Three key principles for the secondary use of general practice data by third parties

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

The Royal Australian College of General Practitioners (RACGP) recognises that in certain circumstances, general practices may wish to provide data for these purposes. If a practice chooses to provide data, the RACGP recommends it get independent legal advice to ensure that any data disclosure is done with careful consideration of a practice's legal and ethical responsibilities. General practitioners (GPs) and general practice staff need to be adept at discerning to whom, when and how to provide their data for secondary use if they choose to do so.

This document aims to help GPs and general practice staff navigate this territory by outlining three key principles. These principles are advisory only and can form the basis for a discussion around data transfer. These principles represent the RACGP's views on best practice in this area. Practices may decide that these principles are not appropriate for their particular circumstances.

In the event that a practice chooses to disclose, general practices can nominate an authorised person (eg, the practice's privacy officer) to assess requests and provide permission to requesting parties for data to be used for secondary purposes. The general practice may wish to keep a log of such requests and permissions.

A checklist for third parties can be found in this document and general practices can provide this to entities requesting data for their consideration.

This document does **not** constitute legal advice. When considering if, and how to provide data to any third party, practices must seek independent legal advice. The RACGP takes no responsibility for any loss of any description by a practice or person as a result of relying on this document.

Data sharing agreements or contracts

Parties who intend to use general practice data for secondary purposes may enter into a formal data sharing agreement or contract with the general practice. In some instances, such an agreement might apply to more than one general practice. The principles discussed in this document can be considered as possible issues to be discussed if an agreement is being contemplated.

Three key principles for the secondary use of general practice data by third parties:

1. **All parties should demonstrate compliance with data management best practice**
    a. All parties should demonstrate compliance with the Privacy Act and Australian Privacy Principles (APPs)
    b. All parties should act ethically with regard to general practice data
    c. Data must only be used for agreed purposes
    d. Data security is everyone's responsibility
    e. Special considerations may apply for data linkage
2. **Healthcare consumers deserve transparency and agency in the use of their health data**
    a. General practices should consider their legal obligations around secondary use to patients

b. Special considerations may apply for data on or about Aboriginal and Torres Strait Islander peoples
c. Special considerations may apply for data on or about other patient groups of particular significance

3. **The contribution of general practice must be valued and recognised**
    a. General practices must retain access and control over what can be extracted
    b. There must be a value proposition for general practice
    c. GP advisors must be involved in data analysis and interpretation

Definitions

Definition of general practice data

In this document, 'general practice data' refers to any data that is collected or created and held in general practice. These data might be information about patients or providers and can include:

- demographic information
- appointment/booking information
- billing information
- clinical/consultation notes
- prescribing information
- clinical images
- investigation reports
- referral information and other correspondence
- income information pertaining to doctors and other staff at the practice.

Definition of secondary use

The provision of clinical care is, generally speaking, the primary use of general practice data. General practices might also use collected data for administration or business support, medico-legal purposes, quality improvement, clinical audits of the practice population, and internal benchmarking. Whether these purposes are also a primary use should be the subject of specific advice for individual practices' circumstances.

For the purposes of this document, '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.

Definition of third party

In this document, 'third party' refers to any entity requesting general practice data for the purposes of secondary use. Third parties referred to in this document could include government, government-funded organisations, not-for-profit organisations, research institutions, and commercial entities including pharmaceutical companies and medical software vendors.

Definitions of de-identified information

De-identification involves removing or altering information that identifies an individual or is reasonably likely to do so..

When personal information (ie, data has not been de-identified) is requested by a third party, practices need to consider, and take specific advice on whether specific patient consent is needed. A requesting entity may need to meet the requirements of a human research ethics committee.

Key principles

1. All parties should demonstrate compliance with data management best practice

a) All parties must act in compliance with the Privacy Act and Privacy Principles

Issues of consent for the disclosure of personal health data are governed under the *Privacy Act 1988* (*Cth*) (Privacy Act) and the Australian Privacy Principles (APPs). All parties that are handling personal data must ensure they act in compliance with the Privacy Act and the APPs. Practices should take specific legal advice to clearly identify their obligations.

b) All parties should act ethically with regard to general practice data

All parties handling general practice data have an obligation beyond that of mere legal compliance. They must behave ethically and recognise their decisions and actions have impacts on general practice teams, their patients, and society more broadly. Third parties using general practice data need to consider whether positive values (e.g. merit, integrity, justice, beneficence) underlie their activities, evaluate whether they are contributing to the community, and reflect whether their behaviour is respectful of social norms.

General practices must 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. Ethical conduct involves more than simply doing the right thing. It involves 'acting in the right spirit, out of an abiding respect and concern for one's fellow creatures.'[1]

Examples of inappropriate secondary uses could include:

- That which is inappropriate from a data management perspective (ie, it does not align with data management best practice)
- That which might reasonably result in the re-identification of individuals
- On-selling or otherwise providing or transferring data to other parties (not specified in the data sharing agreement or contract)
- Publicly benchmarking practices or individual health professionals
- Establishing pay-for-performance systems or performance managing clinicians
- Revalidation or credentialling of health professionals
- Purely commercial purposes not linked to the goal of improving patient care
- Linkage to datasets held by entities such as workers' compensation insurers, private health insurers, or Centrelink
- Low quality or dubious research.

This list is neither exhaustive nor definitive. Practices should always take legal advice to cater for their individual circumstances.

c) Data must only be used for agreed purposes

General practice data usually contains longitudinal and dynamic data, often spanning decades. Third parties should aim to extract the minimum amount of data needed to achieve their purpose (ie, not complete medical records). General practice data must only be used by a third party for the purposes outlined in the data sharing agreement or contract. Dependent on the terms of the contract, the third party may need a variety of consents to use, provide, or transfer the data for any purpose not originally specified, including further analysis or extrapolation of the data. Practices should take specific legal advice to clearly identify their obligations.

d) Data security is everyone's responsibility

Third parties must ensure the data is kept secure. Third parties should also demonstrate compliance with Australian cyber security standards for systems used to store and analyse data. They should explain how they employ cyber security resilience measures to protect extracted data from malicious attempts to access and misuse it by external agents. Details might be provided in the data sharing agreement or contract.

e) Special considerations apply for data linkage

Bringing together data relating to one individual, family, place or event from disparate sources can help answer questions that are not easy to answer using other methods. Dependent on the circumstances, informed patient consent may be necessary and independent legal advice should be taken.. Linkage of de-identified data however carries a risk of re-identifying individuals. In this situation, it is imperative identifiable demographic data is separated from clinical data prior to linkage, and personnel involved in the linking of identifiable data do not have access to the clinical data, and vice versa. If a third party intends to link general practice and other data, they must seek ethics approvals through the relevant channels and demonstrate to the general practice this is being conducted by a reputable body such as the Australian Institute of Health and Welfare (AIHW).

2. Healthcare consumers deserve transparency in the use of their health data

a) General practices should provide information on secondary use to patients

Much effort is taken in general practices, and healthcare settings in general, to ensure patient privacy is protected. Patients must trust they can speak freely with their GP without fear personal information could end up in the hands of a third party without their knowledge.

To retain patient trust, it is important for general practice to have processes and protocols in place informing and reassuring patients data collected in general practice is adequately protected in terms of privacy and ethical principles.

The RACGP *Standards for general practices* (5th edition) recommends general practices advise patients about whether they provide de-identified data to third parties, and by whom and for what purpose the data is used. Clear, easy-to-understand statements about the purpose and benefits of secondary use of health data help foster trust.[2]

Practices can consider a multifaceted approach to inform patients of their data sharing policy, such as through posters in waiting rooms, on the general practice's website, social media channels, practice newsletters, and patient registration forms. As with all patient communications, general practices must consider literacy levels and language barriers when discussing secondary uses of data.

General practice principals should consider which staff working in the clinic need to be informed about any data sharing agreements so they have an understanding about secondary use of patient data and can discuss this with patients as required. Contractors and locums may also need to be made aware of these agreements.

General practices might choose to nominate a point of contact to answer any patient questions or concerns.

b) General practices may need to provide patients with an opportunity to opt out of providing data for secondary uses

Most data extraction software has an opt-out function, therefore, where feasible, general practices should provide patients with a choice to opt out of secondary uses of data.[3] If a patient indicates they wish to opt out of a program to use de-identified data for secondary purposes (whether verbally or in writing), this must be indicated in their record.

Although desirable, there is currently no facility in general practice electronic medical record systems for patients to give consent for use of particular data (eg, all de-identified data except psychiatric information) or for the use of data for particular purposes (eg, only for medical research).

Patients must be advised that once they provide consent for the secondary use of data, it will not be feasible to remove previously provided data should they have a change of mind. Identifiers will have been removed in this process, rendering it impossible to link the supplied data to any individual following extraction. The data may have been used in published research by a third party. It is, however, possible to withdraw consent for future secondary uses of data.

Practices should seek their own independent legal advice to determine when and whether an opportunity to opt out of providing data for secondary uses is necessary.

c) Consent must be obtained from patients for particular secondary uses

For some secondary purposes, patients will be required to give their express consent for their data to be included in the research. The National Health and Medical Research Council (NHMRC) National Statement on Ethical Conduct in Human Research provides guidance on when consent is required in Chapter 2.3: Qualifying or waiving conditions for consent.

Third parties should outline the process by which the patients of a general practice will be approached to provide consent and this can be documented in the data sharing agreement or contract. Consent conversations should be thoroughly documented by the third party, and all efforts made to ensure the patient is aware of the ways in which the data will be used.

Third parties should refrain from passing on or selling data to other third parties without prior agreement with the general practice in the data sharing agreement.

d) Special considerations apply for data on or about Aboriginal and Torres Strait Islander peoples

Data that concerns or that might affect Aboriginal and Torres Strait Islander people, either individually or collectively, must be given specific consideration by third parties.

Indigenous data sovereignty ensures data on or about Aboriginal and Torres Strait Islander people is used in ways consistent with their values, culture, and diversity, and meets their current and future needs.[4]

General practices entering into data sharing agreements should ensure the third party has appropriate Aboriginal and Torres Strait Islander data sovereignty arrangements.

e) Special considerations may apply for data collected specifically related to other patient groups

Data used for research on our about particular populations (eg, people from culturally and linguistically diverse (CALD) backgrounds or individuals with rare health conditions) will often involve smaller data sets, which can increase the risk of re-identification. Third parties using data related to these populations should minimise the risk of de-identification to protect patient privacy.

3. The contribution of general practice must be valued and recognised

a) General practices must retain access and control over what can be extracted

Maintaining accurate and comprehensive patient health records is crucial to providing patients with continuous 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.[5] As the custodians of data, GPs

and their practices have a responsibility to ensure these data are collected, stored, accessed, used and disposed of appropriately.

General practices must retain control over what data can be extracted from their systems by third parties.

Data generated by a practice must be available and remain available for all purposes the practice deems appropriate. Third parties storing electronic medical record data must not restrict access or charge fees to access a practice's own data.

b) There must be a value proposition for general practice

Secondary uses of general practice data should preferably benefit the larger healthcare sector including general practice, not just secondary or tertiary segments of the health care system.

Therefore, third parties requesting data are expected to explain how their use of the data will result in public benefit, and specifically, benefit for general practice. Further, they must specify how they will provide results or outcomes of research from supplied data to participating general practices.

Before agreeing to provide general practice data, practice owners, GPs and administrative staff will need to know the costs, benefits, and risks associated with extraction, storage, analysis, curation and use of general practice data by third parties. General practices can refer to their medical defence organisation (MDO) to determine whether they have any legal exposure in the event a data breach occurs due to a failing by a third party.

General practices might require support, particularly in the form of additional resourcing, to change data entry practices or to engage in quality improvement activities. General practices should discuss how such resourcing might be funded with third party beneficiaries of the data. .

c) GP advisors must be involved in data analysis and interpretation

Third parties should demonstrate meaningful involvement of general practice advisors in analysing and interpreting general practice data. It is important third parties have an understanding of general practice, the context in which the data were collected, and the nature of the data. GPs can help explain the provenance and meaning of data.

Checklist for third parties

Entities requesting general practice data must consider the following points and are expected to provide information on the items in the checklist to the general practice in negotiations around a data sharing agreement or contract. The checklist will help practices evaluate requests for data, minimise risk and comply with relevant legislation.

Data agreements and contracts with requesting third parties should reflect the principles laid out in this document. The checklist is applicable to the extraction, storage, curation, use and analysis of general practice data by third parties.

Note that an alternative framework for research purposes is the Five Safes framework, used by the AIHW, to reinforce management of the privacy and confidentiality of data. The Five Safes is an approach to thinking about, assessing and managing risks associated with data sharing and release.[6]

Prior to negotiating any agreement with a third party, practices should obtain independent legal advice to cover all relevant issues, especially privacy and confidentiality considerations.

What

- The purpose/s for which the data will be used, clearly stated, including potential future use/s of the data set.
- The data the entity intends to access or extract, ensuring that what is requested and used is only that which is directly related to achieving the stated purpose (ie, not complete medical records)

Why

- The benefits for general practice and the broader healthcare sector.

How

- The ways in which the entity will comply with the Privacy Act and the APPs in using personal data (does not apply to de-identified data).
- The details of any ethics approvals for research.
- Evidence of appropriate cultural safety and data sovereignty arrangements for research pertaining to Aboriginal and Torres Strait Islander peoples.
- How information about the proposed use of data will be provided to consumers.
- If required, how consumers would give explicit consent for involvement.
- The method by which data will be extracted and transferred (with assurances the data will be encrypted).
- The process for storing, protecting, or securing data once it has left the general practice.
- The method by which extracted data will be de-identified.
- The process for managing the risk of re-identifying individuals, including indemnity for the general practice providing the data in the event this assurance is breached.
- The process by which data will be destroyed at the end of the life of the data sharing agreement (where personal data is used with the consent of the individual).
- The methods by which the project's impacts will be measured or evaluated.

Where

- The location in which the data will be stored (with assurances that the location is physically secure and is based in Australia as per legislation, noting that technical security of the data is a separate issue).

Who

- The research credentials of the entity.
- The details of individuals with access to the identifiers where the project is subject to ethics approvals.
- The involvement of GP advisors in the project or research, especially with regards to data analysis and interpretation.
- The involvement of Aboriginal and Torres Strait Islander people or organisations in the project or research, if relevant.
- The involvement of representatives of other important patient groups, such as people from culturally and linguistically diverse backgrounds, if relevant.

When

- The duration for which the data will be kept.
- The dates between which the data sharing agreement will last (or a date to review the agreement).
- Provisions to ensure that both parties have the right to terminate the data sharing agreement at any time for failure to comply with principles established in that document.

Additional RACGP resources

- Practice Incentives Program Quality Improvement Incentive (PIP QI) fact sheet

- Privacy and managing health information in general practice

External resources

- Office of the Australian Information Commissioner: Australian Privacy Principles
- Privacy Act 1988 (Cth)

References

1. The National Health and Medical Research Council, the Australian Research Council, and Universities Australia. National Statement on Ethical Conduct in Human Research 2007. Canberra: Commonwealth of Australia; 2007, updated 2018.
2. Consumers Health Forum of Australia and NPS MedicineWise. Engaging consumers in their health data journey: a joint report by NPS MedicineWise and the Consumers Health Forum of Australia. Canberra: CHF and NPS MedicineWise; 2018.
3. Safran C, Bloomrosen M, Hammond WE, et al. Toward a national framework for the secondary use of health data: an American Medical Informatics Association White Paper. J Am Med Inform Assoc. 2007;14(1):1-9.
4. Maiam nayri Wingara Indigenous Data Sovereignty Collective and the Australian Indigenous Governance Institute. Indigenous data sovereignty communique. Indigenous Data Sovereignty Summit; 20 June 2018; Canberra, ACT.
5. 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 20 September 2022]
6. Australian Institute of Health and Welfare. The Five Safes framework. Canberra: AIHW. Available at www.aihw.gov.au/about-our-data/data-governance/the-five-safes-framework [Accessed 20 September 2022]