service providers anywhere in Australia, it does not apply to state and territory public sector health service providers, such as public hospitals.

> *In NSW, Victoria, and the Australian Capital Territory (ACT) private sector health service providers must comply with both Australian and state or territory privacy laws when handling health information.*
>
> *Queensland, the Northern Territory and Tasmania have privacy legislation that applies only to their public sector, including public sector health service providers.*
>
> *Western Australia and South Australia do not have specific privacy legislation.*
>
> (Privacy in your state, 2020)

For further information about how state laws may apply, see https://www.oaic.gov.au/privacy/privacy-in-your-state/.

Other Countries

The Health Roundtable does not currently provide data for secondary use originating from countries outside of Australia and New Zealand. If at any point, this were to change, The Health Roundtable would take into consideration:

- Any relevant laws of the country from which the data originated
- Consent of the members providing the data

3 Governance Model

The Health Roundtable governance model considers the following aspects related to sharing data:

- Consent
- Ownership
- Custodianship
- Benefits / Risk (the 5 Safes model)

3.1 Consent

It is the responsibility of the member health services to ensure that they have gained any necessary consent for the use of patient data for secondary purposes. The health service themselves consent to the secondary use of data via their subscription agreements.

A condition of membership is that health services provide data to HRT for the purposes of benchmarking and innovation sharing. Should a Member have any concerns regarding the use of data for secondary purposes they should notify the HRT via their Relationship Manager.

3.2 Data Ownership

Member health services retain ownership over data they submit to The Health Roundtable. In practice this means they can request that the data be removed from HRT servers, or corrected should errors be found.

At the point when data is received by The Health Roundtable, it does not contain readily identifiable information that would allow attribution to individuals. For this reason it is not possible for individuals to request removal of their data from Health Roundtable datasets.

Where data is in a format that can still be attributed to a member health service or former member health service, health services can request the removal of their data from HRT datasets.

When members leave The Health Roundtable, their data will continue to be held in our historical collections unless HRT are requested to remove the data by the data owner.

When data is aggregated to form a new, less detailed dataset, ownership then depends on whether the data can still be attributed to the original owner. For example, if data has been aggregated along dimensions that do not include a hospital identifier, then that aggregated data can no longer be attributed to any individual health services. In this case, The Health Roundtable will be considered the owner of the data.

3.3 Data Custodianship

The Health Roundtable act as custodians of the data owned by member health services. Secondary use of this data is provided via consent of members.

Responsibility for appropriate use of Health Roundtable data sits with the Health Roundtable board, who act on behalf of the members, however day to day administration of requests is coordinated by The Health Roundtable Data Governance Committee.

3.3.1 The Health Roundtable Data Governance Committee (HRTDGC)

The HRTDGC is responsible for approving requests for secondary data use. Further details on the approval process and the role of the HRTDGC in practice can be found in the accompanying Secondary Use of *Health Roundtable Data - Guidance*.

The HRTDGC will comprise:

- at least one representative from the Board, who will perform the role of Chairperson.

- HRT CEO or delegate
- HRT data expert
- HRT clinician
- an experienced academic researcher.

3.4 The 5 Safes model

In assessing requests for data for secondary use, The Health Roundtable Governance Committee will use the 'Five Safes' Framework (Oppermann, 2017):

Safe projects	Is the use of the data appropriate?
Safe people	Can the users be trusted to use it in an appropriate manner?
Safe settings	Does the access facility limit unauthorized use?
Safe data	Is there a disclosure risk in the data itself?
Safe outcomes	Are the outputs non-disclosive?

In assessing the 'Five Safes', the data governance committee will consider whether the project has already had ethics clearance from a recognised ethics committee. This is a minimum requirement for any research project aiming for peer reviewed publication.

See *Secondary Use of Health Roundtable Data - Guidance* for a guide on how the HRTDGC will assess safety levels for each of the 5 safes.

3.5 Identification of HRT member services

Under no circumstance will approval be granted for projects where the outcome identifies individual Health Roundtable member services or facilities unless explicit consent has been granted by that member.

3.6 Health Roundtable use of derived output

Successful data applicants will be required to agree to provide to the Health Roundtable, on request, and free of charge, any articles, reports, algorithms, machine learning models, or other analytical output derived from Health Roundtable data provided under this policy, for the purposes of making these materials available to its members.

References

Australian Privacy Principles. (2020). Retrieved from Office of the Australian Information Commissioner: https://www.oaic.gov.au/privacy/australian-privacy-principles/

NZ Privacy Principles. (2020). Retrieved from privacy.org.nz: https://www.privacy.org.nz/your-rights/your-privacy-rights/the-privacy-principles/

Oppermann, I. (2017). *Data Sharing Frameworks.* Sydney: Australian Computer Society.

Privacy Act 2020. (2020). Retrieved from Privacy Commissioner: https://privacy.org.nz/privacy-act-2020/privacy-act-2020/

Privacy by Design (PbD). (2020). Retrieved from NZ Digital Government: https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/manage-a-privacy-programme/privacy-by-design-pbd/

Privacy in your state. (2020). Retrieved from Office of the Australian Information Commissioner: https://www.oaic.gov.au/privacy/privacy-in-your-state/

What is personal information? (n.d.). Retrieved from Privacy Commissioner: https://www.privacy.org.nz/further-resources/knowledge-base/view/199?t=82722_108127