National Health (Data-matching) Principles 2020

I, Greg Hunt, Minister for Health, make the following principles.

Dated 22 December 2020

Greg Hunt
Minister for Health

Contents

Part 1—Preliminary

1 Name

This instrument is the *National Health (Data-matching) Principles 2020*.

2 Commencement

(1) Each provision of this instrument specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information		
Column 1	**Column 2**	**Column 3**
Provisions	**Commencement**	**Date/Details**
1. The whole of this instrument	The day after this instrument is registered.	5 January 2021

Note: This table relates only to the provisions of this instrument as originally made. It will not be amended to deal with any later amendments of this instrument.

(2) Any information in column 3 of the table is not part of this instrument. Information may be inserted in this column, or information in it may be edited, in any published version of this instrument.

3 Authority

This instrument is made under section 132F of the *National Health Act 1953*.

4 Definitions

In this instrument:

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

5 Publishing information about authorised information-matching

The Chief Executive Medicare must publish, on the internet, the following information about authorised information-matching:

(a) an overview of authorised information-matching;

(b) the objectives of authorised information-matching;

(c) a description of each of the following:

(i) how Part VIIIA of the Act provides for authorised information-matching;

(ii) reasons why authorised information-matching may be necessary for a permitted purpose;

(iii) sources of information for authorised information-matching;

(iv) methods used for ensuring that information for authorised information-matching is of sufficient quality;

(v) processes involved in authorised information-matching, including what the results of the processes may be and what may happen to those results;

(vi) timing or frequency of authorised information-matching;

(vii) actions that may be taken as a result of authorised information-matching;

(viii) how public notice of authorised information-matching is given;

(ix) processes for review of authorised information-matching;

(x) the role of the Australian Information Commissioner in relation to authorised information-matching;

(xi) laws (other than the Act) that are relevant to authorised information-matching (such as laws relating to the collection, use or disclosure of information or laws relating to compliance processes).

6 Technical standards for authorised data-matching programs

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

(2) The technical standards for an authorised data-matching program 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.

(3) In matching information under subsection 132B(1) of the Act for an authorised data-matching program, the Chief Executive Medicare must comply with the technical standards for the program.

(4) In matching information under subsection 132B(1) of the Act for an authorised data-matching program, an authorised Commonwealth entity must comply with the technical standards for the program.

7 Evaluation of privacy practices for authorised information-matching

The Chief Executive Medicare must, within 3 years after the commencement of authorised information-matching:

(a) evaluate the privacy practices relating to authorised information-matching; and

(b) prepare a report of the evaluation; and

(c) give a copy of the report to the Australian Information Commissioner.

Part 3—Publicly available register

8 Publicly available register of kinds of information matched

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.

Note: For the information that may be matched, see subsection 132B(1) of the Act.

9 Information that must be included on the publicly available register

The Chief Executive Medicare must include the following information in the publicly available register for each kind of information matched by the Chief Executive Medicare or an authorised Commonwealth entity under subsection 132B(1) of the Act:

(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.

Note 1: For paragraph (d), for acts or practices to which the *Privacy Act 1988* applies, see section 7 of that Act.

Note 2: For paragraph (e), for delegation of powers by the Chief Executive Medicare, see subsections 6(9) to (12) of the Act.

10 Information that may be included on the publicly available register

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.

Part 4—Record-keeping

11 General

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

(2) An authorised Commonwealth entity must keep records of information matched by the Commonwealth entity under subsection 132B(1) of the Act.

12 Records for authorised data-matching programs

(1) 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 this instrument 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.

(2) The records for a program must be sufficient to enable the replication of the matching of the information for the program while the datasets remain available.

(3) Subsection (2) does not require the records to include the datasets.

13 Records of destruction of information and results

(1) The Chief Executive Medicare must keep records of the description of:
   (a) personal information destroyed under subsection 15(1) or 17(1); and
   (b) results of matching destroyed under subsection 16(1).

(2) An authorised Commonwealth entity must keep records of the description of:
   (a) personal information destroyed under subsection 15(2) or 17(2); and
   (b) results of matching destroyed under subsection 16(2).

14 Sufficiency of records for assessment purposes

The records mentioned in sections 11, 12 and 13 must be sufficient to enable the Australian Information Commissioner to conduct an assessment mentioned in paragraph 33C(1)(f) of the *Privacy Act 1988* in relation to the matching of information and the handling of information relating to that matching.

Part 5—Destruction of personal information and results of matching

15 Destruction of personal information when no longer needed after matching

(1) 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 the information was matched, the Chief Executive Medicare must, within 90 days after the information ceases to be needed, take reasonable steps to destroy the information.

(2) 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 the information was matched, the authorised Commonwealth entity must, within 90 days after the information ceases to be needed, take reasonable steps to destroy the information.

Note: Each of subsections (1) and (2) is a requirement for the purposes of paragraph 24(2)(a) of the *Archives Act 1983*.

(3) The requirements in subsections (1) and (2):

(a) apply to personal information as held by the Chief Executive Medicare or the authorised Commonwealth entity for the purpose of the matching of that information under subsection 132B(1) of the Act; and

(b) do not apply to that personal information as held by the Chief Executive Medicare or the authorised Commonwealth entity for another purpose; and

(c) do not apply to that personal information as held by another person.

16 Destruction of results of matching when no longer needed

(1) 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.

(2) 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.

Note: Each of subsections (1) and (2) is a requirement for the purposes of paragraph 24(2)(a) of the *Archives Act 1983*.

17 Destruction of personal information not to be matched

(1) If:

(a) 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

(b) the information is not intended to be matched by the Chief Executive Medicare or an authorised Commonwealth entity under subsection 132B(1) of the Act;

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.

(2) If:

(a) 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

(b) the information is not intended to be matched by the authorised Commonwealth entity under subsection 132B(1) of the Act;

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.

Note: Each of subsections (1) and (2) is a requirement for the purposes of paragraph 24(2)(a) of the *Archives Act 1983*.

(3) The requirements in subsections (1) and (2):

(a) apply to personal information as held by the Chief Executive Medicare or the authorised Commonwealth entity for the purpose of facilitating the matching of that information under subsection 132B(1) of the Act; and

(b) do not apply to that personal information as held by the Chief Executive Medicare or the authorised Commonwealth entity for another purpose; and

(c) do not apply to that personal information as held by another person.

Part 6—Accuracy, completeness and currency of personal information

18 Accuracy, completeness and currency of personal information

Reasonable steps

(1) The Chief Executive Medicare must 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.

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

Quality assurance checks

(3) For the purposes of subsections (1) and (2), the steps must include the carrying out of quality assurance checks.

Advising Commonwealth entities about information that is not accurate, complete and up to date

(4) Subsection (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 and up to date.

(5) The Chief Executive Medicare or the authorised Commonwealth entity must tell the Commonwealth entity in writing that the information is not accurate, complete and up to date.

Corrections

(6) If:

(a) 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

(b) the individual requests the Chief Executive Medicare to correct the information;

the Chief Executive Medicare must take such steps (if any) as are reasonable in the circumstances to correct the information.

Part 7—Decisions about matching of information

19 Decisions about matching of information

(1) The Chief Executive Medicare 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.

(2) 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.

20 Decisions about necessary data fields and subjects

(1) If the Chief Executive Medicare is satisfied that it is reasonably necessary to match information for a permitted purpose, the Chief Executive Medicare must decide the following:

(a) the data fields in a dataset containing the information that are necessary for the matching;

(b) the data subjects (for example, individuals or classes of individuals) in a dataset containing the information that are necessary for the matching.

(2) In making a decision mentioned in subsection (1), the Chief Executive Medicare must consider the following:

(a) how the data fields and data subjects that are necessary for the matching can be minimised (for example, by validating existing data rather than seeking new data or by using predefined variables);

(b) how the use of personal information can be minimised (for example, by using identifiers rather than personal information).