RACGP

Royal Australian College *of* General Practitioners

Guiding principles for managing requests for the secondary use of de-identified general practice data

This resource should be used alongside 'Secondary use of de-identified data: A checklist for general practice'.

Introduction

Data collected by general practice have a role to play in improving health in Australia by informing policy, public health initiatives, research and service delivery.

With health information increasingly digitised, government agencies, policymakers, researchers and commercial enterprises are keen to unlock the value of these data.

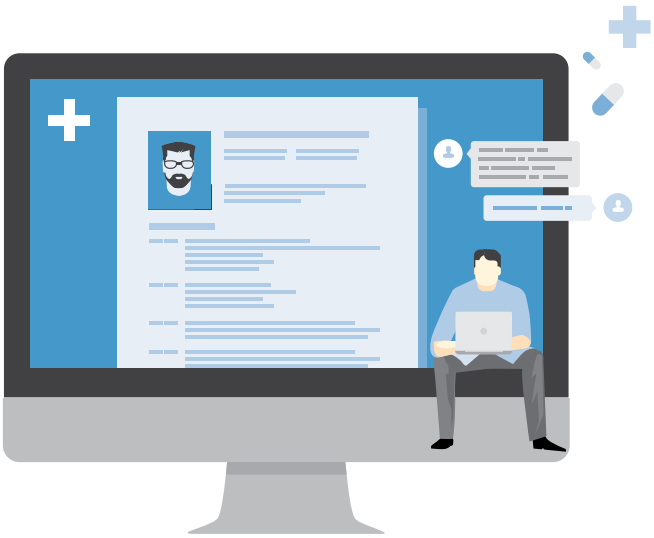
As demand for general practice data will continue to rise, it is important that practices understand their legal obligations when providing the data.

General practices need to become adept at discerning to whom, when and how it is appropriate to provide their data for secondary use.

To help practices evaluate requests for data, minimise risk and comply with relevant legislation,[1] The Royal Australian College of General Practitioners (RACGP) has developed the following guiding principles for the provision of de-identified general practice data for secondary use:

- Secondary use of data must be transparent and appropriate.
- Requesting third parties must extract, manage and secure data to required standards.
- Practices should implement procedures for providing data to requesting parties.
- Agreements and contracts with requesting third parties should reflect these RACGP guiding principles.

A summary checklist is provided with this document to assist practices in their decision making.



Definition of secondary use and de-identified data

'Secondary use' refers to the use of patient health information, collected as part of clinical care, for purposes for which it was not originally collected.

These guiding principles cover the secondary use of general practice datasets where individual patients and providers have been de-identified.

De-identification involves removing or altering information that identifies an individual, or is reasonably likely to do so.[2] Where information has been appropriately de-identified, it is no longer personal information and can therefore be used or shared in ways that might not otherwise be permitted under the *Privacy Act 1988* (Cwlth).

This document does not cover the secondary use of identified patient information due to the additional conditions required, including issues relating to gaining informed individual consent.

It is important to note that de-identified data can be given back to the general practice that supplied the data, and can be re-identified within the practice for quality improvement purposes. Re-identification of data is appropriate in this instance.

These guiding principles do not cover the secondary use of My Health Record data, which is governed by its own framework and legislation.[3]

Data custodianship

Maintaining accurate and comprehensive patient health records is crucial to providing patients with continuity of high-quality and safe care. Patient health records generally belong either to the health professional who created them or to the practice in which they work.[4] As the custodians of data, general practitioners (GPs) and their practices have a responsibility to ensure these data are collected, stored, accessed, used and disposed of appropriately.

Other than giving patients appropriate access and responding to legal processes such as subpoenas, practices are not obliged to give other parties access to patient and practitioner data.

Compensation for the costs of providing data

The provision of data involves time and effort on the part of practices, which may consider charging a fee or compensation in such a situation.

Compensation or reward for providing data can be non-monetary, such as feedback or analysis of the data, or receiving continuing professional development (CPD) points.

Benefits of providing general practice data for secondary use

As the foundation of Australia's health system, and with 87% of the population seeing a GP at least once a year,[5] general practice is an important source of information that can help improve Australians' health through:

- identifying at-risk populations
- public health surveillance
- improved healthcare planning
- informing health policy
- health research
- population health measures.

Although the RACGP encourages practices to provide data for such uses, it is important this is done with consideration of four guiding principles.

Guiding principles

1. Secondary use of data must be transparent and appropriate

Before agreeing to share data, practices should be clear regarding what data will be extracted, and how those data will be used. This will allow practices to make informed decisions about releasing practice data.

Disclosure of all proposed uses by any requesting parties is required. Data provided should only be used for the specific purpose for which a practice has provided consent.

Practices should evaluate whether they believe the requesting third party is a reputable organisation, and whether their aims in using the data are open, honest and appropriate (eg achieving one or more of the benefits outlined in the above Introduction).

It is important requesting third parties have an understanding of general practice, the context in which the data were collected and the nature of the data. Requesting parties can be asked to demonstrate this understanding by, for example, detailing current and planned engagement with general practice.

Data should not be provided for inappropriate purposes. Inappropriate uses of general practice data could include:

- commercial purposes that are not clearly linked to improved patient care or the benefits listed in the above Introduction (eg targeted marketing of a product or screening test)
- linkage to datasets held by agencies such as workers compensation insurers, private health insurers or Centrelink for compliance or risk-assessment purposes
- to performance-manage one or more clinicians
- to publicly benchmark practices or individual health professionals or medical services (without their explicit consent)
- to conduct compliance audits
- to carry out low-quality, dubious or unethical research.

2. Requesting third parties must extract, manage and secure data to required standards

Practices should assess the quality of data management by requesting third parties, assuring themselves they will extract, manage and secure data to acceptable standards. At a minimum, requesting third parties should demonstrate and document how they:

- comply with the Privacy Act and the Australian Privacy Principles, setting out their obligations in an open and transparent manner
- de-identify data, which they should do before the data leaves the practice (if the data are not de-identified before leaving the practice, patient consent may be required)
- evaluate the risks that data could be re-identified and the steps taken to prevent re-identification (the risk of re-identification must be very low)
- adequately protect data, with security processes and procedures in place to ensure appropriate transmission, storage (data should not leave Australia) and management
- implement risk-mitigation strategies to protect against misuse and/or unauthorised access of data
- ensure data are only kept for a specified period and the specific purpose for which they were collected
- will destroy the data once they are no longer needed.

3. Practices should implement procedures for providing data to third parties

As data custodians, practices must protect patients' rights and privacy when providing de-identified data for secondary use. In order to do this, practices should implement procedures for managing requests for access to data.

Patients must be made aware of the practice's approach to the collection and security of healthcare information for primary and secondary purposes, and whether it provides de-identified data to third parties.

This information should be displayed publicly (eg as part of a practice privacy policy in the waiting room, and/or on the practice website).

This information should include assurances and advice on patients' rights to access and correct information.

While individual patient consent for sharing de-identified data is not a legal requirement, most data-extraction tools have functionality that enables individual patients to be removed from the extraction process. A practice may, therefore, wish to put a procedure in place to manage requests from patients who do not want their data to be used for secondary purposes.

Practices should nominate an authorised person (privacy officer) who will assess requests and provide permission to requesting parties for data to be used for secondary purposes in accordance with the advice in this document. The practice may wish to keep a log of such requests and permissions.

Practices should consider how they wish to be involved in the data collection and analysis, or be kept informed of any results and outcomes.

The Office of the Australian Information Commissioner's (OAIC's) *De-identification and the Privacy Act* provides further information to assist businesses to protect privacy when using or sharing information.

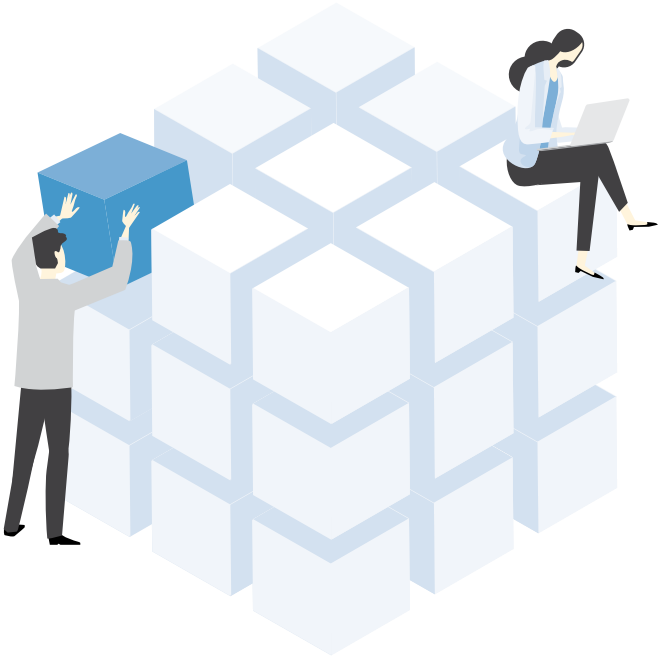
4. Agreements and contracts with requesting third parties should reflect these principles

When entering into agreements to provide data, general practices should consider including clauses in their contracts to explicitly address the principles in this document.

As de-identified data can be re-identified, especially when used in large datasets that combine multiple sources of data, it is recommended the legal agreement between the practice and the requesting party includes assurances the data will not be used in a manner that enables re-identification, as well as an indemnity in favour of the general practice providing the data in the event this assurance is breached.

For example, the legal agreement may include clauses that:

- state data use is limited to the purpose outlined in the contract. Further analysis, sub-analysis or extrapolation requires written permission from the practice
- state the party cannot sell, provide or transfer provided data to other parties without the practice's express permission
- include an assurance the data will not be used in a manner that allows re-identification of individuals (for any secondary use purposes)
- indemnify your practice, its GPs and patients in the event of a breach of the terms of the contract. And if a data breach should occur, due to a failing by the requesting third party, they will pay any cost incurred by the practice in defending any resulting claim
- include assurances the third party will adhere to the Privacy Act and Australian Privacy Principles
- state requesting parties will not use the data to publicly benchmark general practices or manage GPs' performance, or be used for compliance purposes
- include assurances that data analysis will be academically and ethically rigorous, involving a GP in any research process and analysis
- state the agreement expires on a particular date, or includes a date to review the agreement
- state the contract can be terminated at any point for failure to meet the principles.



The RACGP has developed a secondary use of de-identified data checklist for general practice that should be used alongside this document.

References

1. Australian Government Office of the Information Commissioner. Australian Privacy Principles. Sydney: OAIC. Available at www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/ [Accessed 7 November 2019].
2. Australian Government Office of the Information Commissioner. De-identification and the Privacy Act. Sydney: OAIC. Available at www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/ [Accessed 7 November 2019].
3. Australian Government Department of Health. Implementing the Framework to guide the secondary use of My Health Record system data. Canberra: DoH. Available at www1.health.gov.au/internet/main/publishing.nsf/Content/eHealth-framework [Accessed 17 December 2019].
4. Australian Government Office of the Information Commissioner. Chapter 4: Giving access to health information. Sydney: OAIC. Available at www.oaic.gov.au/privacy/guidance-and-advice/guide-to-health-privacy/chapter-4-giving-access-to-health-information/ [Accessed 17 December 2019]
5. Australian Government Department of Health. Annual Medicare statistics: Financial year 1984–85 onwards. Available at www.health.gov.au/internet/main/publishing.nsf/content/annual-medicare-statistics [Accessed 7 November 2019].

We acknowledge the Traditional Custodians of the lands and seas on which we work and live, and pay our respects to Elders, past, present and future.

racgp.org.au

20803.14

RACGP

Royal Australian College *of* General Practitioners