Australian Government

Services Australia

Program Protocol

Data-matching between Services Australia

and

Southern Regional Medical Group

Data Breach in March 2025

Data matching by the Chief Executive Medicare in reliance on s.132B of the *National Health Act 1953*	Yes

Contents

1 Program Protocol 4

1.1 Purpose 4

1.2 Requirement 4

1.3 Definition of data matching 4

2 Data Matching Program 5

2.1 Overview of the program 5

2.2 Objectives 5

2.3 Scope 5

2.4 Previous programs 6

2.5 Public notice 6

3 Data Quality and Handling 6

3.1 File format 6

3.2 Information type 6

3.3 Volume 6

3.4 Data integrity 6

3.5 Data governance 7

3.6 Data exchange 7

4 Data Matching Process 8

4.1 Matching 8

4.2 Resulting actions 8

4.3 Time limits 8

5 Reasons for conducting the program 9

5.1 Services Australia's lawful functions 9

5.2 Social considerations 9

5.3 Costs and benefits 10

6 Legal Authority 10

6.1 Services Australia 10

6.2 Third-Party organisation 11

6.3 Alternate method to obtain the information 11

Appendix A – Technical Standards Report 12

A.1 Purpose 12

A.2 Data to be provided 12

A.3 Matching 13

A.4 Risks and Controls 14

Appendix B – Gazette Notice 16

1 Program Protocol

1.1 Purpose

The purpose of this program protocol is to:

- provide an overview of the program
- outline the objectives of the data matching of records held by Services Australia with information about persons affected by the data breach of Southern Regional Medical Group (**third-party organisation**) in March 2025 (**Data Breach**)
- detail the organisations involved and the data to be provided
- outline the technical controls proposed to ensure data quality, integrity and security in the conduct of the program
- describe the matching process, the output produced and the results of the data match
- outline the possible actions taken in relation to the results of the program
- specify any time limits on the conduct of the program
- indicate what form of notice is to be given, or is intended to be given, to individuals whose privacy is affected by the program

1.2 Requirement

The Office of the Australian Information Commissioner's (**OAIC**) Guidelines on data matching in Australian Government administration (**Data Matching Guidelines**) specify that a program protocol be prepared by agencies conducting certain data matching programs. The Data Matching Guidelines assist Australian Government agencies to use data-matching as an administrative tool in a way that complies with the Australian Privacy Principles (**APPs**) and the *Privacy Act 1988* (**Privacy Act**) and are consistent with good privacy practice. These guidelines are voluntary, but they represent the Information Commissioner's view of best practice. Services Australia complies with these guidelines.

Similarly, the *National Health (Data-matching) Principles 2020* (**Data Matching Principles**) set out several relevant permitted purposes that govern data matching activities undertaken by the Chief Executive Medicare (**CEM**) and authorised Commonwealth entities for the purposes of a Medicare program. The relevant permitted purposes are defined under s. 132AB of the *National Health Act 1953* (Cth).

Services Australia's Privacy Policy outlines how a person may lodge a complaint about how their personal information has been handled and outlines how we will deal with such a complaint. Services Australia's Privacy Policy is available at Your right to privacy - Services Australia

1.3 Definition of data matching

Data matching is the comparison of two or more sets of data to identify similarities or discrepancies. In the context of this protocol, the term data matching means the:

- bringing together of at least two data sets that contain personal information, and
- data sets come from different sources, and
- comparison of those two data sets with the intention of producing a match.

2 Data Matching Program

2.1 Overview of the program

Services Australia administers a range of programs to deliver payments and services on behalf of the Commonwealth. Services Australia maintains the integrity of these payments and services by undertaking activities to ensure customers meet qualification and payability rules, and where required, recover any incorrect payments. Services Australia also maintains the integrity of the information held and disclosed to ensure the privacy of our customers.

This program aims to match records of our customers at risk of identity compromise because of the Data Breach.

Identity crime can result in significant financial loss to individuals, organisations, and government. Fraudsters try to use compromised identities to falsely claim payments and services in the names of other innocent individuals. Identity crime can take the form of theft, as well as manipulation and fabrication. This may result in the creation of new identities, which can grow and remain a burden on agencies and organisations, including Services Australia.

Services Australia will assist affected customers in several ways to prevent and respond to identity fraud.

2.2 Objectives

The key objectives of this program will assist Services Australia to:

- identify Medicare and Centrelink customer records that have been affected, or potentially affected, by the Data Breach
- provide additional protection on these customer records
- undertake targeted detection to ensure payments and services are provided to the right individual
- take action to address any fraudulent activity.

The data matching will enable Services Australia to take appropriate action to:

- respond rapidly to protect those customers whose identities are compromised
- prevent further harm to our customers affected or potentially affected
- provide support to our customers
- detect and disrupt fraud.

These objectives are consistent with the social security law principles of administration including:

- the establishment of procedures to ensure that abuses of the social security system are minimised
- the delivery of services under the law in a fair, courteous, prompt and cost-efficient manner
- the development of a process of monitoring and evaluating delivery of programs with an emphasis on the impact of programs on social security recipients.

2.3 Scope

The scope of this program is restricted to data matching specific attributes if Medicare card numbers and/or Centrelink Customer Reference Numbers (**CRN's**) were exposed, or reasonably suspected to be, as part of the Data Breach.

Services Australia is the matching and primary user of this program with data sourced from the third-party organisation. This is a one-way data exchange. The third-party organisation does not obtain access to the detailed results of the data matching process.

2.4 Previous programs

Services Australia has been conducting similar data matching programs for some time with a range of third-party organisations affected by a data breach. You can find a list of our third-party data matching programs on the Services Australia website:

Data matching activities for third party organisation data breaches - Services Australia

For this reason, a pilot program is not considered necessary for this data matching activity.

2.5 Public notice

The program protocol will be published on Services Australia's website. The program protocol along with any extensions of the program will also be notified in the Australian Government Gazette (see Appendix B).

3 Data Quality and Handling

3.1 File format

Services Australia will request the data attributes in a spreadsheet format. If a spreadsheet cannot be provided, alternate file types will be recommended.

3.2 Information type

The type of information provided will vary according to each third-party organisation and the available data. To ensure match confidence, two primary and one secondary attribute categories are typically requested:

Primary

- Identifier – Centrelink Customer Reference Number or Medicare Number
- Full name – first name and surname (middle name/s if available)

Secondary

- Date of birth
- Address

For some third-party organisations, the date of birth is not available and cannot be provided therefore address attributes may be provided to ensure match confidence.

3.3 Volume

For this protocol, Services Australia has been advised that data attributes relating to approx. 26,000 individuals will be provided by the third-party organisation.

3.4 Data integrity

Services Australia maintains a high level of data integrity and takes measures to maintain these integrity levels, including designing systems that will not accept records that are incomplete and identifying and correcting records that have data items that are inadequate or corrupt.

Measures taken to maintain integrity levels include:

- Developing formulas and systems that will not accept incomplete or illogical records (based on algorithms)

- identifying records for matching that have data items that meet data integrity standards.

Services Australia staff are subject to the *Privacy Act 1988* and statutory secrecy and confidentiality provisions, including under the:

- Centrelink legislation (see heading [6.1])
- Medicare and Health legislation (see heading [6.1])
- *Public Service Act 1999*
- *Criminal Code Act 1995*

3.5 Data governance

Services Australia has adopted several governance principles that provides a logical foundation for achieving good governance at all stages of the data lifecycle.

Principle	Description
Ethical	Data use has a defined business need and aligns to Services Australia's Data Trust and Ethics Framework
Guided	Data management is guided by capable and informed data stewards
Lifecycle managed	Data is actively managed from creation through to archival/destruction
Discoverable	Data is easy to find and accessible
Secure	Data is stored safely, and appropriate access policies are in place
Shared	Data is shared, commensurate with risks and benefits
Defined	The meaning, purpose and context of data is documented
Credible	Data is trusted and data quality is actively managed
Established	Data processes are established, transparent and change is communicated

3.6 Data exchange

Services Australia will negotiate the transfer of the data attributes using one of the following methods:

- email
- secure document sharing platforms approved for government use (such as SIGBOX)
- physical transfer using encrypted removable storage (IronKey USB).

Where required, and before transfer to the Services Australia's network, the data is examined and deemed safe to migrate. The data is then stored on a dedicated network drive. Network drives are controlled through role-based approvals. Only staff with a business need will be able to view the data provided under this program.

4 Data Matching Process

4.1 Matching

Matching involves the comparison of data attributes provided by the third-party organisation with the same customer data attributes held by Services Australia. Services Australia is responsible for completing the data match.

The data attributes are extracted in bulk into a spreadsheet. A matching algorithm and scoring system have been developed for each attribute. This method of matching is used to determine a confidence level.

Services Australia only collects specific data attributes from the third-party organisation that are necessary to ensure a confident match against the same information held in our records. Dates of birth are requested when matching Centrelink data. Dates of birth are requested when matching Medicare data if known to be available from the third-party organisation, otherwise alternate secondary attributes will be requested. If any attributes are unavailable, matching will be attempted using the provided attributes.

Further details can be found in the Technical Standards Report (see Appendix A).

4.2 Resulting actions

Services Australia will assist affected customers in several ways. For each confident match, Services Australia will apply proactive security measures on the impacted customer records. These measures will apply to:

- identify suspicious activity in relation to the customer's accounts, payment and services
- ensure Services Australia can respond quickly and appropriately.

Additionally, affected customer records will be monitored for suspected unauthorised access and changes.

If these measures indicate suspicious activity, certain actions might be taken, which are deemed necessary to alert the customer and mitigate unauthorised access and/or changes, and loss of Commonwealth outlays. For example:

- contacting affected individuals to discuss the suspicious activity
- preventing access to online services or limiting the types of updates that can be made
- an investigation that results in suspension/cancellation of payments.

Services Australia will not create a permanent register or database of matched or non-matched data as part of this program.

Services Australia does not notify individual customers when protective measures have been applied. However, reasonable steps are taken to ensure the public is made aware of the data match and protection measures by publication of this protocol on the Services Australia's website. The website also contains useful information for customers affected by a third-party data breach.

4.3 Time limits

The data matching is most often conducted in a single event after all the required data attributes have been provided to Services Australia. The data matching activities may occur more than once if data is re-examined due to unconfident matches and/or further data is supplied by the third-party organisation. In these situations, Services Australia considers this a single program match cycle.

When the match process is concluded and any protective measures applied, Services Australia considers the data match closed and no subsequent matches will occur.

Services Australia will destroy all data provided by the third-party organisation if it does not lead to a confident match. Destruction occurs within timeframes set out in the *Archives Act 1983* (Cth) and any other relevant laws.

Otherwise, Services Australia will retain the data provided and the records of matched data in accordance with the *Archives Act 1983* and the *Privacy Act 1988*.

5 Reasons for conducting the program

5.1 Services Australia's lawful functions

Services Australia operates under the *Public Governance, Performance and Accountability Act 2013* (Cth) (PGPA Act) and the Commonwealth Fraud and Corruption Control Framework 2024, which makes us responsible to develop appropriate controls and mechanisms to prevent and detect fraud and corruption.

Services Australia is also responsible for administering:

- Centrelink programs – the main Acts being the *Social Security Act 1991*, the *Social Security (Administration) Act 1999, A New Tax System (Family Assistance) (Administration) Act 1999, Student Assistance Act 1973 and Paid Parental Leave Act 2010; and*
- Medicare and health programs – the main Acts being *Health Insurance Act 1973* and *National Health Act 1953.*

The applicable legislative schemes provide eligibility criteria that must be met to enable payments to be made. These requirements are given to payment recipients through written advice authorised under different sections of these Acts for different payment types.

The success of administering Centrelink and Medicare programs is underpinned by the principle that only persons entitled to receive payments do so and receive correct entitlements. It is therefore paramount that Services Australia is well equipped to identify and respond to fraudulent activity arising because of the Data Breach.

5.2 Social considerations

Centrelink and Medicare programs are often topical and of interest to the media and the public. There are some key social issues associated with each program including:

- ensuring those entitled to receive payments and services from the Services Australia do so and that they receive correct entitlements
- the desire of taxpayers to ensure integrity in Services Australia payments, services and recovery processes
- the protection of an individual's right to privacy, including identifying and taking steps to protect individuals who have been the victims of identity theft and minimising or preventing any further harm to those individuals.

There is strong support in the community for Centrelink and Medicare programs that directs available funds only to those who are eligible for assistance. The data-matching program helps to achieve this in two ways:

- through strengthening controls in Services Australia's payment systems, it reduces government outlays, and
- the existence of effective controls in payment systems soon become evident to the community and rapidly increases voluntary compliance.

Suitable safeguards against unreasonable intrusion into the privacy of individuals are built into the data matching arrangements.

5.3 Costs and benefits

There are no capital or establishment costs for this program with incidental running costs offset by the benefits. Internal staffing resources to obtain and prepare data, run analysis activities and review results are delivered within existing agency financial budgets without the need to divert resources from other programs or projects.

Benefits are considered unquantifiable due to fraudulent activities being variable in value and potential in nature. The program outcome to protect the integrity and prevent misuse of customer records will result in financial savings to the Commonwealth in the form of reduced occurrence of fraud. This includes direct reduction in misdirected and fraudulently claimed payments and reduced staffing resources required for record remediation efforts.

6 Legal Authority

6.1 Services Australia

All data collected by Services Australia will be considered personal information. Additionally, data collected by Services Australia will be protected information under Centrelink program legislation and Medicare and Health program legislation. The main Acts are set out in the tables below.

As data matching will occur to identify and prevent abuse of the social security system and/or Medicare and Health programs, the collection of personal information is reasonably necessary for, or directly related to, one or more of Services Australia's functions or activities including the administration of social security law, performing functions in relation to a Medicare and Health programs, and preventing and detecting fraud.

Exceptions to the protected information secrecy provisions will also apply to permit this matching, including:

Centrelink

Legislation	Relevant provision
Social Security (Administration) Act 1999 Division 3 of Part 5, Volume 2 – Confidentiality	ss. 202(2)(d) – for the purposes of the social security law
A New Tax System (Family Assistance) (Administration) Act 1999 Division 2 of Part 6, Volume 2 – Provisions relating to information - Confidentiality	ss. 162(2)(dab) – for the purposes of the social security law
Student Assistance Act 1973 Division 3 of Part 10	ss. 351(2)(dc) – for the purposes of the social security law
Paid Parental Leave Act 2010 Confidentiality Division 3 of Part 4-1 of Chapter 4	ss. 127(2)(db) – for the purposes of the social security law

Medicare and Health

Legislation	Relevant provision
Health Insurance Act 1973	s.130(2)(b) – for the purpose of enabling the officer or any other person to perform duties or functions, or exercise powers, in relation to a medicare program
National Health Act 1953	s.135A(2)(b) - for the purpose of enabling the officer or any other person to perform duties or functions, or exercise powers, in relation to a medicare program

Privacy – APP6

- In relation to Centrelink and Medicare information collected from third-party organisations, Services Australia collects and uses this data for the primary purpose of detecting and addressing fraud.
- In relation to Centrelink and Medicare customer information already held by us, we consider that identifying and assessing fraud is a secondary purpose of collection and so an exception to APP6.1 is required.
- APP6.2(b) provides an exception where the secondary purpose is required or authorised by an Australian law. The disclosure by the third-party, and the collection and use by Services Australia, is permitted under the various Centrelink and Medicare and Health legislation, as set out above - meeting the APP6.2(b) exception.

6.2 Third-Party organisation

In all cases, and before disclosure, Services Australia recommends that organisations obtain advice on any legal restrictions that apply to the lawful disclosure of the requested information.

6.3 Alternate method to obtain the information

Services Australia has several measures in place to prevent and detect identity fraud and government outlays, including detection programs. In addition, Services Australia receives tip-offs from the public in relation to identity fraud.

However, without this program, Services Australia has no mechanism to obtain the information pertaining to the individuals who are, or might be, affected by the Data Breach. Using this program, information received can be assessed to ensure that individual customer records are identified to apply additional protection, and to facilitate targeted detection for suspicious activity.

Appendix A – Technical Standards Report

A.1 Purpose

The purpose of the technical standards report is:

- to ensure that data matching is conducted based on pre-defined standards, including data-quality and security controls
- to ensure compliance with the current requirements of the Data Matching Guidelines and the Data Matching Principles.

A.2 Data to be provided

If a customer's Medicare card number and/or Centrelink Customer Reference Number (**CRN**) was affected as part of the Data Breach, the third-party organisation will provide Services Australia with that attribute and associated personal information to facilitate data matching.

Services Australia will request the data attributes in a spreadsheet, such as Microsoft Excel, saved as one of the following file types *.xlsx, *.csv, *.xml. If a spreadsheet cannot be provided, alternate file types will be recommended, for example, *.txt.

Data attributes	Description	Format preference example
Primary Attributes		
Centrelink Customer Reference Number (CRN)*	Government identifier utilised by the Centrelink Program	A sequence of 9 digits ending with a single alpha character (with or without spaces) – **123456789A** **123 456 789A**
Medicare card number*	Government identifier utilised by the Medicare Program	A sequence of 9-11 numbers (no spaces) Card number only – **123456789** With card issue number – **1234567891** With Individual Reference Number – **12345678911**
Surname*	Customer's Last name	Upper or lower case, hyphens permitted (no other punctuation)
First name*	Customer's First name	Upper or lower case, hyphens permitted (no other punctuation, no nicknames)
Middle names~	Other customer names recorded between First and Last	Upper or lower case, hyphens permitted (no other punctuation)
Full name (can be supplied in place of separated name attributes)	All recorded customer names combined into one string	Upper or lower case, hyphens permitted (no other punctuation, no nicknames or Titles) – **First Middle SURNAME**

* Mandatory ~ only if captured

Data attributes	Description	Format preference example
Secondary Attributes		
Date of birth (DOB) * Centrelink ~ Medicare	Customer's date of birth	Any format recognised as a date in excel (not text) – **DD/MM/YYYY**
Street Address~	Customer's home number and Street or post office box	Any format recognised by Australia Post – **1 Street Name** (no unit number) **U1/1 Street Name** (with unit number)
Suburb~	Customer's home or postal suburb	Any format recognised by Australia Post – **Suburb Name**
State~	Customer's home or postal state	2-3 alpha characters as recognised by Australia Post – **STATE**
Postcode~	Customer's home or postal address	4 digits as recognised by Australia Post – **1234**
Full address (can be supplied in place of separated address attributes)	All recorded customer address components (home or postal) combined into one string	**1 Street Name, Suburb STATE 1234**

* Mandatory ~ only if captured

A.3 Matching

A.3.1 Obtaining, standardising and curating

Services Australia will request the data attributes in an agreed format as per this program protocol. The timing of receipt is subject to the third-party organisations data discovery process, including collation in the format specified.

Services Australia is responsible for:

- receiving the data from the organisation subject to the Data Breach
- matching the data provided with records held and maintained by Services Australia
- the storage and destruction of data during and at the conclusion of the matching process

When received, Services Australia will curate and standardise the data. Services Australia's data matching rules and techniques are well refined. Several manual and automated techniques will be used to complete the curation and standardisation process, such as a data schema, excel formulas (from built-in or developed functions) or power query (or similar) to transform or structure the data as needed. Curation and standardisation also include removal of anomalous and duplicate information. For example:

- names containing numbers or symbols
- names containing repeated letters like 'ZZZZ'
- Medicare or Centrelink numbers in illogical algorithm sequence like '123456789A' or '111222333A'

Format standards are applied to ensure comparison of data attributes e.g. re-formatting a date of birth from DD-MM-YY to DD/MM/YYYY or YYYY-MM-DD to DD/MM/YYYY. Modification is solely for the purpose of format standards.

A.3.2 Comparing

Data will be extracted from the customer records held by Services Australia. The extract is completed in bulk to complete the comparison to the curated data attributes supplied by the third-party organisation. Record matching techniques are used to ensure the correct attributes and customer information is identified.

Comparison involves attribution of a confidence score. For each attribute, scores typically range from 1 to 10. For example, an exact match of full name (first name, middle name/s and surname) will result in a match score of 10, whereas a match of the first name, surname and initial of the middle name, will result in a match score of 8. Similarly, an exact match of the date of birth (day, month and year) will result in a match score of 10, whereas a match of the month and year of birth only will result in a match score of 8.

Scores against all supplied attributes are combined to produce a total for each individual. If the total equals or exceeds a predefined weighting, a confident match result is assigned, and Services Australia will treat the customer's identity as compromised. If the total is less than the predefined weighting, an 'unconfident' match result is assigned. These results are provided to staff for manual assessment.

A.4 Risks and Controls

A.4.1 Unconfident matches and manual assessment

Manual assessment will be undertaken to resolve any matches that generate an unconfident match result. Assessment is completed by staff through comparison of the supplied attributes directly against customer records. Data extracts are not used for this purpose. If the unconfident match based on a data anomaly can be rectified through human logic, the match result will be changed to confident.

Some examples include:

Name variation

An unconfident match may occur because the name provided by the third-party organisation differs to the recorded names on our records. If Services Australia has evidence the person is known by or used this name, the unconfident match will be manually assigned as a confident match. Any contrary outcome will remain as an unconfident match.

Correct government identifier, wrong person

An unconfident match may occur because the third-party organisation recorded a valid Centrelink Customer Reference Number (**CRN**) and/or Medicare card number using the name of another individual. If the oversight can be verified, the unconfident match will be manually assigned as a confident match. Any contrary outcome will remain as an unconfident match.

Transposition error

An unconfident match may occur because the third-party organisation has created a transposition error when collating the data. If the oversight can be verified, the unconfident match will be manually assigned as a confident match. Any contrary outcome will remain as an unconfident match.

A.4.2 Security and confidentiality

Services Australia's core ICT systems have extensive security features to ensure that any information stored within the systems is not:

- subject to accidental or intentional modification
- accessed by Services Australia staff unless such access is necessary for the conduct of the Program or any resulting actions
- disclosed otherwise as contemplated by this protocol or authorised by law

The key security features of the ICT systems are as follows:

- there are system access controls and security groupings
- there are several multifactor log-in protections
- data is encrypted at rest and in-flight
- there are full audit trails of data files and system accesses

Appendix B – Gazette Notice

Commonwealth of Australia Gazette
Published by the Commonwealth of Australia
GOVERNMENT NOTICES

NOTICE OF A DATA MATCHING PROGRAM – SERVICES AUSTRALIA AND SOUTHERN REGIONAL MEDICAL GROUP CUSTOMERS AFFECTED BY MARCH 2025 DATA BREACH

This notice refers to the commencement of a data matching program by Services Australia using information provided by Southern Regional Medical Group about its customers affected by the March 2025 data breach (Data Breach).

The purpose of this data-matching program is to prevent, detect and address fraud relating to customer's Centrelink or Medicare details.

The matching agency is Services Australia. The source entity is Southern Regional Medical Group.

Where a government related identifier e.g. Medicare number or Centrelink Reference Number (CRN) was disclosed, or reasonably expected to have been, as part of the Data Breach, the following data, to the extent captured by and available has been disclosed by Southern Regional Medical Group to Services Australia:

- government identifier number
- customer name
- customer date of birth
- customer address

Services Australia will compare the data provided by Southern Regional Medical Group to Medicare program and Centrelink program customer records. This will assist Services Australia identify affected customers deemed compromised and apply proactive security measures to detect and address fraud.

The initial analysis provided by this organisation indicates that there may be approximately 26,000 impacted customers.

A protocol document describing this program is published here:

Data matching activities for third party organisation data breaches - Services Australia

Services Australia adheres to the OAIC Guidelines on data matching in Australian Government administration and the National Health (Data-matching) Principles 2020 (Health Principles), which include standards for data matching activities. Services Australia's privacy policy is available at:

Privacy Policy - Services Australia

servicesaustralia.gov.au