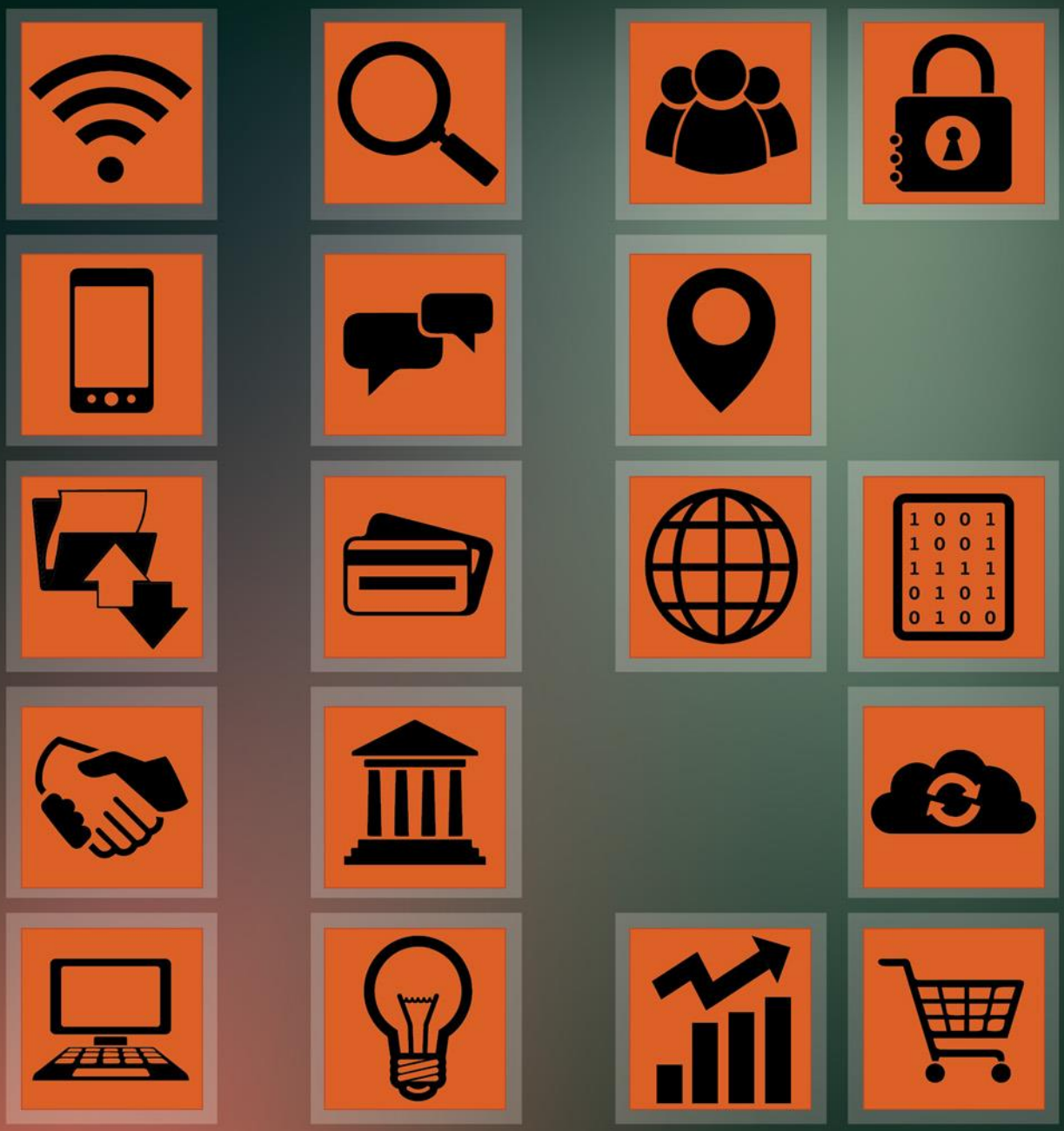

MedicineInsight – Privacy Impact Assessment

Commercial-in-Confidence

For: NPS MedicineWise

Date: 29 January 2021

INFORMATION INTEGRITY SOLUTIONS

managing the **privacy** of **individuals** is **complex** and we can help you get it **right**

Table of Contents

Glossary

Abbreviation or term	Expansion or definition
ADHA	Australian Digital Health Agency
AIHW	Australian Institute for Health and Welfare
APPs	Australian Privacy Principles in the Privacy Act
CAG	Consumer Advisory Group
DATB	Data Availability and Transparency Bill
DGC	Data Governance Committee
DGF	Data Governance Framework
DOH	Commonwealth Department of Health
GPs	General practices
HREC	Human Research Ethics Committee
IIS	Information Integrity Solutions Pty Ltd
NHMRC	National Health and Medical Research Council
NREEC	National Research and Evaluation Ethics Committee
OAIC	Office of the Australian Information Commissioner
PIA	Privacy Impact Assessment
PMF	Privacy Management Framework
PMP	Privacy Management Plan
Practice Agreement	MedicineInsight Participating General Practice Agreement
Privacy Act	*Privacy Act 1988* (Cth)
RACGP	Royal Australian College of General Practitioners

1. Executive summary

NPS MedicineWise engaged Information Integrity Solutions Pty Ltd (IIS) to conduct a Privacy Impact Assessment (PIA) on its MedicineInsight program.

MedicineInsight is large-scale, national general practice dataset, established to support quality improvement in general practice, post-market monitoring of medicines and tests, and Australian health policy and primary care. The program collects de-identified data drawn from the clinical records of participating general practices.

NPS MedicineWise sought a PIA that:

- Identified privacy risks taking account of the *Privacy Act 1988* (Cth), the Australian Privacy Principles (APPs) and community expectations about privacy.
- Provided recommendations to ensure compliance against the APPs and potential further improvements to the consent model, handling of de-identified patient information and data linkage to Commonwealth data assets.
- Considered possible privacy impacts regarding its current collection of de-identified patient information, and improvements which may support data linkage to Commonwealth data assets or compliance to emerging Commonwealth public interest requirements.

IIS commends and supports NPS MedicineWise in taking its role as Data Custodian seriously in collecting, using and storing MedicineInsight information, and ensuring that there are multiple layers of controls to protect the data from inappropriate access. It also supports NPS MedicineWise intentions to safeguard the privacy of individuals that contribute data and to respect their choice not to participate.

1.1 IIS' overall opinion

MedicineInsight contains personal information about a significant number of GPs and extensive holdings of de-identified[1] unit-level data about GP patients. IIS considers that, subject to NPS MedicineWise's steps to avoid re-identification, the latter information is unlikely to be personal information and is not, therefore, formally subject to the Privacy Act. However, in line with NPS MedicineWise's intention to adopt Privacy Act standards, IIS has conducted its assessment as though the APPs would apply to all MedicineInsight data.

For MedicineInsight, its main risks are the potential for re-identification or other security incidents that result in significant data breaches, and the resulting impact on individuals as well as NPS

[1] For the purposes of this report, IIS uses the meaning of 'de-identified' drawn from the Office of the Australian Information Commissioner's (OAIC) guidance. That is, "[i]nformation will be de-identified where the risk of an individual being re-identified in the data is very low in the relevant release context." Changing the release context (e.g., disclosure into another environment as a result of a data breach) could result in the information no longer being de-identified.

MedicineWise's reputation and its ability to maintain good relationships with its stakeholders if its privacy protection measures are not sufficiently robust.

IIS considers that the program has medium inherent privacy risks. We also consider that NPS MedicineWise has a range of measures, including information handling settings and governance arrangements that reduce the residual privacy risk to very low.

Overall, IIS considers that NPS MedicineWise's privacy approach is strong and, while the APPs do not apply as such, it is likely to be consistent with, and would support, compliance with the APPs.

IIS has not identified any areas of 'non-compliance'. We have identified some areas where we consider some additional steps would strengthen NPS MedicineWise's compliance with the APPs (if they applied) or assist it to meet best practice. In particular, IIS suggests ways to strengthen privacy governance and de-identification processes.

IIS was also asked to comment on the suitability of the patient opt-out approach and transparency of MedicineInsight program information. IIS acknowledges the considerable work NPS MedicineWise has undertaken, and is still undertaking, in thinking about its opt-out approach. IIS agrees with the Department of Health that the approach does need to be strengthened and it supports the type of measures NPS MedicineWise is now considering.

In undertaking analysis for the PIA, IIS had in mind that NPS MedicineWise is operating in a fast-moving environment where there is increasing focus on the use, sharing and linkage of information. Particular challenges in the near future include the requirements in the Data Availability and Transparency Bill 2020, if passed, and possible changes arising from the current review of the *Privacy Act 1988.*[2] IIS has made reference to such challenges where relevant in the report. We consider that NPS MedicineWise is likely to be well set up to respond to these future challenges, and that the recommendations in this report would further strengthen its approaches.

[2] On 12 December 2019, the Attorney-General announced that the Australian Government would conduct a review of the *Privacy Act 1988* to ensure privacy settings empower consumers, protect their data and best serve the Australian economy. The Issues paper is available at https://www.ag.gov.au/integrity/publications/review-privacy-act-1988-cth-issues-paper

1.2 Recommendations

IIS has made 10 recommendations summarised below and categorised as follows:0

- Type:
  - Recommendation aims to **strengthen compliance**
  - Recommendation aims for **best practice**
- Priority:
  - High – Implement within 3 months
  - Medium – Implement within 6 months
  - Low – Implement in 12+ months
- Resource (estimated; IIS notes that resource implications will be a matter for NPS MedicineWise to assess)
  - High – Recommendation could require significant additional resources to implement
  - Medium – Recommendation could require some additional resources to implement
  - Low – Recommendation can be implemented as part of normal BAU

#	Recommendation	Type	Priority	Resource
1	Ensure NPS MedicineWise correctly portrays the status of MedicineInsight de-identified patient data under the Privacy Act	Best practice	Low	Medium
2	Strengthen privacy governance measures, including in relation to privacy training, risk management and strategic oversight	Strengthen compliance	Medium	High
3	Update privacy policy to specifically address MedicineInsight	Best practice	High	Low
4	Strengthen security with some additional measures, including access control, data retention and risks related to GPs	Strengthen compliance	Medium	Medium
5	Ensure opt-out approach is transparent, portrayed as best practice and not consent, and supported by positive messages about the MedicineInsight program	Best practice	Varies[3]	High

[3] Priority depends on NPS MedicineWise's time frame for implementing recommendations from its consent model review.

#	Recommendation	Type	Priority	Resource
6	Include data user training as a requirement of MedicineInsight data access	Best practice	Medium	Low
7	Update the documented de-identification procedures	Best practice	High	Low
8	Build in de-identification review into regular assurance cycle	Best practice	Low	Medium
9	Clarify and formalise procedure for responding to (re)identification incidents, in the context of incident management reporting processes	Strengthen compliance	High	Low
10	Explore software-based solutions for managing de-identification risk	Best practice	Low	Low

2. About the PIA

2.1 Scope

NPS MedicineWise sought a PIA report which:

- Identified privacy risks taking account of the *Privacy Act 1988* (Cth) (the Privacy Act), the Australian Privacy Principles (APPs) and community expectations about privacy
- Provided recommendations to ensure compliance against the APPs and potential further improvements to the consent model, handling of de-identified patient information and data linkage to Commonwealth data assets
- Considered possible privacy impacts regarding its current collection of de-identified patient information, and improvements which may support data linkage to Commonwealth data assets or compliance to emerging Commonwealth public interest requirements.

The focus of the assessment will be practitioner and patient information collected for the MedicineInsight program.

IIS was asked to comment on:

- The suitability of the patient opt-out approach and transparency of MedicineInsight program information
- The risk regarding the use of personal information, how the program de-identifies patient information and prevents the future re-identification of patient information
- The community and/or public interest in the privacy aspects of the project
- Privacy impacts of possible alternative consent models which may be suggested by the consent model review (conducted separately and in parallel to this PIA).

It is out of scope for IIS to assess:

- NPS MedicineWise's activities and information holdings outside of the MedicineInsight program
- Future legislative amendments committed to by the Commonwealth or state governments which are not in force, or any other obligations which may flow from planned regulations, or past iterations of the MedicineInsight program, such as the proof-of-concept stage
- Detailed technical compliance against Commonwealth cybersecurity and IT infrastructure standards.

2.2 Methodology

Following a planning phase where IIS confirmed its PIA approach with NPS MedicineWise, IIS carried out its work by:

- Gathering information by reading documents and meeting with staff from NPS MedicineWise (see Appendix A)

- Analysing the information against privacy obligations in the applicable privacy laws, the agreements and governance arrangements that will apply, and guidance and best practice on de-identification
- Identifying privacy risks and suggesting ways to mitigate those risks
- Drafting a PIA report and providing this to NPS MedicineWise for comment.
- Addressing feedback and finalising the report.

IIS does not provide legal advice; rather it provides strategic privacy and security advice.

2.3 How to read the report

Section 3 of the report is descriptive and gives contextual information about the MedicineInsight program, key participants and associated data flows.

Section 4 of the report sets out the positive privacy impacts of the MedicineInsight program, through the lens of the Australian Government's Data Sharing Principles.

The PIA analysis is set out in four parts:

- *PART A – Initial considerations* (see Section 5)
  Sets out initial considerations for the privacy analysis, including the threshold question of whether the Privacy Act applies to MedicineInsight data, level of inherent privacy risk and social licence.
- *PART B – Compliance with the Privacy Act and APPs* (see Section 6)
  Discusses possible compliance risk areas and makes recommendations to improve practice. A high-level assessment against each of the APPs is at Appendix B.
- *PART C – MedicineInsight opt-out approach* (see Section 7)
  Assesses the suitability of MedicineInsight's patient opt-out approach; we note that the opt-out model could be improved as a matter of good practice, rather than having to meet a standard of consent (which is not applicable due to the de-identified nature of the data).

  PART D – Re-identification risk (see Section 8)
  Analyses de-identification from a risk management perspective and makes recommendations to reduce re-identification risk.

3. MedicineInsight overview

3.1 About the program

MedicineInsight is a quality improvement program developed and managed by NPS MedicineWise with funding from the Australian Government Department of Health. It comprises a large-scale general practice dataset that supports quality improvement in Australian primary care and post-market surveillance of medicines. MedicineInsight was initially established by NPS MedicineWise in 2011 and ran as a pilot to the end of 2013. Since then, it has transitioned into an ongoing quality improvement program.

Participation in MedicineInsight is voluntary and free of charge. The general practice owner (principal) decides to participate and signs an agreement authorising NPS MedicineWise to use and share data extracts from their practice. This agreement also provides for individual GPs to provide consent and receive individualised practice reports. NPS MedicineWise installs a data extraction tool that is compatible with the practice's clinical information system. The tool extracts data from practice medical records while removing direct identifiers such as patients' name, date of birth and address. The data is securely transmitted and stored in a data warehouse managed by NPS MedicineWise. According to NPS MedicineWise's 2019-20 annual report, 732 practices – comprising over 5,000 GPs – participate in the MedicineInsight, with the dataset holding the de-identified data of approximately 3.2 million regular patients who have attended participating practices.

MedicineInsight data is used for several key purposes as part of its standard operation (which was approved by the RACGP's National Research and Evaluation Ethics Committee in December 2017):

- **Clinical improvement**
  - Clinical improvement reports – Participating general practices receive customised practice reports based on their practice data; NPS MedicineWise may also provide reports to non-participating general practices and PHN partners based on aggregate data that allow for benchmarking at the PHN, state and national levels
  - Education programs – NPS MedicineWise develops and implements a number of education programs each year for primary care clinicians on particular aspects of therapeutics
  - Knowledge and behaviour change outputs – NPS MedicineWise develops content for online learning, its own publications and awareness campaigns based on insights derived from MedicineInsight data
  - Evaluation – NPS MedicineWise evaluates the impact of its own interventions and programs, as well as the MedicineInsight data itself to ensure data quality
- **Data analyses**
  - Department of Health reports – NPS MedicineWise produce routine reports using aggregated data for the Department of Health to inform policies and programs

- Data extracts – Subject to its Data Governance framework, NPS MedicineWise provides data to non-commercial third parties (such as universities, academic organisations, medical colleges and government agencies) in the form of either patient-level data or tabular data
- Insight reports – NPS MedicineWise develops and publishes Insight Reports which are detailed reports based on analysis and interpretation of MedicineInsight data

- **Publications** – NPS MedicineWise develops scientific publications (including abstracts, posters, oral presentations and manuscripts) using analysis and findings from MedicineInsight data.

3.2 Program participants, roles and responsibilities

The parties participating in the MedicineInsight program are as follows:

- **NPS MedicineWise** – Operates the program and ensures that MedicineInsight data is protected and used appropriately
- **Patients** – Individual patients' details (minus their direct identifiers) from participating general practices are collected for the program
- **GPs** – Details of GPs and their medical encounters with patients are collected for the program; GPs receive insights from the program for improving clinical practice
- **Australian Government Department of Health** – Sponsor and funder of the program; develops other health policies and programs based on the insights
- **Royal Australian College of General Practitioners (RACGP)** – Provides ethics approval for the standard operation of the program; members benefit from insights and publications produced by the program
- **Research community** – Conducts, and benefits from, research that uses MedicineInsight data or insights derived from the data; researchers that receive MedicineInsight data are responsible for protecting and using it in accordance with a formal data access agreement, and as approved by the independent data governance committee
- **Health policy makers, primary health networks** – MedicineInsight insights are used by health policy makers, for practice quality improvement and to improve population health. MedicineInsight data assists by identifying weaknesses or gaps, and in understanding where there is a need to commission services, and also support the evaluation of those services.

3.3 Information flows

3.3.1 Nature of the information involved

MedicineInsight collects the following kinds of information:

Practice and provider categories	Examples
Practice	Encrypted unique ID, software, extract date, location
Provider	Encrypted unique ID, consent, profession, status (active/inactive)

Individual patient categories	Examples
Patient	Encrypted unique ID, birth year, sex, demographic information, postcode, pension, year of death
Encounter	Reason for encounter, duration, data, details of each visit
Medical history	Diagnosis, onset date, status (active/inactive), date
Prescriptions	Medicine, reason, history, ATC, product code, frequency, dose, repeats, authority, date
Tests	Tests performed, name, test result received, LOINC code, unit of result, date
Observations	BP, pulse rate, height, weight, BMI, waist circumference, temperature
Risk factors	Smoking and alcohol status and quantified history
Management activities	Referrals, assessment, management plans
Allergies/ADRs	Type, reason, date
MBS service	MBS item numbers
Vaccinations	Name, batch number, date, where administered, ACIR transmission

3.3.2 Overview of information flows and systems involved

The following is a high-level summary of the MedicineInsight information flow:

Participating practices to NPS MedicineWise

- Practice medical records are created and/or updated in the practices' clinical information system as part of primary healthcare delivery
- Once a month, the data extraction software installed in the clinical information system extracts the records while performing the following de-identification functions:
    - Patient names are replaced by a unique ID for each patient
    - Provider identifiers are replaced by a unique ID for each provider
    - Date of birth is aggregated to year of birth
    - Date of death is aggregated to year of death

- Address and telephone number is aggregated to postcode and suburb
- Medicare number, health insurance, bank information and progress notes are not extracted
- Free text fields that are longer than a predetermined threshold (256 characters) are removed.

- The de-identified data is encrypted and transferred to a secure Australian-based data warehouse managed by NPS MedicineWise
  - For each patient record held in the data warehouse, only the delta (i.e., the difference between what is in the existing record and what is in the monthly data refresh) is updated in the patient record.

NPS MedicineWise back to participating practices

- NPS MedicineWise conducts analysis and prepares customised practice reports based on the patient and provider data associated with each practice, as well as benchmarking against aggregate data
  - The reports are delivered via practice meetings and made available online via a personalised practice report repository
  - Practice members can generate patient lists and re-identify those lists via the data extraction software in order to follow up with their own patients (e.g. patients at-risk or undertreated).

NPS MedicineWise to researchers

- A research team applies for access to MedicineInsight data
- The application is approved by NPS MedicineWise's Data Governance process and the research team signs the data access agreement
- For requests involving tabular data:
  - NPS MedicineWise prepares the data – including applying de-identification techniques – so that it is at a summary level that is not capable of re-identifying individuals (e.g., in tables and diagrams)
  - NPS MedicineWise provides the tabular data to the research team, which is provided via zipped, password protected file and secure transfer via email, or secure transfer mechanism as nominated by the customer
- For requests involving patient-level data:
  - NPS MedicineWise prepares the data extract that meets the research team's requirements and applies de-identification techniques
  - NPS MedicineWise transfers the data extract to an approved Secure Research Data Environment (SRDE) that the research team has specified in its application
  - The research team accesses the data extract and conducts analysis within the SRDE

- The research team retains the data extract for up to five years (unless extended by a separate application) and is contractually required to securely dispose of it afterwards.

Other reports and publications

- NPS MedicineWise conducts analysis on aggregate data and prepares various reports and publications; some are provided to specific parties (such as the Department of Health) while others are made publicly available (such as the GP Insight Report).

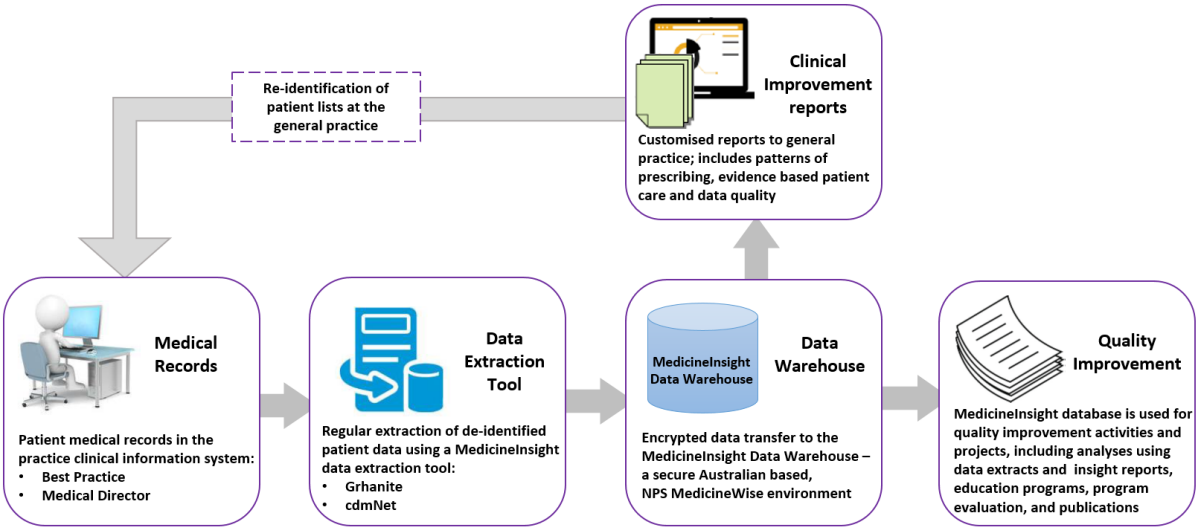

Figure 1: High-level overview of data flows and uses (Source: NPS MedicineWise)

4. Positive privacy impacts

In the context of MedicineInsight's use of de-identified data, IIS has taken the view that the program's positive privacy impacts are best examined by applying the Five Safes Framework, which has been adapted by the Australian Government to become the Data Sharing Principles.[4] The Data Sharing Principles take a risk-based approach to help data custodians share data in a way that delivers public benefit, protects privacy and maintains confidentiality. While NPS MedicineWise is a private entity, the principles are still very relevant as they underpin the broader data ecosystem that NPS MedicineWise will operate in, especially once the Data Availability and Transparency Bill 2020 is passed into law.[5]

The Data Sharing Principles are:

1. **Project** – Data is shared for an appropriate purpose that delivers a public benefit.
2. **People** – The user has the appropriate authority to access the data.
3. **Settings** – The environment in which the data is shared minimises the risk of unauthorised use or disclosure.
4. **Data** – Appropriate and proportionate protections are applied to the data.
5. **Output** – The output from the data sharing arrangement is appropriately safeguarded before any further sharing or release.

Overall, IIS considers that NPS MedicineWise's governance and handling of MedicineInsight data is strong. It has implemented controls in accordance with each Data Sharing Principle. IIS has identified a few areas where NPS MedicineWise can strengthen its approach as a matter of best practice, noting that privacy and de-identification is as much about risk management as it is about compliance with the law. We discuss this further in Section 8.

4.1 Project

Various aspects of the program's design and approval procedures contribute to ensuring that MedicineInsight data is used for an appropriate purpose that delivers a public benefit:

- The MedicineInsight program has received ongoing ethics approval from the RACGP for NPS MedicineWise to use the data for quality improvement purposes.
- NPS MedicineWise has established several expert reference groups to guide how MedicineInsight data is governed and used:
    - Data Governance Committee (DGC) – External and independent committee comprising consumer advocates, data security experts, GPs and researchers that provides oversight and approval of the use of MedicineInsight data.

[4] https://www.pmc.gov.au/resource-centre/public-data/data-sharing-principles

[5] The Five Safes Framework and Data Sharing Principles are also referenced in the MedicineInsight Data Governance Framework.

- Data Development Advisory Group – Advisory body that provides best practice, evidence-based advice to NPS MedicineWise on its big data environment, including matters such as data security, data dissemination and record linkage techniques.
- General Practice Advisory Group – Advisory body that provides independent advice on matters concerning GPs such as clinical practice, governance and secondary use of patient data, comprising academic and practicing GPs.
- Scientific and Publication Review Group – Maintains the NPS MedicineWise Scientific Publications Governance Framework; coordinates and provides oversight of publications, including those that include the use of MedicineInsight data.

- NPS MedicineWise has an established governance process for assessing third party applicants who wish to access, use and share MedicineInsight data, including:
  - Enquiry stage – The applicant discusses their project with the MedicineInsight team, including the aims of the project, project questions and data required.
  - Application stage – The applicant completes a Data Access Application Form that triggers the data governance approval process; the applicant must specify a purpose that is consistent with MedicineInsight's aims[6] and describe how their project will contribute to improving health outcomes for Australians.
  - Approval stage – Applications are sent to the independent Data Governance Committee and New Business Committee for review and approval; the application may be rejected if its purpose(s) meet the exclusion criteria, including data use for:
    - Commercial purposes
    - Performance management of one or more clinicians
    - Conducting compliance audits
    - Publicly benchmarking practices or individual health professionals without their explicit consent
    - Data linkage to workers compensation, private health insurers or Centrelink for compliance or risk purposes
  - Agreement stage – Applicants who require access to patient-level data or tabular data must complete a Data Access Agreement that binds them to only use MedicineInsight data for the specific approved purposes.
- External applicants who require access to patient-level data or tabular data (subject to some exceptions approved by the RACGP HREC) from MedicineInsight for research purposes must obtain their own project-level HREC approval.

[6] They are: (i) quality improvement in primary care, (ii) quality use of medicines and tests, and (iii) improvement in population health and public policy.

- Approved applicants must provide an Annual Report to NPS MedicineWise for the duration of the project, detailing progress and ongoing compliance with requirements.
- Any future linkage of MedicineInsight data to an external dataset will require HREC project ethics approval.

4.2 People

The People Principle is about ensuring that the data user(s) are properly authorised and have the right knowledge, skills and motivations for accessing and using the data. NPS MedicineWise has implemented the following measures for the MedicineInsight program:

- All NPS MedicineWise staff sign a confidentiality deed as part of their employment and undertake information security and privacy training delivered online through an external provider
- Access to MedicineInsight data is restricted to a limited number of authorised persons.[7]
- External parties (typically researchers from tertiary education institutions) must formally apply to access and use MedicineInsight data. As part of the application, they must specify:
    - Who will be involved in, or consulted about, the project, including skill and experience in the following:
        - Practicing in Australian primary care
        - Statistical or epidemiological expertise
        - Handling large datasets
        - Healthcare consumer representation
    - Any other organisations that will have access to MedicineInsight data
- Approved applicants must sign a confidentiality deed and complete a Data Access Agreement that sets out data-related restrictions, conditions and obligations.

4.3 Setting

The Settings Principle considers whether all parties have taken reasonable steps to ensure data will be used in an appropriately safe and secure environment. NPS MedicineWise has implemented the following measures for the MedicineInsight program:

- MedicineInsight data is encrypted during transit and storage; the data warehouse is hosted within an ISO 27001 and IRAP-certified data repository located in Australia.
- MedicineInsight data environments are restricted to authorised persons only.

[7] From time to time, authorised personnel were required to undertake specific privacy and security training relating to MedicineInsight data, although IIS understands this has not been implemented recently. See further Section 6.1.1.

- Patient-level data extracts are only accessible to successful applicants in a Secure Research Data Environment (SRDE) that has been approved by NPS MedicineWise. SRDEs are protected virtual environments with robust security and access controls that hold and enable analysis of sensitive health datasets. Examples of SRDE from the MedicineInsight Data Governance Framework include the Sax Institute's Secure Unified Research Environment (SURE) and BioGrid.
- NPS MedicineWise has policies and procedures for the management of information security incidents and data breaches.
- Approved applicants are required to report data breaches to NPS MedicineWise and to cooperate with NPS MedicineWise to remediate and mitigate the effects of the breach.

4.4 Data

The Data Principle focuses on the treatment or protection applied to the data in order to control the risk of disclosure or (re-)identification. NPS MedicineWise has implemented the following measures for the MedicineInsight program:

- The data extraction tool installed at participating practices removes direct identifiers from patient records before the data is transferred and stored in the data warehouse
- Before providing or reporting tabular data, NPS MedicineWise assesses the risk of re-identification, including requiring a threshold of five or more individuals for contributing to a cell value. For table cells where less than five individuals contribute to the cell value, NPS MedicineWise will take steps to reduce disclosure risk by treating the data, for example:
    - Deletion of variables
    - Cell collapsing
    - Cell suppression.
- Before providing patient-level data, NPS MedicineWise performs the following:
    - Remove the IDs for patients, providers and practices assigned by the data extraction tool and replace them with randomly generated IDs.
    - Suppress sensitive conditions in the following tables: ENCOUNTER_REASON, DIAGNOSIS and SCRIPT_ITEM. These tables are chosen because they contain free text fields that may contain personal information.
    - Check data for small cell counts (<5) (e.g., sex, age groups, Indigenous groups, location, chronic diseases, etc.) and aggregate as necessary.
- The Data Access Agreement sets restrictions on the use of data, including:
    - The data user must not copy or create derivative works unless the action is directly related to the purpose of undertaking the project
    - The data must not be linked with any other datasets unless set out in the Agreement or expressly agreed to by NPS MedicineWise

- The data must not be used to establish the identity of any person or contact any person whose information is contained in the data.

- The data user must only retain and use the data for the agreed period (typically five years) and securely dispose of it at the end of the retention period.

4.5 Output

The Output Principle aims to ensure that the output of the data analysis or sharing is appropriately safeguarded before any further sharing or public release. NPS MedicineWise has implemented the following measures for the MedicineInsight program:

- NPS MedicineWise does not report any information in its publications at the individual patient or practice level that would identify an individual patient or practice.
- The Data Access Agreement sets restrictions on the output of data, including:
  - Where the data user is authorised to copy or make derivative works from the data (i.e. 'secondary data'), they must treat the secondary data on the same basis as the original data
  - The data user must provide NPS MedicineWise with copies of any proposed publications at least one month in advance of submission, so that NPS MedicineWise can check that:
    - The publication does not contain any output with (re-)identification risk
    - There is no 'scope creep' in the research
    - Concepts and terminology are appropriate and understood
  - The data user must not include raw data within any publication.

5. ANALYSIS PART A – Initial considerations

In this section, IIS sets out the initial considerations for its privacy analysis, including:

- The threshold question of whether the Privacy Act applies to MedicineInsight data
- The inherent privacy risk associated with MedicineInsight data
- Community and public interest in, and acceptance of, programs of this nature (i.e., social licence).

5.1 Application of the Privacy Act to MedicineInsight data

NPS MedicineWise is subject to the Privacy Act, which regulates personal information.

For the purposes of this PIA, which focuses on MedicineInsight data, the threshold question is whether this data meets the definition of 'personal information'. If the information is personal information, the APPs will apply. Under the Privacy Act, personal information means:

> …information or an opinion about an identified individual, or an individual who is reasonably identifiable: whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.[8]

MedicineInsight collects personal information about GPs and their staff, and health information about patients. IIS notes that the Privacy Act provides extra protection for sensitive information, which includes 'health information about an individual'.[9]

The information about practitioners identifies the individual practitioner and that constitutes personal information under the Privacy Act. The MedicineInsight patient data is also clearly health information when collected and held by GPs. However, NPS MedicineWise is seeking to only extract de-identified patient information from GP systems. That said, the data is unit-level data, is quite detailed, and capable of being matched longitudinally and/or with other data sets. IIS discusses the potential re-identification risks at Section 8.

IIS considers that the MedicineInsight data is unlikely to qualify as personal information as long as NPS MedicineWise carefully manages any re-identification risks. In this regard, IIS notes that there have been isolated instances of personal information in the free text fields in the past (and even unintentionally disclosed to researchers). Potentially, this may happen again in the future, especially as this is a constantly-refreshing dataset.

5.1.1 NPS MedicineWise's portrayal of its privacy obligations

IIS understands that because of its appreciation of the sensitivity of the data, and its concern to adopt best practice, NPS MedicineWise is treating de-identified patient-level data *as if* it was subject to the Privacy Act. IIS strongly supports this as the correct (cautious) position to take. However, we also

[8] Privacy Act, s 6(1).

[9] Privacy Act, s 6(1)

consider that it should be clear to all internal and external stakeholders, as well as to the community at large, that this is NPS MedicineWise' choice, not a legal obligation.

In making the comments below, IIS is not suggesting that NPS MedicineWise retreat from its strong stance on privacy and security protection. Rather we are encouraging it to find clearer ways to communicate its approach.

In undertaking this PIA, IIS reviewed a wide range of NPS MedicineWise materials. In many cases – including in the information for GPs and the agreements they have with NPS MedicineWise, on posters for patients which would be displayed at GP practices, in patient brochures and on opt-out forms – there is no suggestion that the NPS MedicineWise privacy protection standards as they apply to de-identified patient data are required by the Privacy Act.

However, in other places the messaging appears to convey that the Privacy Act applies to the MedicineInsight program. For example:

- The NPS MedicineWise website's section on privacy, security and governance for the MedicineInsight program states that "We collect, use and store MedicineInsight information strictly in line with Australian privacy laws…"[10]
- The MedicineInsight Data Governance Framework (DGF), page 5, provides that 'MedicineInsight complies with the Privacy Act 1988 and the 13 Australian Privacy Principles (APPs) which apply to NPS MedicineWise as an "APP entity".'
- The MedicineInsight training material notes at page 3 in respect of MedicineInsight data, 'This information is considered by law as "sensitive personal health information" which must be governed and managed in a systematic, transparent and judicious manner.'

These excerpts give the impression that all MedicineInsight data is personal information. The statements are correct in so far as the use of GP personal information, but not patient information. While IIS understands NPS MedicineWise appreciates the distinction – it clearly states in other places that MedicineInsight data is de-identified – the messaging could be clearer. IIS noted similar issues in discussions about consent and the opt-out model – see Section 7.

Recommendation 1 – Ensure NPS MedicineWise correctly portrays the status of MedicineInsight de-identified patient data under the Privacy Act

Develop clear statements about the status of MedicineInsight's de-identified patient data under the Privacy Act, and about NPS MedicineWise's choice to treat the data as though the Privacy Act does apply.

Review internal and external materials, including the NPS MedicineWise website, and the DGF, and amend as needed to accurately reflect the status of MedicineInsight data.

Type: Best practice**, Priority**: Low, **Resource**: Medium

[10] NPS MedicineWise website, MedicineInsight: Privacy, Security and Governance at https://www.nps.org.au/medicine-insight/privacy-security-governance

5.2 Inherent privacy risks

Inherent privacy risks arise from the nature of the health or personal information held, for example, its sensitivity or potential for misuse, and how it is held and managed, including the privacy control environment.

The MedicineInsight data, stripped of direct identifiers, might be considered to carry low or no inherent privacy risks. However, IIS considers this is likely to understate the risk. MedicineInsight data is characterised by:

- A large and increasing data holding – it involves:
  - Personal information about medical practitioners from 732 GPs
  - Unit-level health information about over three million regular patients from the GPs enrolled in the MedicineInsight program; there will be a risk, depending on the circumstances, that the information could be re-identified, with potentially significant impact on any affected individuals
- A longitudinal view of aspects of patient health
- Sharing of data, under controlled conditions, with researchers
- Potential for data linkage with other data sets.

IIS's indicative assessment in the context of this PIA is that MedicineInsight data would have medium inherent privacy risk, which is reduced to very low when the various layers of de-identification measures are applied (thus becoming de-identified information in those protected contexts).

5.3 Community interest and social licence

The Data Futures Partnership in New Zealand has done pioneering work into social licence in the context of trusted data use, and puts it like this:[11]

> When people trust that their data will be used as they have agreed, and accept that enough value will be created, they are likely to be more comfortable with its use. This acceptance is referred to as a social licence.

MedicineInsight program uses de-identified information and so is not subject to the Privacy Act. While this does not guarantee NPS MedicineWise a social licence to continue to collect and use GP data, there is a level of community support for the use of de-identified health information in the public interest. For example, a survey in 2017 by the NSW Information and Privacy Commission found that:

- A survey in 2017 by the NSW Information and Privacy Commission found that:
  - A majority of respondents agreed with using potentially identifiable health information for: research purposes (58%), planning and delivering government services (56%),

[11] Data Futures Partnership, 'A Path to Social Licence: Guidelines for Trusted Data Use' (2015) <http://datafutures.co.nz/our-work-2/talking-to-new-zealanders/>.

help government agencies develop new policies (55%) and help monitor the quality of government services (54%)

- 37% agreed that government providers should be able to make it a condition of obtaining the service that they can use their health information for other purposes; this increases to 52% if they are told that it will be fully de-identified.[12]

- A 2020 Research Australia survey found that:
  - The use of de-identified medical records for research is strongly supported by more than one third (35.8%) and somewhat supported by 47%. Only 17.2% of people are opposed.
  - Support for the use of medical records where individuals can be identified is lower but still high. 22.5% strongly support this, and 43% somewhat support it. The total who are opposed is a little over one third (34.6%).[13]

However, there is also increasing experience (e.g., the 2016 'Census fail', My Health Record opt-out) that social licence can be strongly adversely affected when there is insufficient communication or consultation or when something goes wrong (e.g., the re-identification of 'de-identified' Medicare Benefits Scheme records by researchers at the University of Melbourne in 2016). For MedicineInsight, social licence could be eroded by insufficient or unclear information about the program, or a significant data breach.

IIS has taken community interests and taken social licence into account in our analysis. Our recommendations, which go 'beyond compliance', aim to assist NPS MedicineWise in building and maintaining its social licence.

[12] Information and Privacy Commission, 'NSW 2017 Community Attitudes Towards Privacy Report' (27 June 2017) <https://www.ipc.nsw.gov.au/news-media/news/nsw-2017-community-attitudes-towards-privacy-report>.

[13] Research Australia, 'Public Opinion Poll on Health & Medical Research and Innovation' (2020), p 13 <https://researchaustralia.org/reports/public-opinion-polling-2/>.

6. ANALYSIS PART B – Compliance with the Privacy Act and APPs

This section of the report considers the requirements of the Privacy Act and its APPs and identifies privacy risks for the MedicineInsight program taking account of the Act. The assessment undertaken is a privacy risk assessment. By its nature the assessment is high-level and indicative. It is not an audit or other assurance type of activity.

Although NPS MedicineWise is not legally obliged to comply with the APPs for the de-identified patient data aspects of the MedicineInsight program, IIS understands it seeks to apply the APPs to assist it to manage privacy risks and as a matter of good practice.

For this PIA, IIS considered how each of the APPs would apply to MedicineInsight, on a 'best practice' analysis taking account of NPS MedicineWise's privacy and information management approaches. Its assessment is at Appendix B. The possible risk areas are discussed in more detail below.

6.1 APP 1 – Open and transparent management of personal information

APP 1 requires organisations to put in place governance measures to ensure privacy compliance and have a clearly expressed and up-to-date privacy policy.

6.1.1 Privacy governance

This section considers NPS MedicineWise privacy governance arrangements generally.

IIS undertook a high-level review of relevant documents, and it also compared the NPS MedicineWise's approach to that suggested in the OAIC's privacy management framework (PMF),[14] in particular:

- Step 1 – Embed: a culture of privacy that enables compliance, and
- Step 2 – Establish: robust and effective privacy practices, procedures and systems.

The OAIC framework acknowledges that privacy compliance is not 'one size fits all'. The steps needed should take account of each organisation's activities and privacy risks. For MedicineInsight, its main risks are the potential for re-identification or other security incidents that result in significant data breaches, and the resulting impact on individuals as well as NPS MedicineWise's reputation and its ability to maintain good relationships with its stakeholders if its privacy protection measures are not sufficiently robust.

[14] OAIC Privacy Management Framework, at https://www.oaic.gov.au/privacy/guidance-and-advice/privacy-management-framework-enabling-compliance-and-encouraging-good-practice/

IIS considers that NPS MedicineWise's privacy governance policies and procedures are likely to largely meet the requirements of APP 1; together they should help ensure MedicineInsight could comply with the APPs taking account of the potential privacy risks.

The arrangements include:

- A senior manager – Manager, Legal, Governance & Risk – responsible for privacy and designated as the Privacy Officer.
- Chief Technology Officer – responsible for general oversight and management of cybersecurity risks as identified by the NPS MedicineWise information security specialist.
- he DGF which sets principles, accountabilities and outlines the general approaches including in relation to data management and processes and procedures, and which covers many of the matters the OAIC would include in a PMF.
- Additional specific policies for:
    - Risk management
    - Information security
    - Information classification and handling policy
    - Information System Incident Management
    - Data Breach Response.
- General training on the Privacy Act and APPs.

NPS MedicineWise provided a privacy training program document specifically for staff working with MedicineInsight data. However, it advised that this program is no longer run for reasons which are not recorded.

6.1.1.1 Tailored training and Risk Management Framework

IIS's review of the NPS MedicineWise privacy training materials and of its risk management framework indicates they could be strengthened in a few areas. In particular, IIS considers that NPS MedicineWise should re-establish specific MedicineInsight privacy training, including leveraging training from reputable parties such as the ABS. We consider the Risk Management Framework could identify privacy (and re-identification) risks as needing particular attention.

6.1.1.2 Data inventory and Privacy Management Plan

There are actions from the OAIC's PMF that NPS MedicineWise could be considered in terms of organisation-wide improvements that would benefit MedicineInsight. The actions are:

- Keeping information about the organisation's business's personal information holdings (data inventory including the type of information held and its location) up-to-date

- Developing a privacy management plan (PMP) to a tool to assist organisations to assess the current state of their privacy practices and set privacy goals and targets.[15]

IIS understands that NPS MedicineWise does not have a current complete inventory of its information holdings. IIS encourages NPS MedicineWise to undertake a risk assessment of this activity, to assist it to decide if it would be a useful addition to its privacy governance approach.

IIS considers that a PMP would provide a useful way for NPS MedicineWise to check that it has a strategic view of its privacy risks and that these are being managed. IIS's review (including discussions with NPS MedicineWise staff) indicated a genuine concern to manage MedicineInsight data appropriately, however, it appeared that measures in place to assess the effectiveness of management strategies tend to be ad hoc rather than systematic.

For example, although NPS MedicineWise staff in interviews were fairly confident the DGF is implemented as outlined, this is not systematically monitored. IIS was advised that privacy will be on internal audit agenda in 2020-21, with issues to be scoped then. NPS MedicineWise staff indicated that overall there are limited resources and so, while a lot has been done in terms of building the privacy governance structure, monitoring and assurance tends to be reactive rather than proactive.

6.1.1.3 Shared risk

According to the Federal Department of Finance, a shared risk 'extends beyond a single entity. It is a risk that emerges from a single source and impacts interrelated objectives of entities.'[16]

In our increasingly complex and connected world, shared risk is a common feature of projects and initiatives. For example, many worthwhile programs – including MedicineInsight – require the participation of multiple parties from different sectors. Furthermore, the ICT components of such programs often rely on contracted service providers and a broader supply chain.

The management of shared risk presents challenges, as outlined in the following table:

Distinguishing features of shared risk[17]	Implications for MedicineInsight
A shared risk may have no naturally apparent owner and no one entity may be able to manage the risk on their own	It is important to identify who has (shared) ownership and responsibility for managing each identified privacy risk (as the risk could be unstated, confused or not assigned at all)
Shared risks can have complex causes, and can be influenced by the actions and inaction of a range of participants in different ways	MedicineInsight stakeholders may cause the risk (in terms of contributing to its occurrence) and/or mitigate the risk (in terms of existing controls and potential treatments)

[15] The OAIC website offers information about PMPs and a PMP template, which could be used as a guide <https://www.oaic.gov.au/privacy/guidance-and-advice/privacy-management-plan-template-for-organisations/>.

[16] Department of Finance, 'Understanding and Managing Shared Risk' (2016).

[17] Ibid.

Distinguishing features of shared risk[17]	Implications for MedicineInsight
Should a shared risk be realised, it can affect different parties in different ways	The consequences of privacy risk may impact not only individuals but also the reputation of MedicineInsight stakeholders and the government's broader goal of deriving benefit from valued datasets

In the context of MedicineInsight, shared privacy risks may arise throughout the data lifecycle as data is collected by GPs from patients, extracted by software, stored in NPS MedicineWise's data warehouse, accessed and used by data users (both internal and external), and in the future, potentially linked to other significant datasets.

More concretely, NPS MedicineWise shares some risks and mitigations with GPs (in relation to opt-out management, avoiding the inadvertent collection of personal information, ensuring usernames and passwords for data extraction tools are kept secure) and with its research community (in ensuring MedicineInsight data is handled and used only in accordance with agreements with NPS MedicineWise).

At a higher level, privacy risk is influenced by 'macro' factors that have a downstream effect on the extent to which MedicineInsight data is properly used, protected and governed. These factors include:

- The growing scale and complexity of the shared privacy risk environment over time – for example, more participating practices contributing data, more data sharing, more data linkage, etc.
- Unclear lines of responsibility and accountability for overall shared privacy risk governance
- Increasing appetite to leverage MedicineInsight data, including more use cases and greater volume of use overall
- Lack of resources for implementing protective operational and governance arrangements, and for conducting assurance activities.

IIS considers that NPS MedicineWise is well-placed to play a leading role to identify and coordinate potential responses to shared privacy risks for MedicineInsight, as it sits in the middle of the data 'ecosystem' created by the program. We encourage NPS MedicineWise to identify, assess and document possible shared privacy risks and to actively collaborate with relevant stakeholders in managing such risks.

Recommendation 2 – Strengthen privacy governance measures

(a) Taking account of NPS MedicineWise's privacy objectives, and identified risks, reintroduce specific MedicineInsight privacy training.

(b) Amend the Risk Management Framework to specifically identify privacy risks, including re-identification risks.

(c) Undertake a risk assessment on the need for a data inventory and, if needed, develop and keep up-to-date the inventory.

Recommendation 2 – Strengthen privacy governance measures

(d) Ensure, by using a Privacy Management Plan or other mechanisms, that NPS MedicineWise has a strategic oversight of privacy risks and management practices and that these are systematically monitored.

(e) Identify, assess and document shared privacy risks (e.g., in relation to GPs, the research community, linkage partners, the Department of Health, etc.); NPS MedicineWise to actively collaborate with relevant stakeholders on the management of shared privacy risks and continually strengthen where possible as risks are identified.

Type: Strengthen compliance, **Priority**: Medium, **Resource**: High

6.1.2 Privacy policy

NPS MedicineWise's website includes a detailed privacy policy, which is dated February 2017.[18] IIS reviewed the policy from the perspective of its application to the MedicineInsight program.

The policy does not name MedicineInsight but it does provides that:

> As part of its services, NPS MedicineWise offers health professionals the opportunity to undertake quality assurance activities that require them to collect health information about individuals and disclose it to NPS MedicineWise on a de-identified basis for quality assurance purposes.[19]

The policy gives a brief indicative overview of how NPS MedicineWise protects and uses the de-identified information.

There is no specific requirement in the Privacy Act for organisations to address handling of de-identified information so NPS MedicineWise is doing more than needed by mentioning its activities in this area. However, the current explanation does not cover the scope of the MedicineInsight program, for example as described in the MedicineInsight DGF:

> MedicineInsight was initially established by NPS MedicineWise in 2011 as a mechanism to support post-market medicine surveillance. Access to pooled electronic health records, stored in general practice clinical information systems also provides an important data resource which has the potential to contribute significantly to primary care policy, health research and quality improvement activities.[20]

[18] The policy viewed is at https://www.nps.org.au/privacy

[19] NPS MedicineWise Privacy Policy, paragraph 7.3

[20] NPS MedicineWise MedicineInsight Data Governance Framework, page 5

Moreover, the explanation seems unlikely to help patients understand that information about them is collected into the MedicineInsight database. It also does not specifically mention disclosures to external bodies for research or data linkage.

IIS considers that a more detailed explanation, specifically mentioning the MedicineInsight program, would better support NPS MedicineWise's transparency and best practice objectives.

Recommendation 3 – Update privacy policy to specifically address MedicineInsight

Update privacy policy to provide an overview of the MedicineInsight, its data, and how this is de-identified, shared and disclosed for quality improvement, evaluation, research and data linkage.

Ensure the privacy policy:

- Provides clear information about the application of the Privacy Act to MedicineInsight
- Explains NPS MedicineWise's intentions with respect to patient interests and wishes by offering them the facility to opt out of the data collection
- Explains how patients may opt out.

Type: Best practice, **Priority**: High, **Resource**: Low

6.1.3 Transparency

APP 1 is overall intended to promote the open and transparent handling of personal information. IIS therefore considered the information about MedicineInsight, in addition to its privacy policy, that NPS MedicineWise makes available on its website, particularly from the perspective of its likely utility in informing patients about how unit-level information about them could be handled.

In addition to a high-level overview of MedicineInsight, IIS notes that NPS MedicineWise also provides:

- Copies of reports, for example, General Practice Insights Report 2017-18 and 2018-19
- A list of approved projects using MedicineInsight data.[21]

IIS considers that the website could provide more information for patients and community members to assist them to better understand the program and how MedicineInsight data is protected, used and disclosed. IIS understands NPS MedicineWise is now considering options in this regard, including for:

- A more user-friendly website
- More information on the MedicineInsight governance framework

[21] https://www.nps.org.au/approved-projects-using-medicineinsight-data

- More information on the work of the DGC, including summaries of its decision and its members.

IIS supports these approaches and does not have additional recommendations to make.

6.2 APP 3 – Collection of solicited personal information and consent requirements

APP 3 protects privacy by setting limits on the collection of personal and sensitive information. It provides that organisations must:

- Only collect personal information that is reasonably necessary for their functions and activities
- Use fair and lawful means to collect information and collect from the individual concerned unless unreasonable or impractical.

In addition, organisations must have consent to collect sensitive information, including health information, unless exceptions apply.

IIS assessed the MedicineInsight program against the obligations in APP 3 (see Appendix B). We consider that MedicineInsight complies with APP 3. In particular, we consider that NPS MedicineWise does not need consent to collect de-identified patient data.

6.3 APP 11 – Security of personal information

APP 11 requires organisations to take steps that are reasonable in the circumstances to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

The OAIC specifically encourages organisations handling de-identified information to take reasonable steps to protect it and to minimise the risk of unauthorised access or loss that could lead to re-identification.[22]

IIS considers that security is a significant risk area for NPS MedicineWise. A cyber security breach of any scale is likely to have a strong impact on trust in NPS MedicineWise and its reputation. It could massively impact on patients if unit-level data accessed. IIS understands that NPS MedicineWise takes these risks seriously; it has recently expanded its IT security capacity and has an uplift plan in place.

This section considers NPS MedicineWise's security approach generally. It takes into account that the MedicineInsight program holds personal information about practitioners, as well as de-identified unit-level data about patients.

[22] See: OAIC, 'De-identification and the Privacy Act' (March 2018) <https://www.oaic.gov.au/agencies-and-organisations/guides/de-identification-and-the-privacy-act> and 'Publication of MBS/PBS data: Commissioner initiated investigation report' (23 March 2018) <https://www.oaic.gov.au/resources/privacy-law/commissioner-initiated-investigation-reports/publication-of-mbs-pbs-data.pdf>.

It was out of scope for IIS to undertake a detailed technical assessment against Commonwealth cybersecurity and IT infrastructure standards. However, IIS reviewed information about NPS MedicineWise's security approaches, and discussed this with staff. On the whole, IIS considers NPS MedicineWise has sound security practices.

IIS has identified some issues that indicated areas where some additional steps might be needed to strengthen the approach for protecting the MedicineInsight data holdings. These are as follows.

6.3.1 Monitoring compliance with security policies and procedures

IIS understands from discussions with staff that there are possible gaps in the procedures to manage access to MedicineInsight data.

For example, IT might not know when someone moves from one team to another team, with the risk that a staff member might have more access than needed. Staff further mentioned that in some cases, resource constraints means it is not possible to maintain full separation of duties for the extraction and preparation of data to be provided to an external party.

IIS also understands that although access to information in the data warehouse, or held in other systems, is logged, there is no routine review of the logs. We appreciate the points made in discussions that generally access is limited to highly-trained professional staff, and that the nature of work means extensive and varied access is needed, making it difficult to identify any pattern of misuse.

6.3.2 Managing internal movements of data

Discussions with NPS MedicineWise staff indicated that an inventory of its systems exists, but does not include a comprehensive inventory of all data, where it is held, or how it moves within the organisation. The development of a data inventory has been considered but IIS understands that the risk/resource balance has so far meant this action has not been taken. A data inventory is usually considered best practice when managing personal information. See IIS's **Recommendation 2(c)** above.

6.3.3 Managing third party contracts

IIS considered aspects of NPS MedicineWise's management of its third-party service providers, especially around assurance. NPS MedicineWise advised that it has a right of audit with Precedent, but not with the University of Melbourne for the Grhanite extraction tool. It has asked for agreement on a bilateral right and will seek to include it when the contract is being updated. We encourage NPS MedicineWise to check that its procurement process builds in privacy provisions (including right of audit) into third party contracts and that they are appropriately monitored.

NPS MedicineWise advised that it also has a standard contract which includes privacy provisions. Any departure is assessed by its Legal section. There is no rolling program to assess compliance with privacy provisions. Responsibility for monitoring contracts, including compliance with provisions, lies with the contract manager, or other named person.

6.3.4 Data retention

IIS understands that the MedicineInsight patient-level dataset would be retained permanently. The dataset would include information about GPs, including those that have withdrawn from the MedicineInsight program. NPS MedicineWise states in its practice agreement that it 'will retain and continue to use data already collected from that General Practice, however, this data will never identify the practice, or any healthcare professional, staff or individual patient of the practice'.

IIS notes that the NPS MedicineWise Data Classification and Handling Policy includes a data retention policy. The policy does not specifically address the retention of MedicineInsight data, including personal information about GPs. IIS encourages NPS MedicineWise to review its policy to ensure retention of MedicineInsight data is appropriately covered in the policy.

6.3.5 Managing shared risks with GPs

As already flagged (see Section 6.1.1.3), NPS MedicineWise has some exposure to shared risks from its relationships with participating GPs. For example, it relies on GP's to keep the keep extraction tool passwords and username secure and to maintain practice data security. It sets requirements in this regard in practice agreements. These also include provisions for mutual advice on data breaches.

IIS understands NPS MedicineWise undertakes some monitoring of GP practices in the course of GP quality reviews, but it does not audit practice agreements. In discussions with staff there was some concern about GPs' approaches to managing data, privacy and security. We encourage NPS MedicineWise to assess whether its current activities in this area are sufficient to manage risks and to rectify if necessary.

Recommendation 4 – Strengthen security with some additional measures

(a) Improve access controls so that staff can only access data relevant to their role; ensure this is checked and maintained over time.

(b) Take steps to quantify risks from internal movements of data and institute more access controls and audits as needed.

(c) Review procurement policy and ensure that privacy provisions (including right of audit) are built into third party contracts.

(d) Review data retention policy to ensure identified information about practitioners is de-identified once identifying information is no longer needed.

(e) Review risk assessments at GP level and develop strategies to manage identified risks.

Type: Strengthen compliance, **Priority**: Medium, **Resource**: Medium

7. ANALYSIS PART C – MedicineInsight opt-out approach

IIS was asked to comment on the suitability of the MedicineInsight's patient opt-out approach. IIS emphasises that NPS MedicineWise is not seeking to collect identified patient health information. It therefore does not need patient consent for its collection. NPS MedicineWise is also not intending for the opt-out model to be taken as a consent process. IIS makes the observations in this section from the perspective that the opt-out model is a matter of good practice and respect for individuals' privacy, rather than NPS MedicineWise having to meet a standard of consent.

In making our comments, IIS first of all considered the approach from a 'theoretical' perspective taking account of:

- The Privacy Act consent standard
- Provisions in the Privacy Act that apply where organisations are collecting, using or disclosing health information for the purposes of research, compilation or analysis of statistics and the management of health services, where it is impractical to get consent or use de-identified information.

The aim here was to assess the opt-out approach, and variations between it and the Privacy Act consent standard, to help inform IIS' analysis.

We then considered NPS MedicineWise's objectives for its opt-out approach and made some observations that should assist NPS MedicineWise to better meet its objectives.

7.1 Theoretical assessment of the MedicineInsight opt-out approach

7.1.1 The Privacy Act consent provisions

The Privacy Act provides that consent can be express or implied.[23] The OAIC's APP guidelines set out four key elements of consent, which are that:

- The individual is adequately informed before giving consent
- The individual gives consent voluntarily
- The consent is current and specific
- The individual has the capacity to understand and communicate their consent.[24]

The guidelines note that 'use of an opt-out mechanism to infer consent will only be appropriate in limited circumstances. The conditions under which consent can be implied include that:

[23] Privacy Act s 6.

[24] OAIC guidelines to the APPs, Chapter B, key concepts, [B.35]

- The opt-out option was clearly and prominently presented
- It is likely the individual received and read the information
- The opt-out process is easy to exercise
- The consequences of failing to opt-out are not serious.[25]

7.1.2 Consent waiver processes

Organisations seeking to collect identified health information need to take steps to gain patient consent or they would need a consent waiver.[26] IIS considers whether the MedicineInsight opt-out approach would meet consent requirements in the following section.

To get a consent waiver, the organisation in question would generally need to apply to an ethics committee and both the organisation and the ethics committee would need to comply with the s 95A guidelines.[27] The section 95A guidelines establish a process for ethics review. They specify what information must be included in a proposal to an HREC and require the proposal to refer to the relevant section of the Privacy Act. The guidelines also set out what matters the HREC must consider in making its decision. These include why it is impractical to gain consent, and the public interest in the activity proceeding versus the risks to privacy and other interests.

The NHMRC National Statement on Ethical Conduct in Human Research is also relevant and is referenced in the s 95A guidelines. The National Statement sets out general requirements for consent and how consent might be qualified or waived. It notes that 'the opt-out approach is unlikely to constitute consent when applying commonwealth privacy legislation to the handling of sensitive information, including health information.[28]

Subject to this qualification, the National Statement contemplates the use of opt-out mechanisms to infer consent, for example, where the scale and significance of the research means that using explicit consent is neither practical nor feasible.[29] The conditions where opt-out might be used include:[30]

- Where involvement in the research is low risk for the participants
- The public interest in the proposed activity substantially outweighs the public interest in the protection of privacy
- Reasonable attempts are made to provide all prospective participants with appropriate information.

---

[25] Ibid, [B.40].

[26] See Privacy Act, APP 3.4(c) and s 16B(2).

[27] Privacy Act, s 95 provides for similar guidelines for Commonwealth agencies

[28] NHMRC National Statement on Ethical Conduct in Human Research, Chapter 2.3, p 19.

[29] Ibid, paragraph 2.3.5, page 20

[30] Ibid, paragraph 2.3.6, page 21

7.1.3 Assessment of the MedicineInsight opt-out model

NPS MedicineWise's current opt-out model involves requiring GPs to display a poster advising patients about the MedicineInsight program and that they can opt-out, to provide additional information for patients in a brochure, and to offer, and process, an opt-out form on a patient's request.[31]

NPS MedicineWise also provides information about the MedicineInsight program on its website.

IIS considers that the existing measures could meet some, but not all, of the requirements that would allow informed choice to be inferred. In particular, IIS considers that it would be difficult to say with confidence that individuals had 'received and read the information'. We therefore consider the opt-out approach would be unlikely to meet the requirements for consent for collection and use of identified personal information in terms of the Privacy Act. For similar reasons, it might be difficult for the MedicineInsight program, if it involved identified health information, to meet the opt-out requirements in the National Statement.

Importantly, as already indicated, MedicineInsight is using de-identified information and therefore there is no requirement for NPS MedicineWise to get patient consent to collect the information.

7.2 Better practice for the opt-out approach

Best practice is to give individuals as much choice and control over their information as possible. Measures that strengthen patient choice include ensuring transparency of data flows and giving individuals the option not to participate.

Although NPS MedicineWise is not required to seek consent, it nevertheless seeks to conduct the MedicineInsight program transparently and to respect patient privacy; the opt-out model is an important mechanism in this regard.

As indicated earlier, IIS considers that the current model opt-out model, which relies on GPs to display posters, provide brochures and action opt-out requests, would not meet the Privacy Act consent standard. However, we also understand that NPS MedicineWise is now assessing if there are ways the opt-out model could be strengthened to meet is its privacy and transparency objectives.

IIS appreciates that devising an appropriate opt-out model does have significant challenges. NPS MedicineWise relies on practices to implement the approach. Although it sets out requirements in its practice agreements, it works with over 700 GPs. The GPs are universally time-poor and have varying levels of privacy understanding. IIS understands that GP privacy and security practices vary massively in terms of their policies and procedures and accountability for data.

There would also be risks if the opt-approach is 'too successful' – for example, reducing data quality and introducing biases in the data. On the other hand, if the approach is considered token, or lacks transparency, it will be harder to maintain social licence to collect and use the data.

[31] These conditions are included in the MedicineInsight Participating General Practice Agreement

7.2.1 NPS MedicineWise's current activities to strengthen the opt-out approach

IIS acknowledges the considerable work NPS MedicineWise has done, and is doing, is this area. In addition to its current consent model review, its activities include the following:

- Establishing a Consumer Advisory Group (CAG)
- Establishing an independent DGC
- As noted in the NPS MedicineWise proposal to the RACGP ethics committee, testing patient poster and information sheet with consumers, and privacy experts for readability and appropriateness. This includes review and endorsement of modifications by a second Ethics group Bellberry Ltd HREC.[32]
- Undertaking research and participating in discussion about its approaches, including for opt-out. These included:
    - NPS MedicineWise research, 2013, on specific questions including opt-out approach and information about the MedicineInsight program. Recommendations included emphasising the benefits of the program and sending clear messages
    - Consumers Health Forum of Australia and NPS MedicineWise. Engaging consumers in their health data journey. Canberra: CHF and NPS MedicineWise, 2018.
- NPS MedicineWise CAG and DGC discussion about MedicineInsight governance, transparency and consent.

IIS has seen draft recommendations from NPS MedicineWise's consent model review. We strongly support the directions, in particular, which seek to:

- Ensure NPS MedicineWise understands more about how the opt-out approach is working at the GP level, and captures and provides more public information on the number of opt-out requests.
- Encourage GP conversations with patients about MedicineInsight and its benefits.
- Provide more, and more easily accessible, information about the MedicineInsight program on the NPS MedicineWise website.

IIS identifies below some areas that we consider would further strengthen the approach.

7.2.2 Complementing the NPS MedicineWise work on opt-out

7.2.2.1 Patient awareness of the opt-out option

IIS does not have the expertise to suggest an appropriate balance between quality research and risks in informing individuals about opt-out options; that will be a matter for NPS MedicineWise and its stakeholders. However, we suggest that it would be helpful to have a target in mind by which to

[32] MedicineInsight: Proposal for Ethics Approval, Royal Australian College of General Practitioners National Research And Evaluation Ethics Committee, November 2017, p 21.

assess the efficacy of the opt-out approach. A target would not necessarily focus on the number of people opting-out. Rather, it might be level of awareness of the opt-out option, or of practice involvement in the MedicineInsight program. IIS notes in this regard the recent Australian National Audit Office (ANAO) review of the implementation of the My Health Record System. The implementation involved a very extensive communication campaign and the ANAO found that awareness of the opt-out option increased from 16.5% to 69.2% over an eight month period.[33]

7.2.2.2 GP action to support awareness

IIS notes that GPs are sharing de-identified information with NPS MedicineWise. While such disclosure by GPs of de-identified information would not be subject to the Privacy Act, part of the transparency strategy could be to encourage GPs as a matter of best practice to include information about the MedicineInsight program in privacy policies or privacy statements.

7.2.2.3 NPS MedicineWise's portrayal of its opt-out approach

Although NPS MedicineWise is not obliged to get consent and is not seeking to portray the approach as a consent model, IIS found, in reviewing materials for the PIA, that this message is not always clear.

Importantly, IIS considers that NPS MedicineWise's basis for offering patients an opt-out are reasonably clear in the MedicineInsight Participating General Practice Agreement (Practice Agreement), and the information for patients (see Appendix C).

However, in other places the messaging could convey that the MedicineInsight program is consent-based or is relying on a 'consent waiver'. For example:

- In its ethics proposal to the RACGP, in arguing that the program is low risk, information about the opt-out mechanism is included under the heading 'consent'
- The DGF, page 5, provides that the *Privacy Act 1988* also provides the basis for MedicineInsight consent arrangements, and outlines conditions where it is not practicable to obtain individual consent.
- The DGF, section 1.2, Principles of consent, notes that patient consent is not required but justifies the opt-out approach by reference to the NHMRC National Statement.

IIS strongly supports NPS MedicineWise's approach of offering an opt-out. However, it would be preferable if it made clear that this is a matter of respect for patient's preferences, and is not intended as a consent mechanism, nor endorsed by a consent waiver.

[33] The Auditor-General Report No.13 2019–20 Performance Audit *Implementation of the My Health Record System,* of the Australian Digital Health Agency and Department of Health, 2019, Chapter 2, 'were communication strategies appropriate', pp 27-29.

Recommendation 5 – Ensure opt-out approach is transparent, portrayed as best practice and not consent, and supported by positive messages about the MedicineInsight program

IIS strongly supports the approach in the draft recommendations for the NPS MedicineWise consent model review. To complement the expected recommendations:

- Avoid references to consent and consent waivers when describing the opt-out model in written materials or in discussions
- Ensure conversations about the opt-out model are based on accurate portrayals of its intent and basis
- In discussions and written materials, including for patients and GPs, be transparent about the possible implications for the data quality and data bias if the opt-out model leads to a significant reduction in participation
- **In consultation with stakeholders, set criteria to measure the efficacy of the opt-out approach. These might include, for example, level of patient awareness of the opt-out option**
- Work with GPs to identify ways to promote conversations with patients about the benefits of their data being included in data sets such as MedicineInsight
- Amend the practice agreement to, at least, encourage and preferably to require, GPs to include advice about involvement in the MedicineInsight program on their websites, in privacy policies and in privacy notices
- Continue to work with key stakeholders, including DOH, the RACGP, NHRMC and consumers, to develop resources to assist GPs and consumers to make informed decisions to allow (or not allow) use of their information in programs such as MedicineInsight.

Type: Best practice, **Priority**: Varies, **Resource**: High

NB: Priority depends on NPS MedicineWise's timeframe for implementing recommendations from its consent model review.

8. ANALYSIS PART D – Re-identification risk

8.1 De-identification and risk management

Given the acceleration of data availability and use across sectors, de-identification is becoming an increasingly important tool for deriving benefits from data use while preserving privacy. According to the OAIC, whether information is personal or de-identified depends on the context:[34]

> Information will be de-identified where the risk of an individual being re-identified in the data is very low in the relevant release context (or data access environment). Put another way, information will be de-identified where there is no reasonable likelihood of re-identification occurring. [Emphasis added]

The OAIC considers de-identification to involve two steps:

- Firstly, the entity should remove direct identifiers (such as name, date of birth and contact details)
- Secondly, the entity should take one or both additional steps:
  - Removal or alteration of other information ('quasi-identifiers') that could potentially be used to re-identify an individual
  - The use of controls and safeguards in the data access environment to prevent re-identification.

The OAIC and CSIRO-Data 61 have produced the *De-Identification Decision-Making Framework*,[35] which is a comprehensive guide for de-identification in accordance with the Privacy Act. In anticipation of the national data sharing framework that will be enabled by legislation, the Department of Prime Minister and Cabinet (PM&C) has produced the *Best Practice Guide to Applying Data Sharing Principles* which takes a holistic approach to de-identification.[36] For the remainder of this report, IIS refers to the resources mentioned in this section as the 'de-identification guidelines'.

Common across all the de-identification guidelines is the idea that de-identification is a risk management exercise. It is not always possible to draw a bright line between personal and de-identified information, hence NPS MedicineWise's cautious approach to treating MedicineInsight data as if it was personal information subject to the Privacy Act. IIS notes that the MedicineInsight DGF references the above guidelines and commits to the principle of functional de-identification. We commend NPS MedicineWise for this approach.

---

[34] https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/

[35] https://data61.csiro.au/en/Our-Research/Our-Work/Safety-and-Security/Privacy-Preservation/De-identification-Decision-Making-Framework

[36] https://www.pmc.gov.au/sites/default/files/publications/data-sharing-principles-best-practice-guide-15-mar-2019.pdf

IIS sees de-identification risk management playing the following roles for NPS MedicineWise and in particular its MedicineInsight program:

- To enable the sharing and release of information – including both MedicineInsight data (in tabular and patient-level form) and insights derived from such data
- To reduce the risk that personal information will be compromised in the event of unauthorised access, use, distribution or data breach

To build trust and meet community expectations around the safe handling of patient data that is collected indirectly from participating general practices.

8.2 Maintaining de-identification of MedicineInsight data

IIS starts from the position that patient-level data that has been stripped of direct identifiers by the data extraction tool continues to carry a medium level of re-identification risk. As noted above (see Section 5.2 on inherent privacy risks):

- MedicineInsight data comprises very detailed and longitudinal health data pertaining to millions of patients – this makes the data susceptible to re-identification when placed in another context
- Should the information become re-identified (especially in bulk), there could be significant impacts to affected individuals and NPS MedicineWise.

This is consistent with OAIC's advice that removal of direct identifiers is a necessary first step, but is not sufficient on its own to achieve de-identification. As discussed above in Positive Privacy Impacts (see Section 4), IIS considers that NPS MedicineWise has also implemented a range of controls and safeguards in line with the Data Sharing Principles to further reduce the risk of re-identification for MedicineInsight data to a very low level.

In the rest of this section, IIS discusses ways in which NPS MedicineWise can further strengthen its approach.

8.2.1 MedicineInsight data access by external parties

From the perspective of MedicineInsight's standard operations, managing de-identification risk is most relevant when making data available to external parties. As noted in Positive Privacy Impacts, this is mostly done well through NPS MedicineWise's implementation of the five Data Sharing Principles. In particular, there is a robust process for approving potential projects and patient-level data is accessible only in an approved SRDE setting.

People Principle

With respect to ensuring that data users are properly authorised and have the right knowledge, skills and motivations for accessing and using MedicineInsight data, NPS MedicineWise requires applicants to provide information on who will be involved in, or consulted about, the project. This includes skill and experience in statistics and handing large datasets.

However, IIS understands that NPS MedicineWise does not provide specific training to external parties who will access MedicineInsight data, nor does it currently mention training in its Data Access Application Form and Data Access Agreement.

In its *Best Practice Guide to Applying Data Sharing Principles*, the Department of PM&C has an extended discussion of user training in its section on the People Principle. It observes that:[37]

> International and Australian experience in data sharing has shown that the main cause of data breaches is people making mistakes when using data rather than failures of technology or deliberate misuse. For example, a user who has been given individual access to a secure dataset assumes they can share their access with a colleague who is not authorised to access the same dataset.

The guide goes on to say that training is an effective approach to minimise mistakes and that it should constitute the following:

- Ensuring everyone understands their obligations and responsibilities
- Emphasising positive behaviours and attitudes that facilitate proper data use
- Raising both the legal and non-legal consequences of data misuse.

NPS MedicineWise should develop and implement training, or if this is not possible due to resource or practicality reasons, it should take other steps to ensure that external parties applying for access to patient-level MedicineInsight data receive relevant training. For example, IIS understands that researchers who use SURE (which is one of the approved SRDEs) are required to participate in mandatory training, including training in privacy and confidentiality regulatory regimes and in the principles of statistical disclosure control. NPS MedicineWise could leverage these and other training opportunities available to external parties to strengthen the training element of its formal data access arrangements.

Recommendation 6 – Include data user training as a requirement of MedicineInsight data access

For data access involving patient-level data:

- Include in the Data Access Application Form a field for the applicant to confirm that data users have received training on protecting the privacy and confidentiality of unit-level datasets (and if not, why not; and what they plan to do about it)
- Include in the Data Access Agreement, as one of the Data User safeguards, that project personnel with direct access to the Data must have received training on protecting the privacy and confidentiality of unit-level datasets.

Type: Best practice, **Priority**: Medium, **Resource**: Low

[37] Guide, p 16

Data Principle

The need to apply treatment or protection to the data (in addition to stripping direct identifiers) will depend on what the data is used for and the environment it is released into. The de-identification guidelines recognise a trade-off in treating the data itself, since making alterations to the data in order to preserve privacy (e.g. rounding, perturbation, suppression, etc.) may significantly reduce its utility.

In the context of MedicineInsight, there are two ways that its data is made available – tabular and patient-level – and they are accompanied by different approaches to data treatment.

For tabular data, the goal is to provide a summary (i.e. not patient-level) view of the data. Therefore, de-identification techniques are required to ensure that the data is aggregated and not capable of being re-identified. IIS has reviewed a high-level description of its de-identification procedure for tabular data in NPS MedicineWise's 2017 ethics application to the RACGP for MedicineInsight, which includes deletion of variables, cell collapsing and cell suppression for table cells where fewer than five individuals contribute to a cell value.[38] This is useful not just for providing data to researchers, but also for NPS MedicineWise's own analyses and publications.

For patient-level data, the goal is to provide detailed and high quality data for researchers to analyse. Therefore, the focus is less on treating the data itself (which could reduce its utility) but rather relying on the layers of risk management in accordance with the other Data Sharing Principles such as Project and Setting. However, one important and necessary step in protecting the privacy of the patient-level data extract is to remove or suppress any free text fields that could contain personal information. IIS has reviewed the excerpt of a de-identification procedure for data extracts which addresses this by including a step for suppressing three tables (ENCOUNTER_REASON, DIAGNOSIS and SCRIPT_ITEM) that contain free text fields.

In the course of conducting the PIA, IIS was provided a report prepared for NPS MedicineWise by CSIRO, 'Confidentiality Procedures in Data Extraction for MedicineInsight' (the CSIRO Report) dated 28 July 2015. The CSIRO Report comprehensively covers the kinds of data involved, the actual and potential activities that rely on MedicineInsight data, overview of confidentiality protection measures, and recommended confidentiality procedures for both tabular and patient-level data. In discussions with IIS, NPS MedicineWise reported that it was unsure of the status of this report and whether standard operating procedures (SOPs) have been developed taking into account the CSIRO advice.

IIS makes the following further observations:

- The CSIRO advice is only mentioned once, in the 2017 RACGP ethics application
- The de-identification procedure excerpt provided to IIS is written at a high level (e.g. "Check data for small cell counts") and does not make a clear distinction between treatment of tabular and patient-level data
- There has been at least one disclosure incident where a research team received personal information (names) in the IMMUNISATION data table, within the CONSENT_PROVIDER

[38] Ethics application, p 20.

variable; the de-identification procedure reviewed by IIS did not address this potentially vulnerable data table.

Overall, IIS considers that NPS MedicineWise should improve the documentation of its de-identification procedures. Clear and detailed procedures make training and onboarding easier, promotes consistency of practice, and allows NPS MedicineWise to demonstrate (both internally and externally) that it has a considered approach to de-identification. This reduces the risk of a re-identification event that could expose NPS MedicineWise to compliance and reputational consequences.

Recommendation 7 – Update the documented de-identification procedures

Update the current de-identification procedures:

- Make a clear distinction between the steps required for tabular data vs patient-level data
- Be specific in the procedures about the decisions and steps (e.g., specify what is a small cell count, such as <5)
- Review the CSIRO Report and determine which recommended confidentiality procedures can be adopted; where a different approach is proposed, explain why.

Once the procedures have been updated and formalised into an SOP, conduct periodic refresher training on the SOP, along with the above-mentioned specific training on the MedicineInsight program (see **Recommendation 2(a)**).

Type: Best practice, **Priority**: High, **Resource**: Low

8.2.2 Ongoing review of de-identification

As with all risk management, de-identification is a dynamic process that must be monitored and updated over time. In its *Best Practice Guide to Applying Data Sharing Principles*, the Department of PM&C notes that the context for a data sharing arrangement may change over time, as well as the projects, users, organisations, technology and public expectations involved. Therefore, "a clear review process should be built into all governance, reporting and assurance arrangements."[39]

In its de-identification guide, the OAIC states that good data governance procedures should apply at all stages of the process and provides a list of indicative activities – IIS has set these out as follows, along with observations on how they are, or could be, operationalised by NPS MedicineWise:

- **Ongoing and regular re-identification risk assessments (to check that methods used are still effective and appropriate at managing the risks involved)**

  Based on discussions with NPS MedicineWise, IIS understands that it currently does not do this. We recognise that this kind of assessment will need to take into account the operating context of MedicineInsight and the resources available to NPS MedicineWise. Nevertheless,

[39] Department of PM&C, *Best Practice Guide to Applying Data Sharing Principles*, p 29.

it would be advisable for NPS MedicineWise to incorporate this kind of periodic assessment into its strategic oversight of privacy risks and management practices. (See **Recommendation 8** below and also **Recommendation 2(d)** above)

- **Auditing data recipients to ensure that they are complying with the conditions of any data sharing agreements**

  Data recipients are required to provide an Annual Report to NPS MedicineWise for the duration of the project, including their ongoing compliance with data sharing requirements. NPS MedicineWise informed IIS that due to resource constraints, it does not systematically audit existing data users although it has commenced audits this year. The Data Access Agreement does give NPS MedicineWise the right to audit the data user and obliges the data user to provide reasonable assistance.

- **Considering new information that becomes available, and whether any such information increases re-identification risk in a particular data access environment**

  Although IIS did not assess this directly for NPS MedicineWise as an organisation, we found through consultations that staff are knowledgeable and motivated in keeping up with new information including threats and mitigations to do with re-identification risk. It would be good to include this topic as a regular (perhaps half-year or yearly) discussion item for the data governance and analytics teams.

- **Building and ensuring ongoing transparency around the entity's de-identification practices**

  NPS MedicineWise has taken active steps in considering how to improve transparency as part of its consent model review; IIS discusses this further in Section 7.5. We consider that clear and accessible information about MedicineInsight's de-identification practices should be part of the communication package.

- **Ensuring that your entity knows who is accountable for de-identification internally**

  Based on the roles and responsibilities table in MedicineInsight's DGF, there are Specialist Advisor and Data Processor roles whose responsibility includes 'curates, deidentifies, and manages data outputs'. The ultimately accountability for de-identification appears to be the role of the Data Custodian (held by the Deputy Chief Executive Officer), although this is not specified but inferred by the description ('understands and accepts business ownership and accountability for MedicineInsight data').

- **Putting in place a plan to deal with any re-identification attacks or events (this could be part of your entity's broader data breach response plan)**

  There is one document ('MedicineInsight Training – Privacy and Security', currently inactive) that mentions the situation when a staff member finds an unexpected occurrence of personal information. How NPS MedicineWise prepares for and handles such situations could be improved – see further discussion in the following Section 8.2.3.

- **Ensuring that in-house staff who undertake de-identification have adequate and up-to-date training, and/or ensuring appropriate external expertise is sought where appropriate**

  IIS has found that currently NPS MedicineWise does not conduct specific MedicineInsight privacy training, which would include topics such as de-identification. We have made recommendations to rectify this – see especially **Recommendations 2(a)** and **8**.

Recommendation 8 – Build in de-identification review into regular assurance cycle

Incorporate periodic re-identification risk assessment as part of the strategic oversight of privacy risks and management practices, to ensure that MedicineInsight's de-identification regime remains fit-for-purpose. NPS MedicineWise should tailor the frequency based on its capacity and contextual factors (such as emergence of technologies that could exacerbate or mitigate re-identification risk).

Type: Best practice, **Priority**: Low, **Resource**: Medium

8.2.3 Personal information within MedicineInsight data

In addition to managing the de-identification of MedicineInsight data broadly, NPS MedicineWise also has to deal specifically with the issue of personal information that is inadvertently retained within the patient-level data. Due to the extensive number of records and practices involved, the variability of how data is entered in practice (e.g., in free text and other unexpected fields), as well as the ongoing nature of data collection – it is inevitable that MedicineInsight will inadvertently collect some amount of personal information.

This is not a hypothetical exercise. As noted above in Section 8.2.1, NPS MedicineWise recorded an information security and privacy incident whereby personal information was discovered in a MedicineInsight data extract provided to a research team. In this case, the team discovered six names in the IMMUNISATION data table, within the CONSENT_PROVIDER variable.

The presence of personal information within the MedicineInsight dataset is problematic as it undermines NPS MedicineWise's publicly-stated position that it only collects de-identified information about patients.

IIS considers that NPS MedicineWise's approach to functional de-identification and its public claims of MedicineInsight data being 'de-identified' are not necessarily incompatible with isolated incidences of personal information collection. The OAIC's standard is not perfection but rather that the entity is committing to de-identify data and taking reasonable steps to prevent the re-identification of data.

Having said this, IIS considers that NPS MedicineWise could strengthen its response to a re-identification event, or the discovery of identifying information. At least one document, 'MedicineInsight Training – Privacy and Security', contemplates this situation. It notes that if staff discover personal information in the dataset, that they should treat it as a reportable incident. However, IIS was informed that this document is inactive and has not been used in recent times.

During the information gathering phase, NPS MedicineWise advised that it is currently preparing some guidance material for its data analysts in relation to this situation. IIS considers that this is a good opportunity to formalise the approach in an active policy/procedure.

Recommendation 9 – Clarify and formalise procedure for responding to (re-)identification incidents, in the context of incident management reporting processes

Include specific mention of (re-)identification incident (i.e., when an internal or external data user discovers personal information in the MedicineInsight data) in a relevant internal document, for example the Information System Incident Management Policy or the Data Breach Response Plan. Develop a procedure for responding to the incident, including:

- The reporting and escalation process
- What will be done with the information (e.g. deletion, contacting individual(s) whose data may have been affected by a breach or re-identification incident)
- The record-keeping, review and improvement process.

Type: Strengthen compliance, **Priority**: High, **Resource**: Low

In the longer term and as a matter of pursuing best practice, IIS considers that NPS MedicineWise should explore options for proactively finding and removing personal information remnants from the incoming extracted data. That is, in addition to the initial removal of direct identifiers, NPS MedicineWise should aim to cleanse all (potentially) problematic fields from its data tables.

There is a market of software-based de-identification solutions that are compatible with both on-premise and cloud data warehouses. It would be necessary to have a solution that is dynamic, since the dataset is longitudinal and changes over time with addition of new information.

Recommendation 10 – Explore software-based solutions for managing de-identification risk

Explore software-based solutions to streamline the identification and removal of data fields that contain personal information within the MedicineInsight data set.

Type: Best practice, **Priority**: Low, **Resource**: Low

9. Appendix A – Methodology

IIS took a consultative, practical and strategic approach to the consultancy and worked closely with the relevant staff of NPS MedicineWise at all stages. In planning and undertaking the PIA, IIS drew on international best practice and its own depth of experience in conducting PIAs. IIS also ensured that the PIA was consistent with the OAIC's PIA Guide.

The PIA work involved the following stages:

- Planning – In this stage, IIS finalised the methodology in consultation with NPS MedicineWise
- Information gathering and meetings – The main objective of this stage of the PIA was to ensure that IIS had a sufficient understanding of MedicineInsight program to conduct our assessment. IIS also sought to understand the data flows, technical controls, assurance processes and governance structures. IIS gathered information by reading relevant documents and holding meetings with NPS MedicineWise. The documents reviewed and meetings held are listed below.
- Analysis and data mapping – Following the information-gathering stage, IIS mapped the data flows and identified and analysed privacy issues taking into account the Privacy Act's APPs as well as against broader privacy considerations including risk management and community expectations
- IIS produced a high-level summary of findings containing our initial analysis and preliminary recommendations as requested by NPS MedicineWise
- Draft and final PIA – Following our analysis, IIS developed our recommendations and drafted the PIA report. IIS provided the draft PIA report to NPS MedicineWise for review and feedback. We then finalised the report taking into account NPS MedicineWise's feedback.

9.1 Documents reviewed

Documents reviewed
NPS MedicineWise documents
Accessing MedicineInsight Data Products – Frequently Asked Questions (September 2018)
Confidentiality Deed – Access to MedicineInsight Data
Confidentiality Procedures for Data Extraction or MedicineInsight (22 July 2015)
Consultation recommendations to be finalised late November
Data Breach Management Plan
Data Dictionary (Internal Only) Sep 2020
Data Governance Committee – Terms of Reference

Documents reviewed
De-identification procedure – MedicineInsight data extract process
Developing data linkage capability within the MedicineInsight data set – Project Protocol (March 2020)
Engaging consumers in their health data journey (March 2018)
Ethics approval correspondence relating to MedicineInsight program
External Environment Assessment
External Approval Letter examples and templates
Guide for Data Access Application Form (May 2019)
Information Classification and Handling Policy
Information Security and Privacy Incident Report (#003)
Information Security and Privacy Incident Report (#004)
Information Security Incident Response Plan
Information Security Policy
Information System Incident Management Policy
Internal Approval Letter examples
Item 2.11 Combined CAG DGC discussion notes
MedicineInsight Data Access Amendment Form
MedicineInsight Data Access Annual Report
MedicineInsight Data Access Agreement templates
MedicineInsight Data Access Application Form (May 2020)
MedicineInsight Data Access Assessment Form (October 2020)
MedicineInsight Data Access Enquiry Form
MedicineInsight Data Book (June 2020)
MedicineInsight Data Governance Framework (March 2020)
MedicineInsight Privacy and Security Governance Flyer
MedicineInsight Privacy Impact Assessment (Draft) (February 2013)
MedicineInsight Privacy Impact Threshold Assessment and Scope for the Department of Health (August 2020)
MedicineInsight Proposal for Ethics Approval for Royal Australian College of General Practitioners, National Research and Evaluation Ethics Committee (November 2017)
MedicineInsight Report – Consumer Focus Groups (March 2013)

Documents reviewed
MedicineInsight team diagram
MedicineInsight Training – Privacy and Security (February 2015)
Personal Information incident process ProMapp
Recommendations for the consent review
Risk Management Framework
Other documents
CSIRO, Confidentiality Procedures in Data Extraction for MedicineInsight (28 July 2015)
Data Resource Profile: MedicineInsight, an Australian national primary health care database
NHMRC, Statement on Consumer and Community Involvement in Health and Medical Research

9.2 Meetings held

Meetings held	
Kick-off meeting	1 October 2020
Information gathering meeting – Health Intelligence Manager	20 October 2020
Information gathering meeting – Senior Epidemiologist	20 October 2020
Information gathering meeting – Lead Epidemiologist	21 October 2020
Information gathering meeting – Data Custodian (Deputy CEO)	21 October 2020
Information gathering meeting – Cybersecurity Advisor	2 November 2020
Information gathering meeting – Data Analytics Lead	2 November 2020
Information gathering meeting – Business Growth Manager	4 November 2020
Information gathering meeting – Data Governance Specialist	9 November 2020
Information gathering meeting – Data Governance Specialist	11 November 2020
Information gathering meeting – Legal Counsel	11 November 2020

10. Appendix B – Assessment against the APPs

NPS MedicineWise collects information about practitioners, including practitioner names and other details; this information is clearly personal information and subject to the Privacy Act.

IIS's view is that subject to steps to manage de-identification risk, the Privacy Act will not apply to de-identified patient information collected for the MedicineInsight program. However, it appreciates that NPS MedicineWise is keen to understand to what extent its practices would meet compliance obligations under the Act so that it can ensure it is applying best practice to its collection and handling of MedicineInsight data.

The table below considers the application of all APPs to MedicineInsight data. In accordance with the PIA scope, the focus is on MedicineWise data (about practitioners and patients). However, where relevant, for example in relation to APP 1, IIS has also considered NPS MedicineWise data handling approaches more generally.

Privacy principles (summary)	Possible risks – patient data	Possible risks – GP data
APP 1 — Open and transparent management of personal information Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy. APP entities must also take reasonable steps to implement practices, procedures, and systems relating to ensure compliance with the APPs	Privacy governance – NPS MedicineWise takes a range of steps to ensure compliance with the APPs. IIS considers there are some possible gaps, for example, NPS MedicineWise does not have a formal PMP. See Section 6.1.1 for discussion and recommendations. Privacy policy – NPS MedicineWise's privacy policy is generally consistent with OAIC guidance on privacy policies; preferably it would be updated, as it was last reviewed in 2017. The privacy policy provides reasonably clear information about the collection of information about practitioners, but does not mention MedicineInsight specifically, and could provide a clearer explanation of its collection and handling of both practitioner and de-identified patient data. See Section 6.1.2 for better practice suggestions	
APP 2 — Anonymity and pseudonymity Requires APP entities to give individuals the option of not	APP 2 not applicable for patient data. NPS MedicineWise is not collecting identified patient information	If a practice chooses to participate in MedicineInsight, NPS MedicineWise will be collecting personal information about GP staff. Staff are given notice, but will not have the option of anonymity/pseudonymity at point of collection. However, their consent will be sought before any identified information is

Privacy principles (summary)	Possible risks – patient data	Possible risks – GP data
identifying themselves, or of using a pseudonym. Limited exceptions apply.		included in reports back to the practice or in other specified circumstances. Otherwise, no identified information will about practitioners will be included in reports or shared. No compliance issues identified.
APP 3 — Collection of solicited personal information Outlines when an APP entity can collect personal information that is solicited – the personal information must be reasonably necessary for one or more the entities' functions and activities. APP 3 applies higher standards to the collection of 'sensitive' information. Entities should also collect directly from the individual concerned unless it is unreasonable or impracticable.	IIS has not identified compliance risks against APP 3 for MedicineInsight patient data. The data collected seems necessary for the purpose. In the circumstances, it would be impracticable to collect the information directly. The APP 3 requirement to have consent before collecting sensitive (including health) information unless exceptions apply, does not apply to de-identified information. NPS MedicineWise does not need consent to collect MedicineInsight data but it does offer patients an opt-out mechanism, on a best practice basis. See discussion and recommendations at Section 7.	IIS has not identified compliance risks against APP 3 for MedicineInsight practitioner information. The information collected seems reasonably necessary for the purpose. Although NPS MedicineWise collects information about practice staff indirectly, its likely to be unreasonable/impractical to collect directly. In addition, the Practice Agreement requires GP to inform staff about involvement in MedicineInsight and give them opportunity to read material.
APP 4 — Dealing with unsolicited personal information Outlines how APP entities must deal with unsolicited personal information.	Appears to be no mechanism for NPS MedicineWise to receive unsolicited information – not applicable	
APP 5 — Notification of the collection of personal information Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.	NPS MedicineWise does not need to comply with APP 5 when collecting de-identified information. If considering APP compliance, the question would be whether NPS MedicineWise was taking reasonable steps to let people know about the collection. IIS considers that more steps would be preferable. See Section 6.1.2 and Section 7 IIS notes that GPs are sharing de-identified information with NPS MedicineWise. While it's unlikely they have direct	NPS MedicineWise would need to consider APP 5 when collecting personal information about practitioners. APP 5 applies both to information about individuals collected from them, as well as information collected from third parties (as is the case when NPS MedicineWise is collecting information about staff of GPs). IIS considers the Healthcare Professional Information Sheet, which the Practice Agreement requires participating practices

Privacy principles (summary)	Possible risks – patient data	Possible risks – GP data
	obligations under the APPs, it would be best practice to include information about the MedicineInsight program in privacy policies or privacy statements. See Section 7.5	to give to their staff, addresses the relevant matters in APP 5.2. The Information sheet explains the purpose of collection, further uses and disclosures, and provides a link to the NPS MedicineWise privacy policy. No compliance issues identified
APP 6 — Use or disclosure of personal information Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.	NPS MedicineWise is collecting MedicineInsight information to assist GPs by providing reports on prescribing, data quality, and clinical activity. It also uses and discloses de-identified information for purposes of research and evaluation including: ● Chronic disease and other conditions ● Quality use of medicines, such as antibiotics ● Post market surveillance of medicines ● Delivering medical education ● Evidence for PBS listings.[40] IIS considers that NPS MedicineWise's use and disclosure of MedicineInsight data would be for the purpose for which it was collected or for secondary purposes which, if they involved identified health information, would come within the Privacy Act's permitted general situations for health information.[41] Subject to specified conditions, organisations are permitted to use and disclose health information for research or compilation of statistics relevant to public health or safety, or the management, funding or monitoring of a health service. No compliance issues in the current approach. However, if NPS MedicineWise was using identified health information, it	The analysis for GPs is similar. IIS notes that use or disclosure of identified information about GPs and their staff is likely to be consistent with the primary purpose of collection but is also consent-based. No compliance issues identified.

[40] MedicineInsight proposal for Ethics Approval, Appendix 7 Appendix 7 - Healthcare Professional Information Sheet.

[41] Privacy Act, s 16B

Privacy principles (summary)	Possible risks – patient data	Possible risks – GP data
	would need to consider consent or the other mechanisms in s 16B. It would be up to NPS MedicineWise and relevant ethics bodies to make specific decisions against the provisions. (See also discussion on NPS MedicineWise's application of the Five Safes at Section 4 and its opt-out mechanism at Section 7)	
APP 7 — Direct marketing An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.	MedicineInsight patient data would not allow for direct marketing as it does not contain details. No compliance issues identified	NPS MedicineWise does not engage in any direct marketing activities – no compliance issues identified.
APP 8 — Cross-border disclosure of personal information Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.	Not applicable – NPS MedicineWise ensures MedicineInsight data held within Australia	
APP 9 — Adoption, use or disclosure of government related identifiers Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.	NPS MedicineWise takes steps to avoid collection of patient identifiers such as Medicare Numbers, practice ID numbers – no compliance issues identified.	NPS MedicineWise collects various identifiers for practitioners, including Prescriber number, Provider number, RACGP/ACCRM number, Registration number and HPI-I. HPI-I is a government related identifier and its use is authorised by Healthcare Identifiers Act 2010. No compliance issues identified.

Privacy principles (summary)	Possible risks – patient data	Possible risks – GP data
APP 10 — Quality of personal information An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.	NPS MedicineWise undertakes validation and other activities to improve the quality of the data it collects for MedicineInsight. Its activities do not impact patients directly. GP practice reports might contain information about identified practitioners, however, this is subject to their consent. No compliance issues identified.	
APP 11 — Security of personal information An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.	It was out of scope for IIS to undertake a detailed technical assessment against Commonwealth cybersecurity and IT infrastructure standards. IIS reviewed information about NPS MedicineWise security approaches, and discussed approaches with staff. On the whole, IIS considers the approach is consistent with sound security practices. It identified some areas where some additional activities could strengthen compliance. See Section 6.3	
APP 12 — Access to personal information Outlines an APP entity's obligations when an individual makes a request for access to personal information held about them by the entity. This includes a	Not applicable – NPS MedicineWise does not have identified data about patients	The Healthcare Professional Information Sheet includes a link to the NPS MedicineWise privacy policy, which provides information about access and correction. No compliance issues identified.

Privacy principles (summary)	Possible risks – patient data	Possible risks – GP data
requirement to provide access unless a specific exception applies.		
APP 13 — Correction of personal information Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.	Not applicable – NPS MedicineWise does not have identified data about patients	As above

11. Appendix C – Extracts from MedicineInsight patient poster, brochure and consent form

The following is a summary of the information elements of the MedicineInsight opt-out mechanism:

- Patient poster

  Provides information about: what information MedicineInsight collects; how does MedicineInsight use the information; how this practice uses the information; how to get more information about MedicineInsight. Provides information about how to opt out.

  'If you do not want the information in your medical record to be included in MedicineInsight, you can choose to opt out of the program at any time. Opt-out forms are available at reception. Choosing not to take part in MedicineInsight will not affect the medical care that you receive in any way.'

- Patient information sheet

  Your choice – NPS MedicineWise and the staff in this practice respect if you choose not to take part in MedicineInsight. If you do not want this practice to continue to share information from your medical record with MedicineInsight, you can opt out of the program at any time by filling out the form overleaf and giving it to reception. Choosing not to take part in MedicineInsight will not affect the medical care that you receive in any way.

- Patient consent form

  I acknowledge that:

  I have read and understood the MedicineInsight patient information sheet.

  I have had the opportunity to ask questions about MedicineInsight. The program has been explained to me, and my questions have been answered to my satisfaction.

  I understand that if I opt-out, the practice will stop releasing my non-identifiable information to MedicineInsight.

  I know that the signed opt-out form will be kept at this medical practice and not shared with NPS MedicineWise.

  I understand that under the Australian Privacy Act (1988), NPS MedicineWise has the authority to retain and use non-identifiable information already collected.

  My medical care will not be affected by my choice not to participate in MedicineInsight.

  I want to opt-out of the MedicineInsight program

INFORMATION
INTEGRITY
SOLUTIONS

Information Integrity Solutions Pty Ltd
PO Box 978, Strawberry Hills NSW 2012, Australia
P: +61 2 8303 2438
F: +61 2 9319 5754
E: inquiries@iispartners.com
www.iispartners.com

ABN 78 107 611 898
ACN107 611 898