EXPLANATORY STATEMENT

National Health Act 1953

National Health (Data-matching) Principles 2020

This Explanatory Statement relates to the legislative instrument titled the *National Health (Data-matching) Principles 2020* (the Principles).

The *National Health Act 1953* (the National Health Act) establishes the Pharmaceutical Benefits Scheme (PBS) and provides Australians with timely, reliable and affordable access to necessary and cost-effective medicines. Part VIIIA of the National Health Act enables the Chief Executive Medicare to match certain information for permitted purposes, which are Medicare compliance and related administrative purposes.

Part VIIIA of the National Health Act improves the capability of Chief Executive Medicare to detect instances of fraud, inappropriate practice and incorrect claiming in relation to medicare programs such as the Medicare Benefits Schedule (MBS) and the PBS.

Subsection 132F(1) of the National Health Act requires the Minister for Health to make, by legislative instrument, principles in relation to the matching of information under subsection 132B(1). Subsection 132B(4) states that information must not be matched under subsection 132B(1) until the principles made under subsection 132F(1) have commenced.

Part VIIIA of the National Health Act, as passed by Parliament, specifically requires delegated legislation in the form of the Principles. Relevantly, the operational provisions that both enable and restrict data matching are in primary legislation. This includes detailed minimum requirements for the content of the Principles in subsection 132F(2). However, requiring further detail in a legislative instrument provides flexibility, by enabling, for example, the inclusion of technical concepts and detail that would not be suitable for primary legislation, and the ability to reflect changes in best practice in the evolving technological and privacy environment. It also allows for consideration of the guidelines on data-matching in Australian Government administration made by the Australian Information Commissioner under paragraph 28(1)(a) of the *Privacy Act 1988* (Privacy Act).

The Principles will support the National Health Act and provide further safeguards as to the use of information for data matching for Medicare compliance purposes, by setting out certain responsibilities that must be met by the Chief Executive Medicare as part of the matching of information. The Principles also incorporate applicable underlying privacy obligations. The Chief Executive Medicare may authorise a Commonwealth entity to match information on the Chief Executive Medicare's behalf for the same permitted purposes, and the Principles also apply to these authorised Commonwealth entities.

As some of the information to be matched may include personal and/or sensitive information, the Principles will lay the foundation for the governance of matching activities by establishing high standards for privacy safeguards and the protection of information. Although the Privacy Act still applies, the Principles impose additional specifications as to the handling and use of personal information as part of data matching. As the National Health Act requires a principles-based legislative instrument, the Principles do not include

Authorised Version Explanatory Statement registered 04/01/2021 to F2021L00006

process steps and can accommodate changes to technology or privacy. This enables flexibility in their practical application over time.

In summary, the Principles set out:

- good privacy practice to be observed in the matching of information including the publication of information about authorised information-matching, technical standards and an evaluation of privacy practices;
- a requirement that the Chief Executive Medicare establish and maintain a publicly available register of the kinds of information matched, and a description of the information that must be included on this register;
- a requirement that the Chief Executive Medicare, and authorised Commonwealth entities, keep records of information matched, and a description of those records;
- a requirement that the Chief Executive Medicare, and authorised Commonwealth entities, take reasonable steps to destroy personal information which has been matched, the results of matching, or information not to be matched, within 90 days of the information no longer being needed for the purpose for which it was matched;
- a requirement that the Chief Executive Medicare, and authorised Commonwealth entities, take reasonable steps to ensure that personal information that is matched is accurate, complete and up to date; and
- a requirement that the Chief Executive Medicare, and authorised Commonwealth entities, do not match information unless satisfied that the matching is reasonably necessary for the relevant permitted purpose, with decisions to be made about how to minimise the necessary data fields, data subjects and personal information.

Consultation

The Department has consulted on the development of the Principles in accordance with section 17 of the *Legislation Act 2003*. A targeted consultation was chosen as the Principles only apply to the Chief Executive Medicare and any authorised Commonwealth entities, and do not impose obligations on individuals, health organisations or health providers. Selected health professional groups and peak bodies with an interest in the Principles were provided with an exposure draft of the Principles and given the opportunity to provide feedback both in writing and via discussions. Relevant Commonwealth agencies were also consulted throughout the development of the Principles. All comments and suggestions from stakeholders were carefully considered and this content ultimately contributed substantially towards the finalisation of the Principles. It is also relevant to note that the enabling legislation was subject to a public consultation process and pertinent themes from this process were considered in the preparation of the Principles.

Details of the Principles are set out in the Attachment.

In making the Principles, the Minister has met the statutory obligation to take into account the guidelines on data-matching in Australian Government administration made by the Australian Information Commissioner under paragraph 28(1)(a) of the Privacy Act.

The Principles are a legislative instrument for the purposes of the *Legislation Act 2003*.

The Principles commence on the day after registration.

Authority: Section 132F of the *National Health Act 1953*

Authorised Version Explanatory Statement registered 04/01/2021 to F2021L00006

ATTACHMENT

Details of the *National Health (Data-matching) Principles 2020*

Part 1 – Preliminary

Section 1 – Name

Section 1 provides that the name of the instrument is the *National Health (Data-matching) Principles 2020* (the Principles).

Section 2 – Commencement

Section 2 provides that the Principles commence the day after the Principles are registered.

Section 3 – Authority

Section 3 provides that the Principles are made under the *National Health Act 1953* (the Act).

Section 4 – Definitions

Section 4 provides definitions of expressions or terms used in the Principles, which are as follows:

'***Act*** means the *National Health Act 1953.*

authorised Commonwealth entity has the same meaning as in Part VIIIA of the Act.

authorised data-matching program means a program of authorised information matching for one or more permitted purposes.

authorised information-matching means the matching of information that is authorised by Part VIIIA of the Act.

Commonwealth entity has the same meaning as in Part VIIIA of the Act.

identifier has the same meaning as in the *Privacy Act 1988.*

permitted purpose has the same meaning as in Part VIIIA of the Act.

personal information has the same meaning as in Part VIIIA of the Act.'

Part 2 – Good privacy practice

Section 5 – Publishing information about authorised information-matching

Section 5 provides that the Chief Executive Medicare must publish, on the internet, certain information about authorised information-matching. This information includes an overview of authorised information-matching, the objectives of authorised information-matching, and certain descriptions of topics related to authorised information-matching.

By requiring this information to be published, section 5 is intended to provide transparency around all authorised information-matching occurring under the Act. As the Act already sets

Authorised Version Explanatory Statement registered 04/01/2021 to F2021L00006

out clear limits and parameters in relation to the matching of information, it is not necessary to restate this information for each authorised data-matching program.

Section 6 – Technical standards for authorised data-matching programs

Subsection 6(1) provides that the Chief Executive Medicare must prepare and maintain, in writing, technical standards to govern the conduct of each authorised data-matching program.

Subsection 6(2) further provides that the technical standards must include the following:

a) a description of data supplied by sources of information for the program;
b) the specification for each matching algorithm for the program;
c) any risks that have been identified in relation to the program and how those risks will be addressed;
d) controls to be used to ensure the continued integrity of:
   (i) the information used for the program; and
   (ii) the system for the program;
e) security features that control and minimise access to personal information.

Subsections 6(3) and 6(4) provide that the Chief Executive Medicare and any authorised Commonwealth entity must each comply with the technical standards for an authorised data-matching program when matching information under subsection 132B(1) of the Act for that program. This provision is intended to ensure that the technical standards applying to all authorised data-matching programs are considered, documented and complied with, to promote clarity and consistency when matching information under subsection 132B(1) of the Act.

Section 7 – Evaluation of privacy practices for authorised information-matching

Section 7 provides that the Chief Executive Medicare must, within 3 years after the commencement of authorised information-matching, evaluate the privacy practices relating to authorised information-matching, prepare a report of the evaluation and give a copy of the report to the Australian Information Commissioner. This provision is intended to ensure that authorised information-matching is subject to a privacy self-evaluation, and that the Australian Information Commissioner has visibility over this evaluation. The Chief Executive Medicare may choose to undertake further evaluations in an ongoing capacity as required. The Chief Executive Medicare will consider the subject and any findings of the initial evaluation when determining the content and frequency of any future evaluations.

Part 3 – Publicly available register

Section 8 – Publicly available register of kinds of information matched

Section 8 provides that the Chief Executive Medicare must establish and maintain a publicly available register of the kinds of information matched by the Chief Executive Medicare or an authorised Commonwealth entity under subsection 132B(1) of the Act.

The publicly available register is intended to provide public awareness and transparency in relation to the kinds of information matched in authorised information-matching. However, as authorised information-matching must be for permitted purposes which relate to Medicare

Authorised Version Explanatory Statement registered 04/01/2021 to F2021L00006

compliance, the extent of this published information should not prejudice related compliance activities.

Section 9 – Information that must be included on the publicly available register

Section 9 provides that the Chief Executive Medicare must include the following information in the publicly available register required by section 8, for each kind of information matched by the Chief Executive Medicare or an authorised Commonwealth entity:

a) a description of the kind of information and the datasets from which the information was taken;
b) each permitted purpose for which the information was matched;
c) if any of the information that was matched was obtained by the Chief Executive Medicare from, or disclosed or provided to the Chief Executive Medicare by, another person or entity:
   (i) a description of that information; and
   (ii) if the other person or entity is not an individual—the name of the other person or entity;
d) if the information was matched by an authorised Commonwealth entity, and the matching is an act or practice to which the *Privacy Act 1988* applies—the name of the entity;
e) if the information was matched by a person as delegate of the Chief Executive Medicare, and the person is not an individual—the name of the person.

These minimum requirements of content for the public register provide an opportunity for public awareness and transparency. This content will enable members of the public to be aware of the kinds of information matched, the related permitted purpose(s) for which these kinds of information were matched and the source(s) of these kinds of information. This content also provides awareness in the case of any authorised Commonwealth entities matching on the Chief Executive Medicare's behalf, or the name of a person (other than an individual) matching the information as a delegate of the Chief Executive Medicare. It is not intended that the information on the publicly available register contain descriptive parameters that might risk jeopardising or prejudicing compliance activities.

In relation to paragraph (e) of section 9 of the Principles, it is relevant that subsection 6(9) of the Act enables delegation of the Chief Executive Medicare's powers under the Act, including the power to data match under subsection 132B(1), to a person. This delegation power to a person is in accordance with the other delegation powers in the Act. In practice, any delegation of the Chief Executive Medicare's legislative powers to data match will be restricted by certain safeguards: firstly, by the technical and specialist skills required for data matching; secondly, by secrecy provisions (including section 130 of the *Health Insurance Act 1973* and section 135A of the Act) which prevent persons who are not working within the Medicare compliance framework from accessing medicare program information for matching; and finally, by subsection 6(11) of the Act which provides delegates are subject to any directions of the Chief Executive Medicare in the exercise of their delegated powers. However, as references to a person in legislation include a body politic or corporate as well as an individual (section 2C of the *Acts Interpretation Act 1901*), paragraph (e) of section 9 of the Principles requires transparency in the event any power is delegated to a body corporate. It is not normal practice for the Chief Executive Medicare's powers to be delegated to a body corporate. However, paragraph (e) of section 9 was included due to

Authorised Version Explanatory Statement registered 04/01/2021 to F2021L00006

specific requests made by stakeholders, during the consultation process, for transparency in the event of a delegation to a body corporate.

Section 10 – Information that may be included on the publicly available register

Section 10 provides that the Chief Executive Medicare may include in the publicly available register other information about the matching of information under subsection 132B(1) of the Act. This enables the Chief Executive Medicare to include additional information on the public register on a case-by-case basis as appropriate. The type and extent of any additional information included on the public register will be carefully considered by the Chief Executive Medicare, to balance transparency with the protection of compliance activities.

Part 4 – Record-keeping

Section 11 – General

Subsection 11(1) provides that the Chief Executive Medicare must keep records of information matched by the Chief Executive Medicare under subsection 132B(1) of the Act.

Subsection 11(2) provides that an authorised Commonwealth entity must keep records of information matched by that authorised Commonwealth entity under subsection 132B(1) of the Act.

Section 12 – Records for authorised data-matching programs

Subsection 12(1) provides that the Chief Executive Medicare must keep records of the following for each authorised data-matching program:

a) each permitted purpose for the program;
b) the matters considered under Part 7 of the Principles in relation to the program;
c) a description of the information that was matched for the program;
d) the timing or frequency of the matching of information for the program;
e) if the information that was matched for the program was obtained by the Chief Executive Medicare from, or disclosed or provided to the Chief Executive Medicare by, another person or entity for the purpose of facilitating the matching—the date the information was so obtained, disclosed or provided.

Subsection 12(2) provides that the records of the authorised data-matching program must be sufficient to enable the replication of the matching of the information for the program while the datasets remain available. In this context, it is expected that the records (for the purposes of record-keeping) would contain the details of how to replicate an authorised data match by recording and setting out the steps or processes which applied to the information or data in question as part of the matching process. This is intended to ensure consistency and clarity in authorised data-matching programs.

The term ‘sufficient’ is not defined and is intended to have its ordinary meaning. In this context, when determining ‘sufficient’ records, the Chief Executive Medicare will consider the appropriate level of detail required to perform replication of datasets having regard to the complexities and requirements of each authorised data-matching program.

Authorised Version Explanatory Statement registered 04/01/2021 to F2021L00006

Subsection 12(3) provides that subsection 12(2) does not require the records to include the datasets. This provision is intended to clarify that the information or data itself is not expected to be considered a record that is required to be kept.

Section 13 – Records of destruction of information and results

Section 13 provides that the Chief Executive Medicare and an authorised Commonwealth entity (as applicable) must each keep records of the description of personal information and results of matching which are destroyed under Part 5 of the Principles. This provision is intended to promote consideration and monitoring of information that is destroyed.

Section 14 – Sufficiency of records for assessment purposes

Section 14 provides that the records mentioned in sections 11, 12 and 13 must be sufficient to enable the Australian Information Commissioner to conduct an assessment under paragraph 33C(1)(f) of the *Privacy Act 1988*, in relation to the matching of information and the handling of information related to that matching. This provision provides guidance on the standard for record-keeping and is designed to be facilitative of the Australian Information Commissioner's assessment role.

The term 'sufficient' is not defined and is intended to have its ordinary meaning. In this context, when determining whether records are 'sufficient', the Chief Executive Medicare will consider the appropriate content and level of detail required to effectively enable assessment by the Australian Information Commissioner.

Part 5 – Destruction of personal information and results of matching

Section 15 – Destruction of personal information when no longer needed after matching

Subsection 15(1) provides that if personal information that has been matched by the Chief Executive Medicare under subsection 132B(1) of the Act is no longer needed for any purpose for which it was matched, the Chief Executive Medicare must, within 90 days after the information ceases to be needed, take reasonable steps to destroy the information.

Subsection 15(2) provides that if personal information that has been matched by an authorised Commonwealth entity under subsection 132B(1) of the Act is no longer needed for any purpose for which it was matched, the authorised Commonwealth entity must, within 90 days after the information ceases to be needed, take reasonable steps to destroy the information.

Subsection 15(3) provides that the obligations in subsections 15(1) and 15(2) apply to personal information held for the purpose of matching that information (copies), and do not apply to that personal information held for another purpose or by another person. It is intended that only the copies of personal information for matching be destroyed.

This provision is intended to prevent personal information for data matching being kept unnecessarily, whilst not requiring premature destruction of information that is still needed.

Authorised Version Explanatory Statement registered 04/01/2021 to F2021L00006

Section 16 – Destruction of results of matching when no longer needed

Subsection 16(1) provides that if the results of the matching of information by the Chief Executive Medicare under subsection 132B(1) of the Act are no longer needed for any purpose for which the information was matched, the Chief Executive Medicare must, within 90 days after the results cease to be needed, take reasonable steps to destroy the results.

Subsection 16(2) provides that if the results of the matching of information by an authorised Commonwealth entity under subsection 132B(1) of the Act are no longer needed for any purpose for which the information was matched, the authorised Commonwealth entity must, within 90 days after the results cease to be needed, take reasonable steps to destroy the results.

This provision is intended to prevent results of data matching being kept unnecessarily, whilst not requiring premature destruction of information that is still needed.

Section 17 – Destruction of personal information not to be matched

Subsection 17(1) provides that if the Chief Executive Medicare holds personal information that was obtained by the Chief Executive Medicare from, or disclosed or provided to the Chief Executive Medicare by, another person or entity for the purpose of facilitating the matching of that information under subsection 132B(1) of the Act, and the information is not intended to be matched, the Chief Executive Medicare must, within 90 days after becoming aware that the information is not intended to be matched, take reasonable steps to destroy the information.

Subsection 17(2) provides that if an authorised Commonwealth entity holds personal information that was obtained by the Chief Executive Medicare from, or disclosed or provided to the Chief Executive Medicare by, another person or entity for the purpose of facilitating the matching of that information under subsection 132B(1) of the Act, and the information is not intended to be matched, the authorised Commonwealth entity must, within 90 days after becoming aware that the information is not intended to be matched, take reasonable steps to destroy the information.

Subsection 17(3) provides that the obligations in subsections 17(1) and 17(2) apply to personal information held for the purposes of facilitating the matching of that information (copies), and do not apply to that personal information held for another purpose or by another person. It is intended that only the copies of personal information for matching be destroyed.

Part 6 – Accuracy, completeness and currency of personal information

Section 18 – Accuracy, completeness and currency of personal information

Subsection 18(1) provides that the Chief Executive Medicare take reasonable steps to ensure that personal information that is matched by the Chief Executive Medicare under subsection 132B(1) of the Act is accurate, complete and up to date.

Authorised Version Explanatory Statement registered 04/01/2021 to F2021L00006

Subsection 18(2) provides that any authorised Commonwealth entity take reasonable steps to ensure that personal information that is matched by the authorised Commonwealth entity under subsection 132B(1) of the Act is accurate, complete and up to date.

Subsection 18(3) provides that the reasonable steps referred to in subsections 18(1) and 18(2) must include the carrying out of quality assurance checks.

Subsection 18(4) provides that subsection 18(5) applies if the Chief Executive Medicare or an authorised Commonwealth entity becomes aware that personal information, that was obtained by the Chief Executive Medicare from, or disclosed or provided to the Chief Executive Medicare by, a Commonwealth entity for the purpose of facilitating the matching of that information under subsection 132B(1) of the Act, is not accurate, complete or up to date.

Subsection 18(5) provides that the other Commonwealth entity be advised in writing that the information is not accurate, complete or up-to-date. This imposes an obligation on the Chief Executive Medicare and authorised Commonwealth entities to notify, in writing, Commonwealth entities that are sources of information to be used for matching under subsection 132B(1) of the Act, if the information provided by the source Commonwealth entity is not accurate, complete or up to date.

Subsection 18(6) provides that if information matched by the Chief Executive Medicare or an authorised Commonwealth entity under subsection 132B(1) of the Act is personal information about an individual, and the individual requests the Chief Executive Medicare to correct the personal information, the Chief Executive Medicare must take such steps (if any) that are reasonable in the circumstances to correct the information. Examples of reasonable steps might include correcting the information, or notifying the source of the information that the individual wishes to correct the information. However, the reasonable steps will be considered in line with the relevant circumstances and the *Privacy Act 1988*. This provision is intended to facilitate individuals in seeking corrections to their own personal information in accordance with the *Privacy Act 1988*.

Part 7 – Decisions about matching of information

Section 19 – Decisions about matching of information

Subsection 19(1) provides that the Chief Executive Medicare must not match information for a permitted purpose under subsection 132B(1) of the Act unless satisfied that the matching is reasonably necessary for that purpose.

Subsection 19(2) provides that an authorised Commonwealth entity must not match information for a permitted purpose under subsection 132B(1) of the Act unless the Chief Executive Medicare is satisfied that the matching is reasonably necessary for that purpose.

Section 19 complements subsection 132B(1) of the Act, which provides the ability for the Chief Executive Medicare to match information for a permitted purpose, by requiring consideration of the link between the matching of information and the permitted purpose(s). As part of the consideration by the Chief Executive Medicare as to whether data matching is reasonably necessary, examples of factors which may inform this consideration might include: the intended permitted purpose(s) for data matching, whether there are any alternative measures to data matching for those permitted purpose(s), and any related

Authorised Version Explanatory Statement registered 04/01/2021 to F2021L00006

compliance concerns, risks, or other insight. The factors which may form part of the consideration by the Chief Executive Medicare are likely to differ on a case-by-case basis.

Section 20 – Decisions about necessary data fields and subjects

Subsection 20(1) provides that if satisfied that it is reasonably necessary to match information for a permitted purpose, the Chief Executive Medicare must decide the data fields and data subjects, in a dataset, that are necessary for the matching.

Subsection 20(2) provides that as part of the decision as to which data fields and data subjects are necessary under subsection 20(1), the Chief Executive Medicare must consider how both the data fields and data subjects can be minimised, and how the use of personal information can be minimised.

Paragraphs 20(2)(a) and 20(2)(b) include examples of how the Chief Executive Medicare may consider how to minimise data fields, data subjects and personal information. For example, to minimise data fields and data subjects, the Chief Executive Medicare may choose to validate existing data rather than seeking new data (such as seeking to confirm existing data with a positive or negative validation like a yes or no response, and only seeking updated or new data where the validation indicates that the existing data is not up to date). Alternatively, the Chief Executive Medicare may choose to use predefined variables (such as only seeking data if it falls within set options, rather than obtaining unique information). The Chief Executive Medicare must also consider how the use of personal information can be minimised, such as by using identifiers within its meaning in the *Privacy Act 1988* (which is a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identify of the individual, but does not include, amongst other things, the individual's name). This provision is intended to support consideration of how the matching of information under section 132B(1) can occur with the minimum amount of information required. However, all situations referred to are illustrative examples of data minimisation and are not describing specific steps to be followed.

Authorised Version Explanatory Statement registered 04/01/2021 to F2021L00006

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

National Health (Data-matching) Principles 2020

This Legislative Instrument is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the Legislative Instrument

The *National Health Act 1953* (the Act) enables the Chief Executive Medicare to match certain information for permitted purposes, which are Medicare compliance and related administrative purposes. This improves the capability of Chief Executive Medicare to detect instances of fraud, inappropriate practice and incorrect claiming in relation to medicare programs such as the Medicare Benefits Schedule and the Pharmaceutical Benefits Scheme.

The Act requires the Minister for Health to make, by legislative instrument, principles in relation to the matching of information: the *National Health (Data-matching) Principles 2020* (the Principles). The Principles provide further safeguards as to the use of information for matching for Medicare compliance purposes, by setting out certain responsibilities that must be met by the Chief Executive Medicare as part of the matching of information. Information must not be matched under the Act until the Principles have commenced.

As some of the information to be matched may include personal and/or sensitive information, the Principles will lay the foundation for the governance of matching activities by establishing high standards for privacy safeguards and the protection of information. Although the *Privacy Act 1988* (Privacy Act) still applies, the Principles impose additional specifications as to the handling and use of personal information as part of data matching.

The Principles only apply to the Chief Executive Medicare and any Commonwealth entity authorised to data match on behalf of the Chief Executive Medicare. The Principles do not impose any obligations on individuals, health organisations or health providers.

Right to Health

The Principles engage the right to health. Article 12(1) of the International Covenant on Economic, Social and Cultural Rights promotes the right of all individuals to enjoy the highest attainable standard of physical and mental health, which may be understood as a right of access to a variety of public health and health care facilities, goods, services, programs, and conditions necessary for the realisation of the highest attainable standard of health.

Authorised Version Explanatory Statement registered 04/01/2021 to F2021L00006

These Principles assist with the progressive realisation of the right of all individuals to enjoy the highest attainable standard of physical and mental health by supporting the integrity of Australia's medicare programs. The Principles will support the matching of information under the Act, enabling the Chief Executive Medicare to confirm whether payments that have been made under medicare programs were made correctly, and recoup incorrect payments where appropriate. This means that more money will be able to be reinvested in new services and medications for the Australian community, improving access to medicare programs for a greater number of Australians.

Right to Privacy
The Principles engage the right to privacy as the matching of information under the Act for permitted purposes may include the disclosure, collection or use of personal information and potentially health information. The Principles set out specific requirements to be met by the Chief Executive Medicare and any authorised Commonwealth entities when matching.

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) provides that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home, correspondence, nor to unlawful attacks on their honour and reputation. This right to privacy can be limited, however, to achieve a legitimate objective where the limitations are lawful and not arbitrary. In order for an interference with the right to privacy to be permissible, the interference must be authorised by law, be consistent with the ICCPR and be reasonable in the circumstances.

To the extent that the matching of information enabled by the Act could be considered to include a limitation on the right to privacy, this limitation is necessary, reasonable and proportionate to the legitimate objective of matching information. This matching enables the Chief Executive Medicare to confirm whether payments that have been made under medicare programs were made correctly, and recoup incorrect payments where appropriate, to support the integrity and sustainability of Medicare.

The Principles aim to promote accountability and minimise potential impacts in the handling personal information, by ensuring that any personal information used in matching for permitted purposes is subject to strict governance obligations. In particular, by requiring a publicly available register, record-keeping, data destruction, data quality and data minimisation, the Principles promote transparency, accountability and good privacy practices. This is in addition to the Privacy Act which continues to apply. Further, the Principles include provisions designed to support the role of the Australian Information Commissioner in the oversight and assessment of information matching.

As a result, the Principles promote the right to privacy by requiring good privacy practice and establishing safeguards and high standards for the protection of personal information when used in matching for permitted Medicare compliance purposes.

Conclusion

The Principles are compatible with human rights because the Principles promote the protection of human rights. To the extent that information matching for permitted Medicare compliance purposes supports the integrity and sustainability of Australia's medicare

Authorised Version Explanatory Statement registered 04/01/2021 to F2021L00006

programs, the Principles also promote the right to health. By setting out safeguards and privacy practices for information matching, the Principles promote the right to privacy.

Greg Hunt

Minister for Health

Authorised Version Explanatory Statement registered 04/01/2021 to F2021L00006