Prepared for the Australian Commission on Safety and Quality in Health Care

Our ref: 25000161
22 July 2025

Supplementary Privacy Impact Assessment – MedicineInsight Program

1. The Australian Commission on Safety and Quality in Health Care (**Commission**) requests advice about privacy issues arising from the MedicineInsight Program (**the Program**).

2. In this supplementary privacy impact assessment (**PIA**), we have assessed the privacy issues or risks that arise in the Program, and recommend steps the Commission can take to address them.

Summary

3. We have reviewed the Program documentation supplied to us by the Commission, and undertaken a 'gap analysis' to consider any legislative and regulatory changes that have taken place in the past four years to minimise or mitigate any risk of adverse privacy impacts to individuals.

4. Our advice makes 8 recommendations. The key recommendations are to strengthen consent and notice provided to general practitioners, update the privacy policy, reduce the amount of unstructured data that can be collected and to take reasonable steps to improve data quality.

5. If our recommendations are implemented, in addition to those of the previous PIA completed in relation to the Program, we think the Program will comply with the Australian Privacy Principles (**APPs**) in Sch 1 to the *Privacy Act 1988* (**Privacy Act**).

Recommendations

6. Our recommendations indicate the nature of the risk using the following flags:

STOP	**Compliance risk**: The Commission should implement this recommendation to ensure compliance with the requirements of the Privacy Act.
	Privacy protection: Implementation of this recommendation will minimise privacy risk and improve privacy protections.

#	Recommendation	Flag
1	Review and update privacy policy	STOP
2	Update GP consent form to ensure valid consent	
3	Limit collection of unstructured data where practicable	STOP

4	Consider opportunities to strengthen the opt-out process	
5	Update Program information to address APP 5.2 matters	
6	Take steps to ensure GP data is accurate and up to date	
7	Develop a shared approach to data breach response	
8	Implement additional measures with respect to CSPs	

Next steps

7. We recommend the Commission implement the recommendations in this advice as soon as practicable.

Reasons

8. This advice is based on our understanding of the activities and personal information flows are set out in Annexure A. which we derived from the information the Commission supplied to us about the Program (see Material).

9. In preparing this advice, we also considered the relevance of the *Data Availability and Transparency Act 2022* (**DAT Act**) and the recent amendments to the Privacy Act arising from the *Privacy and Other Legislation Amendment Act 2024* (**Privacy Amendment Act**).

Assumptions

10. We do not think the Program involves any new or changed ways of handling personal information to the information handling practices described in the NPS MedicineWise program as examined in the 2021 NPS MedicineInsight PIA (**NPS PIA**).

11. This assessment is based on the following assumptions:

    11.1. the Program involves the same data elements, and deidentification, collection and opt in processes, as the program when it was previously the subject of a PIA

    11.2. transition to the Commission has not resulted in any significant changes to the handling of patient data or general practitioner (**GP**) personal information

    11.3. the Commission intends to implement any relevant recommendations from the NPS PIA, as set out in Annexure B.

APP 1 – Review and update privacy policy

12. APP 1.3 requires an agency to have a clearly expressed and up-to-date privacy policy addressing the matters set out in APP 1.4.

13. The Commission's privacy policy (last updated February 2024) does not currently refer to the Program. To the extent the Commission will collect and handle personal information about GPs as part of the Program, and will handle de-identified patient data, the Commission's privacy policy should be updated to address relevant APP 1.4 matters, including:

13.1. the kinds of GP personal information collected and held: **APP 1.4(a)**

13.2. how GP personal information is collected and held: **APP 1.4(b)**

13.3. the purpose for which GP personal information is collected, held, used and disclosed, including that de-identified patient data from participating practices will be collected with the patient's consent: **APP 1.4(c)**.

Recommendation 1 – Review and update privacy policy	
	In addition to implementing NPS Recommendation 3, the Commission should review and update its privacy policy to reflect the information handling practices of the Program.
Response:	Agree

APP 3 – Collection of GP personal information

14. APP 3 provides that the Commission must not collect personal information unless it is reasonably necessary for, or directly related to, one or more of its functions.

15. As we understand it, the Commission primarily collects GP personal information in order to provide customised reports for participating practices. Information collected is combined with data from other general practices across Australia to form a database, which enables the Commission to compare and discover trends in diagnoses, treatments, and outcomes of general practice patients at a national level. The reports are used to assist the general practice with the provision of patient care informed by data in the reports.

The Commission's functions

16. The Commission is an independent statutory authority funded jointly by the Australian Government and State and Territory governments. The Commission's role, functions and responsibilities are governed by the *National Health Reform Act 2011* (Cth) (**NHR Act**)

17. The Commission's functions that are relevant to the Program, in summary, are:

17.1. to promote, support and encourage the implementation of arrangements, programs and initiatives relating to health care safety and quality matters: s 9(1)(a)

17.2. to collect, analyse, interpret and disseminate information relating to health care safety and quality matters: s 9(1)(b)

17.3. to publish reports and papers relating to health care safety and quality matters: s 9(1)(d)

17.4. to consult and co-operate with other persons, organisations and governments on health care safety and quality matters s 9(1)(m).

17.5. to do anything incidental or conducive to the performance of any of the above functions: s 9(1)(q)

Collection of GP data reasonably necessary for the Commission's functions

18. To the extent the Commission collects limited GP personal information in medical reports extracted from the practices' CIS as part of Activity 5, we think the collection of limited GP personal information for the delivery of the Program is 'reasonably necessary' or 'directly related' to the performance of the Commission's functions, specifically those set out in s 9(1)(a)-(b) of the NHR Act.

19. Further, the 'indirect' collection of GP personal information (from the practices) will be authorised on the basis that it would be impracticable to collect this information directly from individuals: APP 3.6(1)(b). GPs are to be notified about this collection as part of the practice agreement.

Collection of optional GP data with consent

20. We understand that the Commission also collects 'optional GP data' to facilitate individualised reports for consenting GPs in Activity 2. This collection is also directly related to the delivery of the Program which is reasonably necessary for the Commission's functions under s 9(1)(a)-(b).

21. The Commission obtains consent to collect 'optional GP data.' Obtaining consent supports the Commission's ability to collect that data indirectly from the practice CIS (relevant to APP 3.6(1)(a)). If valid consent is given, it will also support the Commission's later use of that personal information for the purposes of the Program (discussed under APP 6).

22. To be valid, consent obtained as part of Activity 2 must be voluntary, informed, current and specific, and from an individual with capacity. We have reviewed the GP consent form against these elements and consider that the consent form, when read alongside the GP information form broadly meets the requirements. However, we think that amendments could be made to the consent form to ensure GPs are giving informed and current consent. In particular, the consent form should include information about how GPs can withdraw their consent if they wish to do so. This should be supported by a clear process to manage withdrawn consent.

23. With respect to the handling of GP data if consent is withdrawn, the Commission will need to consider its Commonwealth records management obligations in deciding whether to delete, de-identify or appropriately archive optional GP data. For example, it should confirm that this is permitted under the Commission's records disposal authority.[1] If deletion or destruction is not permitted, the Commission should consider measures to separate that information so that it is not readily available for access or use.

Recommendation 2 - Update GP consent form to ensure valid consent	
	To ensure GP consent is valid, the Commission should update the consent form to include information about how GPs can withdraw their consent in the consent form as well as in the separate information form.

[1] It is likely that the Commission's records relating to the Program will constitute Commonwealth records as defined by s 3 the *Archives Act 1983,* the disposal or destruction of which must comply with s 24 of that Act.

Response:	Agree

APP 3 - Collection of Patient information

24. The Program is premised around the collection of de-identified patient data. That is, practices use de-identification tools to remove identifying information before transferring the data to the Commission. APP 3 issues will not arise in respect of the patient data if the Commission only collects de-identified patient information.

25. However, risks that the Commission will collect patient personal information may arise in the following ways:

    25.1. The Program will solicit unstructured data (e.g. clinical data) which the GP will input into a free text field. While the de-identification tool is expected to remove identifying patient information prior to collection by the Commission, this will significantly increase the risk of inadvertent collection of identifying personal information, including irrelevant third-party personal information.

    25.2. Where clinical notes contain unique information, this could enable re-identification of patients when matched with other identifying data.

    25.3. The Program is reliant on third party data extraction tools to manage compliance with the APPs by effectively removing all identifiers from information extracted from the CIS.

    25.4. The Program has documented previous instances of inadvertent collection (and disclosure) of personal information[2] (see NPS PIA at p 46).

26. As set out at [44] below, where a patient can be identified from the data collected by the Commission, the APPs will apply to its handling and their data may become protected Commission information under the NHR Act, subject to the offence provisions in s 54A (discussed below from [37]).

27. In addition to the NPS recommendation 7 and 8, we suggest that, to the extent practicable, the Commission could consider options to further limit the collection of unstructured data to decrease the program's risk profile with respect to potential re-identification. In the event this suggestion is not practicable, for example, because the unstructured data has a specific utility for the Program, the Commission should ensure it has robust systems in place to otherwise manage and mitigate this risk.

28. We understand the Commission currently implements measures, including data cleansing, quality assurance, and its data governance release process, to further control its risk profile with respect to re-identification (see discussion from [64]).

Recommendation 3 – limit collection of unstructured data where practicable	
	To the extent practicable, the Commission should consider opportunities to limit the collection of free text fields (unstructured data) to decrease the program's risk profile with respect to re-identification.

2 See NPS PIA at p. 46

Response:	Agree in principle

Opt-out process

29. If patient data was to contain sensitive information (which it would if it were identifying) the collection would only be permissible if the Commission obtained consent or if an exception applies. While we generally agree with the findings of the NPS PIA that the Program does not need to obtain consent to collect de-identified patient data, we consider the program's 'opt-out' process (combined with other transparency measures discuss under APP 5) to be an important and necessary measure to manage the risks associated with de-identified patient data.

30. Due to the greater privacy risks associated with sensitive information, the APP Guidelines suggest that an APP entity should generally seek express consent from an individual before handling this information (at [B.44]). However, we acknowledge that an express consent process would be burdensome for the Program and potentially intrusive for patients, which may undermine the benefit of collecting data through the practices.

31. We think additional measures to strengthen the opt out process will assist the Commission to manage the risks associated with the Program's reliance on de-identification, by giving individuals choice regarding their participation and control over their personal information. In particular, the Commission relies on practices displaying the patient information poster (digitally or via hardcopy) and making the opt-out forms available to patients (see practice agreement at [6.2]). We think there is a risk that patients may not view or engage with program material displayed in this way, particularly where patients may only attend a Telehealth consultation.

Recommendation 4 – Consider opportunities to strengthen the opt-out process	
	To the extent practicable, the Commission could consider opportunities to strengthen the opt-out process, for example, by requesting participating practices to: • provide clear notice by a physical or electronic flyer to all new patients (i.e. with new patient form or booking confirmation) so they have an opportunity to opt out prior to their appointment • keep Program flyers on front desk • include information about the MI Program on their website or booking tool.
Response:	Agree

APP 5 – Notice of collection

32. Insofar as the Program collects personal information about GPs, we agree with the conclusions set out in the NPS PIA that the Healthcare professional information sheet generally addresses APP 5.2 matters. However, we suggest that the Commission update this form to indicate that GP personal information will not be sent overseas: APP 5.2(i), APP 5.2(j).

33. If the program is implemented as intended, the Commission is not required to issue privacy notices to patients in accordance with APP 5, because the Commission will not collect their personal information. That said, we endorse the Commission's approach of providing clear information to patients about the program so they understand how practices will use their personal information and can choose whether to participate.

34. We have assessed the updated consumer materials[3], available on the MI website. While the updated materials broadly address APP 5.2 matters, they do not disclose that GPs will hold linking information to enable them to 're-identify' their patients in the practice reports. As this means the Commission will facilitate a regular disclosure of personal information to participating practices, ideally this would be addressed in the consumer materials: APP 5.2(f)

Recommendation 5 – Update Program information to address APP 5.2 matters	
	To strengthen transparency and APP 5 compliance, the Commission should: • update the healthcare professional information to indicate that personal information will not be sent overseas: APP 5.2(i), APP 5.2(j) • update consumer information to indicate that in some cases, GPs may be able to re-identify patient information in de-identified reports prepared by the MI program: APP 5.2(f)
Response:	Agree

APP 6 - Use and disclosure of personal and protected Commission information

35. Under APP 6.1, the Commission can only use and disclose personal information for the purpose for which it was collected unless consent is obtained or an exception in APP 6.2 applies. Relevantly APP 6.2(b) authorises use and disclosure where it is authorised by or under law.

Commission must comply with NHR Act secrecy provisions, where relevant

36. In addition to considering the application of the Privacy Act to any personal information handled by the Program, the Commission must ensure it complies with the secrecy provisions in Part 2.7 of the NHR Act insofar as the Program involves the use and disclosure of 'protected Commission information.'

37. Where the secrecy provisions apply to the data the Commission handles in the Program, they will limit the Commission's handling of the data but also authorise its use and disclosure in certain circumstances. Where an authorisation applies, this may also have the effect of modifying the application of certain APPs.

The secrecy provisions restrict use / disclosure of protected information

---

3 As indicated in the MedicineInsight Program Changes document, the updated consumer material is intended to improve transparency and reflect the Commission's strengthened position on consumer engagement

38. The general secrecy provision in s 54A of the NHR Act applies to the use and disclosure of 'protected Commission information' by an official of the Commission, which relevantly includes:

38.1. a member of staff of the Commission

38.2. a person whose services are made available to the Commission under s 48 of the NHR Act, or

38.3. a person engaged as a consultant under s 49 of the NHR Act.[4]

39. Section 54A provides that a person commits an offence if the person is, or has been, an official of the Commission; has obtained protected Commission information in their capacity as an official of the Commission; and discloses the information to another person or uses the information, except in certain circumstances, including when an exception in the NHR Act applies.

40. Section 5 of the NHR Act defines 'protected Commission information' to mean information that a person obtained in the person's capacity as an official of the Commission, and relates to the affairs of a person other than an official of the Commission. In this context, a 'person' includes a body politic (e.g. a State), a body corporate or an individual: s 2C of the *Acts Interpretation Act 1901*.

Certain Program data is 'protected Commission information'

Program data is obtained by an official of the Commission

41. The Commission operates the Program in accordance with its functions as set out at [16].

42. Program data is extracted, transferred and stored in a data warehouse hosted by the Commission (Activity 5, Activity 6), where the data can be accessed by authorised people from the Commission and used for purposes set out in Activity 7. The Commission instruct that staff of the Commission (APS employees) only deliver the Program, while external contractors manage the data warehouse. We consider the definition of 'official' is broad enough to cover these arrangements. As such, Program data is provided to, and therefore obtained by, a Commission official in their capacity as an official of the Commission. With respect to the data warehouse, contractors would be operating and handling information as agents of the Commission and the collection would be by an 'official'.

Data about identifiable practices and individuals is protected Commission information

43. To deliver the Program, the Commission will collect data set out in Activity 5 from the Clinical Information System (**CIS**) of participating practices. This includes participating practice data (name, postcode etc) and GP information (site, name, provider number and prescriber number). Given this, in our view it is likely that the data will 'relate to the affairs' of the general practices and GPs and will be protected by s 54A of the NHR Act.[5]

---

4 'Official of the Commission' is defined in s 5 of the NHR Act

5 The expression 'affairs of a person' is not defined in the NHR Act. According to the *Macquarie Dictionary* (online), 'affairs' relevantly means 'matters of interest or concern'. Information that relates to the affairs of a person would include information about matters of interest or concern to an approved provider as a body corporate.

44. It follows that although the prohibition in s 54A of the NHR Act applies to practice data, its use and disclosure in Activities 5-7 will be authorised under s 54(b) of the NHR Act, in the performance of Commission's functions. In turn, the use and disclosure of GP personal information is permissible under APP 6.2(b) on the basis that it is authorised under law.

De-identified patient data may comprise protected Commission information in certain circumstances

45. Insofar as Program data that the Commission holds includes de-identified patient data and clinical information, the data is unlikely to constitute protected Commission information in relation to individuals (natural persons) provided that it is properly de-identified.[6] In this context we consider that 'affairs of a person' should be taken to include only information that identifies a person or enables the person to be identified, and not information that relates to the affairs of any person whether or not that person is capable of identification. We take this view as we understand the Commission does not hold the means to re-identify individuals in the data.

46. However, the patient data *may* comprise protected Commission information when the Commission discloses reports to participating practices in circumstances where those practices can re-identify their patients in the data. In these circumstances, the patient's name and associated information will be information related to the affairs of an individual, and the secrecy offence in s 54A of the NHR Act will apply.

47. The Commission will be authorised to use and disclose the data in this way, provided that this is necessary for the purposes of the Program, because of the operation of s 54B(b) of the NHR Act. That provision authorises the use of protected Commission information for the purposes of the performance of the functions of the Commission under the NHR Act. This will also constitute an authorisation for the purposes of APP 6.2(b). This authorisation would also apply to permit the use and disclosure of GP personal information to a limited extent, as necessary to implement the program.

Application of APP 6 to Program data

48. APP 6 requires the Commission to use and disclose personal information for the primary purpose of collection, which is our view is to deliver the Program in accordance with the use cases outlined at Activity 7. An agency must not use or disclose personal information for a secondary purpose, unless the individual consents or an exception applies.

49. Overall, depending on the specific circumstances of the use or disclosure, we do not think APP 6 issues arise in the Program either because:

    49.1. the Commission is using and disclosing de-identified data (e.g. where it produces reports for publication); or

    49.2. the Commission is disclosing personal information which is also protected Commission information, for the primary purpose of collection and, additionally, in circumstances where this is authorised by s 54B(b) of the NHR

---

6 As the practices install de-identification software in their own IT environments, and undertake de-identification of the patient data before they transfer it to the Commission, the Commission itself never collects or holds patient personal information.

Act (i.e. where it gives reports to practices in circumstances where they can identify their patients in the data).

APP 6 will not apply to de-identified data

50. Subject to the proper mitigation of re-identification risks discussed below in relation to APP 11, APP 6 will generally not apply to the extent that the Commission uses and discloses de-identified patient data as part of Activity 7.

51. Provided patient information held by the Commission is de-identified, the use and disclosure of this information will not be subject to the prohibition in s 54A as it will not fall within the definition of protected Commission information.

APP 6 will apply to disclosure of re-identifiable patient data

52. However, we understand that GPs will hold linking information to enable them to re-identify their own patients within practice reports to inform the standard of care they provide to their patients. While this data may not comprise personal information in the hands of the Commission, the Office of the Australian Information Commissioner (**OAIC**) has confirmed that the 'APP 6 will remain relevant in relation to the sharing or release of information, if the status of the information would change to being personal information in the hands of another entity.'[7]

53. Where information in the practice report disclosed to the GPs will allow the GP to re-identify the patient, we think the better approach and privacy practice is to treat this as a disclosure of personal information and protected Commission information by the Commission. As the disclosure is consistent with the primary purpose of collection, that is, to prepare and distribute customised practice reports, we consider the disclosure is authorised by law for the purposes of s 54B(b) of the NHR Act. Accordingly, the disclosure will be authorised under the exception in APP 6.2(b).

54. In Activity 5, the tool will 'use' personal information to prepare a de-identified dataset. While this activity is a 'use' by the participating practices, not the Commission, they will do this for the Commission's purposes. For completeness, we note that de-identification is generally permissible under APP 6.1 because, as part of an APP entity's normal business practices, it is considered to be undertaken for the primary purpose of collection.[8]

Use and disclosure of GP data authorised under APP 6

55. We understand that the Commission will use limited GP information collected in Activity 5 for the purpose of preparing and distributing customised practice reports. This use is consistent with the primary purpose of collection. Further the use of Protected Commission information is consistent with s 54B(b) of the NHR Act, as discussed above.

56. Finally, where GP's consent to the collection of their optional data in Activity 2 for the purpose of preparing individualised GP reports, we understand that their name (and individual prescribing clinical data) will be used and disclosed consistently with the primary purpose of collection and will not be disclosed outside of the individual GP.

---

7 See De-identification and the Privacy Act | OAIC

8 APP Guidelines at para [B.106].

APP 10 – data quality

57. APP 10 relates to the quality of personal information that APP entities collect, use and disclose. GPs will enter patient data into the CIS. As such, the Program will be subject to the same data quality risks that exist within each practice's CIS.

58. Personal information quality issues will not arise to the extent that information collected, used and disclosed is de-identified. However, APP 10 obligations will attach to patient data which GPs can re-identify through linking (see Activity 7) and identifiable GP data. Inaccurate data has the potential for real-world consequences, for example, if a GP's details are entered incorrectly, or if there are errors in linking the report to a GP, this could result in a misattribution of patient data.

59. To address this, the practice agreement includes an obligation to ensure practice data[9] (which includes patient data, and GP data collected in Activity 1) aligns with applicable data quality standards (i.e. those imposed by the Royal Australian College of General Practice (**RACGP**) Standards for General Practice) to ensure accurate and up-to-date records (see 6.2(g)).

60. We observe that the obligation in the practice agreement does not extend to the optional GP data (including email and residential address) collected in Activity 2 and used as part of Activity 7. As such, we think the Commission should take reasonable steps, to ensure that this information is accurate and up-to-date. For example, by including a requirement in the GP consent form or practice agreement to update GP contact details with the Commission as required.

Recommendation 6 - Take steps to ensure GP data is accurate and up to date	
	To the extent practicable, the Commission should take reasonable steps to ensure GP information collected as part of Activity 2 and used as part of Activity 7 is accurate and up-to-date.
Response:	Agree

APP 11 – security of personal information

61. APP 11 requires APP entities to take reasonable steps to keep their personal information holdings secure. In accordance with recent changes to the APPs, it is clear that reasonable steps include both technical and organisational measures: APP 11.3.[10]

62. The 'reasonable steps' an APP entity is required to take to ensure the security of personal information will depend on the circumstances, including the following:

    62.1. the nature of the entity

    62.2. the amount and sensitivity of the personal information held

    62.3. the possible adverse consequences for individuals in the case of a breach

---

9 *Practice Data* means the data extracted from the Participant's CIS

10 APP 11.3 was introduced to Sch 1 of the Privacy Act by s 34 of the Privacy Amendment Act.

62.4. the practical implications of implementing the security measure, including the time and cost involved

62.5. whether any relevant security measure is itself privacy invasive.

63. While de-identified patient data will not generally attract APP 11 obligations, we think GPs and the community generally would expect the Commission to implement robust protections for of this type of information, given the sensitivity of the underlying data. This is particularly the case given the potential for inadvertent collection of personal and sensitive information, as well as re-identification risks in the event of a data breach.

64. The Office of the Australian Information Commissioner's (**OAIC**) *Guide to securing personal information, June 2018* (**Security Guide**) outlines 9 broad topics that ought to be considered when assessing how to best secure personal information held by an APP entity. While certain topics are examined in more detail below, we have included some high level suggestions against topics for which we do not have specific instructions in the table below:

Topic	Recommendation
Governance, culture and training	• Ensure Commission staff involved in the Program receive appropriate training in relation to the handling of personal and protected Commission information
Practices, procedures and systems	• Review policies to ensure they incorporate the acts or practices which occur as part of the Program.
Access security	• Limit access privileges and access to Program data and review those privileges on a regular basis. • Audit access to program data and conduct regular review of audit logs • Incorporate the Five Safes framework into data access arrangements.
ICT security	• Ensure Program data is stored separately to the Commission's other data holdings and do not use data for an unrelated/unauthorised purpose • Ensure Program data shared with participating practices and/or external entities is shared via a confidential and secure platform (i.e. PowerBI instead of email)
Physical security	Not relevant.
Standards	• Store Program data in systems that comply with ISM

De-identification and data breach

65. The NPS PIA identified de-identification as a substantial risk for the Program. In particular, it referred to the risk that the Program may inadvertently collect and in turn disclose identifiable patient data to external entities via third party access requests. For example, the report highlighted an incident whereby personal information (including six patient names) was discovered in a data extract provided to a research team.[11]

[11] See NPS PIA, p 46.

66. The transition to the Commission introduces a further secrecy risk in this context. As indicated at [44], if the Commission inadvertently collects identifiable patient information, this may comprise protected Commission information under the NHR Act. In turn, the inadvertent disclosure of this information via a third party data request may amount to a disclosure of protected Commission information to which the offence provision in s 54A of the NHR Act applies.

67. We are instructed that certain strategies were put in place following the data breach incident to more tightly control free text fields, including measures to cleanse data by sweeping free text fields for identifiable information. The NPS PIA assessed the Program against the Five Safes framework[12] (or Data Sharing Principles) and found that the Program has implemented controls in accordance with each Data Sharing Principle.

68. Additionally, we understand that external access requests are subject to internal review and approval process as described in the Commission's Data Governance Framework (**Framework**).

69. Given the additional secrecy risk, we consider that implementation of NPS Recommendation 8, 9 and 10 are key to managing compliance with APP 11.

70. Further, to manage future suspected or actual data breaches, the Commission should ensure it has a data breach response plan in place as well as a shared approach to managing data breaches or other cyber security incidents with participating practices, CSPs, or external entities.

Recommendation 7 – Develop a shared approach to data breach response	
	The Commission should ensure it has a data breach response plan in place as well as a shared approach to managing data breaches or other cyber security incidents with participating practices, CSPs, or external entities.
	Agree

Data Availability and Transparency Act 2022

71. As instructed, we have considered the application of the DAT Act to the Project. In particular, we have considered the relevance of the DAT Act to the sharing of Program data with external entities[13] in Activity 7.

72. The DAT Act establishes an alternative pathway (and limited statutory authorisation) for the sharing of 'public sector data,'[14] but does not replace or effect existing pathways or mechanisms for data sharing. While the Commission is the data custodian for public sector data (Program data), the DAT Act does not require data sharing to occur consistently with the framework where this is otherwise authorised. As such, we think the DAT Act has no relevance to the Program.

---

12 See NPS PIA, section 4.

13 See definition of 'entity', DAT Act s 9.

14 'Public sector data' means data lawfully collected, created or held by or on behalf of a Commonwealth body, DAT Act s 9.

Contracted service providers

73. The Project uses contracted services providers (**CSPs**) with respect to the Synergise data warehouse and extraction tools.

74. The Commission must take contractual measures to ensure that its contractors and any subcontractor,[15] do not do an act, or engage in a practice, that would breach an APP if done or engaged in by the Commission.[16] Annexure C sets out the recommended contractual clauses to satisfy s 95B.

75. The Commission instruct that clause 12 (Obligations of Service Provider in Relation to privacy) of the standard contract for services template (prepared by AGS) outlines the requirements for complying with the Privacy Act, the relevant privacy requirements of New South Wales (as the governing law of MI contracts) and the APPs. As such, we have not undertaken review of the contracts for compliance with s 95B of the Privacy Act as part of this advice. However, as we have concluded that certain Program data will comprise protected Commission information, we note that where Contractors will handle information protected by secrecy provisions, they must also comply with statutory information handling requirements.

76. As an additional step, we suggest that the Commission take steps to audit compliance with contractual privacy obligations on a regular basis.

Recommendation 8 – Implement additional measures with respect to CSPs	
	As an additional measure to protect personal information handled by CSP on behalf of the Commission, the Commission should audit compliance with contractual privacy obligations on a regular basis.
Response:	Agree

Context

Background

77. The Program is a national primary health care data program run by the Commission in partnership with participating general practices across Australia. At a high level, the Program collects de-identified patient information from the medical records of participating general practices as well as personal information about their GP s. This information is combined with data from other general practices across Australia to form a database which enables the Commission to compare and discover trends in diagnoses, treatments, and outcomes of general practice patients at a national level.

78. The Commission is the custodian of the MI program and data collection established by the now defunct ‘NPS MedicineWise’. A PIA commissioned by NPS MedicineWise

15 An organisation that is or was a party to the government contract and that is or was responsible for the provision of services to an agency or a State or Territory authority under the government contract; or a subcontractor for the government contract. A 'government contract' includes a Commonwealth contract, s 6(1) Privacy Act.

16 Privacy Act, s 95B.

in 2021 (**NPS PIA**) assessed the Project against the *Privacy Act 1988* (**Privacy Act**) and the Australian Privacy Principles (**APPs**) contained in Sch 1 of the Privacy Act and made 10 recommendations to improve privacy compliance.[17] The Commission seeks a 'gap analysis' of the project, including through the lens of any legislative and regulatory changes that have taken place in the past four years.

Scope and preparation of the advice

79. To prepare this advice, we analysed the program against the Privacy Act and the APPs. We undertook this assessment in light of relevant Commission functions under the NHR Act, and in the context of the secrecy provisions in Part 2.7 of that Act.

80. In this advice we:

    80.1. check for any potential non-compliance with the APPs

    80.2. identify any other matters that might give rise to privacy risk

    80.3. recommend remedial actions.

Material considered

81. We considered the following material in preparing this advice:

    81.1. NPS MedicineWise PIA, undertaken by Information Integrity Solutions on 29 January 2021

    81.2. MedicineInsight Program Changes Document

    81.3. MedicineInsight Data Access Deed - finalised 25 July 2024

    81.4. ACSQHC Data Access Application Form 2024

    81.5. MedicineInsight Agreement - Commission and General Practice ~ Existing Practices (Ghranite Sites)

    81.6. MedicineInsight Data Access Deed - finalised 25 July 2024

    81.7. medicineinsight_gp_consent_form_v2.1

    81.8. medicineinsight_gp_information_form_v2.1

    81.9. medicineinsight_patient_information_form_v2.1

    81.10. medicineinsight_patient_opt-out_form_v2.1

    81.11. medicineinsight_practice_poster_for_print_v2.1

Assumptions and exclusions

82. This advice examines the potential privacy impacts in relation to APPs 1, 3, 5-6 and 10-11.

83. In preparing this advice, we have not examined the following APPs which are unlikely to raise significant privacy issues in the context of the Project.

---

17 See Annexure C.

APP	Description
APP 2 – Anonymity and Pseudonymity	To the extent the Project handles information about patients, APP 2 will not apply as the Project will not deal directly with identified individuals. To the extent the Project does deal with identified individuals (i.e. GP s), APP 2 will not apply as it would be impracticable for the Commission to deal with unidentified individuals.
APP 3 – Collection of personal information	The Project will not involve any collection of personal information by the Department.
APP 4 – Unsolicited personal information	APP 4.1 applies to the handling of unsolicited personal information. As the Commission will not receive any unsolicited personal information as part of the Project, APP 4 issues will not arise.
APP 7 – Direct marketing	APP 7 does not apply to the Commission in relation to the Project
APP 8 – Overseas disclosure	APP 8 does not apply as the Project will not involve any overseas disclosure of personal information.
APP 9 – Adoption, use or disclosure of government related identifiers	APP 9 does not apply to the Commission in relation to the Project.
APP 12 – Access to personal information	An individual can request access to their personal information held by the Commission in accordance with the Commission's ordinary processes as set out in its privacy policy.
APP 13 – Correction of personal information	An individual can request the correction of their personal information held by the Commission in accordance with the Commission's ordinary process, as set out in its privacy policy.

ANNEXURE A – INFORMATION FLOWS

Annexure A summarises the key information handling activities of the Program. Cells shaded in **green** represent collection, **red** represents use, **purple** represent collection and use, and **orange** represent use and disclosure.

Activity	Description
1	**The Commission obtains general practice consent to participate in Program**
	Participation in the Program is voluntary and free of charge. The Commission obtains the consent[18] of general practice owners to use and share data extracts from the practice's medical records with the Commission, for the purposes described in **Activity 7**. If a general practice agrees to participate, they sign an agreement (**practice agreement**) authorising the use and disclosure of their practice data for these purposes. The Commission will collect limited personal information (name, provider number, prescriber number) about GPs contained in the practice's medical records (**Activity 5**) for the purpose of preparing customised practice reports (see Activity 7). Upon joining, practices are required to notify all health professionals (including those who commence after the practice has joined the program) of their participation in the program and subsequent collection of GP information as an employee of the practice.[19] Additionally, the Commission uses Survey Monkey to seek expressions of interest to participate in the Program.
2	**The Commission obtains GP consent to collect optional data for individualised practice reports**
	The practice agreement provides an opportunity for GPs to separately consent to the Commission collecting their personal information so the Commission can send them individualised practice reports. With GP consent, the Commission will collect and store additional personal information about the GP (optional GP data), including their gender, year of birth or age group, email, address and number of years practicing.[20]
3	**Participating practices display Program and 'opt out' information for patients**
	Under the practice agreement, participating practices are required to notify patients that the practice participates in the Program and provide information about how patients can 'opt out' at any time. The Commission supplies each participating practice with a kit containing the information sheets, opt-out forms, and instructions on how to help a patient opt out of the program. If a patient 'opts out', the Commission will no longer collect the patient's information and (to the extent practicable) the Commission will take steps to remove information that it has already collected. Participating practices retain the opt-out forms and do not provide them to the Commission.

18 Or reconsent, following the transition.

19 See MedicineInsight - Information for Doctors

20 See medicineinsight_gp_consent_form_v2.1.pdf

Activity	Description
4	**The Commission installs a compatible data extraction tool on the clinical information system of participating practices**
	The Commission installs a compatible data extraction tool (**tool**) on the CIS of participating practices. Currently, there are two tools available which operate in the same way: GRHANITE (owned by the University of Melbourne) and INCA (owned by Precedence HealthCare).
5	**The tool extracts and 'de-identifies' data from participating practices' medical records**
	The tool extracts data from the medical records of participating practices (**Program data**). This includes unstructured data (i.e. free text clinical data). At the same time, it removes direct identifiers such as the patient's name, date of birth and address and replaces them with a unique reference number which allows the Commission to obtain data about a patient over time (i.e. longitudinal data). Program data includes[21]: • practice data (e.g. name of practice, postcode, software and extraction date) • GP information (e.g. site, name, provider number and prescriber number) • patient demographics (e.g. unique encrypted identification number, birth year, gender, remoteness indicator, Indigenous status, SEIFA indicators) • clinical data entered directly by healthcare professionals and practice staff about a patient (e.g. encounter, medical history, prescriptions, medical tests performed, observations, risk factors, management activities, allergies/ADRs, MBS service and vaccinations) • system-generated data (e.g. start time and date of patient encounter).
6	**The tool encrypts, transmits and stores Program data in the Synergise data warehouse**
	The tool extracts, transfers and stores Program data in an Australian cloud-based data warehouse (Synergise) managed by the Commission.[22] The data warehouse contains holdings of: • non-identifiable unit-level patient data • identifiable GP data (including name, provider number and prescriber number (contained in medical records) 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. The Commission instructs that it does not have access to the legacy dataset that was previously collected and managed by NPSMedicineWise. As such, this dataset is outside the scope of this advice.
7	**The Commission uses Program data for several key purposes**
	The Commission uses and discloses Program data for several key purpose[23] in relation to its functions, including:

21 See MedicineInsight - Information for Doctors, p. 1.

22 See MedicineInsight - Information for Doctors, p. 2.

23 See MedicineInsight - Information for Doctors, p. 2-3.

Activity	Description
7.1	**Clinical improvement purpose:** • To provide customised practice reports to participating practices. These comprise regular aggregated clinical reports on quality use of medicines topics that are customised to the activities of a participating practice. These reports are based on the practice's own data and offer insights into patterns of prescribing and patient care, comparing these with benchmarks at local, regional and national levels. They also provide an opportunity for improved data quality, facilitate data interpretation and the development of local plans to support clinical interventions. Reports are made available to the participating practice online via a confidential and secure platform. • To prepare individualised reports to consenting GPs in which their patients are allocated to the quality use of medicines topic contained in the report. This supports the reduction of preventable harm, as well as clinical patient interventions with a view to improving health outcomes for patients. This report uses the GP's name to enable reporting on the correct patients. The unique reference number assigned to the patient record at the time of de-identification, allows the GP to re-identify their own patients within data, within the confines of the practice, to inform the standard of care they provide to their patients: s 9(1)(a)-(b)
7.2.	**Reporting purpose:** • The Commission uses Program data to produce routine aggregated reports for key stakeholders (such as state and territory health departments and health services organisations) on national quality improvement activities to inform primary care policies, programs, and initiatives. These reports help to improve policies about the way people across Australia can access and use medicines, medical tests and vaccines. They also support evidence for listings in the Pharmaceutical Benefits Scheme: s 9(1)(d)
7.3	**Data analysis purpose** • The Commission may disclose Program data to requesting third parties (e.g. government departments, government-funded organisations, not-for-profit organisations and research institutes) for purposes related to informing primary care policy, public health initiatives, research and service delivery. All requests to access data are subject to review and approval processes as described in the Commission's Data Governance Framework which involve robust privacy, confidentially and security assessments and a determination of benefit to public good and primary care. A public register of projects that have been approved to use Program data can be found on the Commission's website: s 9(1)(b), s 9(1)(m)
7.4	**Quality assurance purpose** • The Commission may use Program data to undertake audit, training, evaluation or quality improvement activities to validate the accuracy and reliability of data collected: s 9(1)(q)

ANNEXURE B – NPS MEDICINEINSIGHT PIA RECOMMENDATIONS

The below recommendations are extracted from the NPS MedicineInsight PIA, undertaken by IIS on 29 January 2021.

#	IIS Recommendation	Type
1	Ensure NPS MedicineWise correctly portrays the status of MedicineInsight de-identified patient data under the Privacy Act	Best practice
2	Strengthen privacy governance measures, including in relation to privacy training, risk management and strategic oversight	Strengthen compliance
3	Update privacy policy to specifically address MedicineInsight	Best practice
4	Strengthen security with some additional measures, including access control, data retention and risks related to GPs	Strengthen compliance
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
6	Include data user training as a requirement of MedicineInsight data access	Best practice
7	Update the documented de-identification procedures	Best practice
8	Build in de-identification review into regular assurance cycle	Best practice
9	Clarify and formalise procedure for responding to (re)identification incidents, in the context of incident management reporting processes	Strengthen compliance
10	Explore software-based solutions for managing de-identification risk	Best practice

ANNEXURE C – CONTRACTUAL PRIVACY MEASURES

Annexure C sets out the recommended contractual clauses to satisfy s 95B of the Privacy Act.

Topic	Recommended contractual requirement
Overarching requirements (s 95B)	SP will comply with / not breach the APPs
	Subcontractors must meet the same requirements as SP
	Agency has rights to conduct audits relevant to the performance of the SP's obligations under the contract
Notice of collection (APP 5)	SP will facilitate issue of collection notices
Use and disclosure (APP 6)	SP will only access, use and disclose personal information for the purpose of delivering services under the contract
Overseas disclosure (APP 8)	SP must not disclose personal information overseas unless contractual measures achieve APP 8 compliance
	SP must obtain agency approval prior to transmission outside of Australia
	SP must notify agency of requests from foreign governments or agencies for access to agency data.
Security – general (APP 11)	SP must take reasonable steps to protect personal information.
Personnel security (APP 11)	Personnel must execute a confidentiality agreement before obtaining access to personal information
	Personnel must hold appropriate security clearance
	Personnel must complete privacy and security training
	Contractors who will handle information protected by secrecy provisions must comply with statutory information handling requirements.
ICT and access security (APP 11)	SP must comply with the PSPF and ISM
	Contract specifies requirements regarding: • access to data • data security • data destruction • safeguards to comply with APP 11
Physical security (APP 11)	SP and personnel may be subject to other requirements regarding:

Topic	Recommended contractual requirement
	• obtaining agency prior approval for removal of data from premises • storage of data
Data breaches (APP 11)	SP must have a data breach response plan
	Contract specifies data breach arrangements, eg: • SP must notify agency within a prescribed period (e.g. 2 days) if it has reasonable grounds to suspect an event amounts to an eligible data breach • Parties must nominate contact persons / methods • Consequences of a breach are (e.g. whether breaches of obligations to comply with the Privacy Act and APPs constitute a material breach).