Australian Government
Department of Human Services

PROGRAM PROTOCOL

Department of Human Services
New Compliance Data Sources
Matching of Centrelink and Medicare Data

July 2019

Table of Contents

1. Description of the Program Protocol

1.1 PURPOSE

The purpose of the program protocol is to:

(i) identify the matching lead and the source lead within the Department of Human Services (DHS)

(ii) detail the direct relationship of the program to the performance of the lawful functions or activities of the matching agency

(iii) set out the legal basis for any collection, use or disclosure of personal information involved in the program

(iv) outline the objectives of the program, the procedures to be employed, the nature and frequency of the data-matching covered by the program and the justifications for it

(v) explain what methods other than data-matching were available and why they were rejected

(vi) detail cost/benefit analysis or other measures of effectiveness, which were taken into account in deciding to initiate the program

(vii) outline the technical controls proposed to ensure data quality, integrity and security in the conduct of the program

(viii) provide details of pilot testing of the program

(ix) outline the nature of the action proposed to be taken in relation to the results of the program, including any letters to be issued by the agency involved

(x) indicate what form of notice is to be given, or is intended to be given, to individuals whose privacy is affected by the program, and

(xi) specify any time limits on the conduct of the program.

1.2 REQUIREMENT FOR A PROGRAM PROTOCOL

The Office of the Australian Information Commissioner's (OAIC's) *Guidelines on Data-Matching in Australian Government Administration* (Guidelines) specify that a program protocol be prepared by agencies conducting certain data-matching programs. These Guidelines are voluntary, but represent OAIC's view of best practice. DHS complies with these Guidelines.

DHS's Privacy Policy outlines how a person can complain about how DHS has handled their personal information and how DHS will deal with such a complaint. DHS's Privacy Policy is available at humanservices.gov.au/privacy.

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 is used to denote the use of computer techniques to compare data found in two or more computer files, to identify cases where there is a risk of incorrect payments and/or fraudulent behaviour.

2. Description of the Data-Matching Program

2.1 SUMMARY OF THE DATA-MATCHING PROGRAM

The purpose of this program is to select non-compliant individuals for investigation and / or administrative action. The focus of this program is to identify persons of interest (POI) who have a high likelihood of fraudulent behaviour ("high risk identities").

Specifically, this program seeks to match identities and details held in Centrelink records with those held in Medicare records. The purpose of this activity is to discover individuals who are not recorded as having experienced a series of expected 'life events' across both programs. Where expected life events have not occurred this may highlight high-risk identities and the need for further analysis to determine possible fraudulent behaviour and/or record correctness.

The key elements are:

- an initial match between identities in Centrelink and Medicare records
- checking for Medicare usage within the past five years (date of medical and/or health providers service only) in relation to Centrelink customers, and
- checking whether original creation of Medicare records occurred at the appropriate time according to the individual's age or residency status in Australia.

DHS's programs are a target for identity and other employment and income-based welfare fraud. Data-matching multiple records is more likely to identify recipients who are possibly engaged in premeditated fraudulent activities.

Alongside fraud considerations, this protocol supports data cleansing activity. When high-risk identities are analysed and found to be genuine, details will be forwarded to the relevant business area to update customer records where appropriate.

Data-matching will occur in accordance with the Technical Standards Report at Attachment A.

2.2 OBJECTIVES

The objectives of the data-matching program are to:

- assist in ensuring that Centrelink payments are only made to those individuals who are entitled to those payments
- provide rigour around the authenticity of recipient identities which will contribute significantly to the Government's desire to provide more services online
- detect and investigate fraud
- provide net savings by detecting overpayments and recovering debt
- contribute to the whole-of-government approach to identify serious and complex fraud so that the integrity of payments and taxpayer expectations are met, and
- increase public awareness and raise voluntary compliance.

3. Agency Involvement

3.1 SOURCE AGENCY

The source that supplies data for the purposes of the data-matching program is Medicare.

3.2 DATA-MATCHING AGENCY

The data-matching agency involved in this program is DHS (Centrelink), which:

- receives the data from Medicare
- matches the data with Centrelink payments of welfare recipients (recipients)
- ensures the security of the data during processing, and
- destroys non-recipient data at the end of each data-matching process.

3.3 PRIMARY USER AGENCY

DHS will be the only entity that makes use of the program's data. The data-matching results will not be shared with or provided to any other agency or organisation. DHS will use the matched data to identify potential non-compliance and fraud.

4. Data Issues

4.1 DATA QUALITY

Poor quality data is of limited value in data-matching. DHS has controls and processes for staff to ensure the accuracy of data. DHS also has a Data Quality Unit dedicated to ensuring records in both the Centrelink and Medicare programs are correct, up to date, de-duplicated and accessible only to authorised persons.

Centrelink and Medicare source data will be examined to ensure that data has been formatted correctly and all required fields have been completed prior to data-matching occurring. This will be conducted by a dedicated data analytics team who will review and enrich relevant data. Where data errors are identified in customer records, these records will not participate in the data-matching activities.

4.2 DATA INTEGRITY

DHS maintains a very high level of data integrity. Measures taken to maintain integrity levels include: designing systems that will not accept records that are incomplete, and identifying and correcting records containing data items that are inadequate or corrupt.

DHS's data items that are used in the data-matching process are standardised. Standardisation is the process whereby data items such as name, address and date of birth are converted to ensure that these items are consistent across all files used for data-matching.

4.3 DATA SECURITY

DHS's staff are subject to existing security controls and the secrecy provisions of the *Social Security (Administration) Act 1999*, *A New Tax System (Family Assistance) (Administration) Act 1999*, the *Paid Parental Leave Act 2010*, the *Student Assistance Act 1973*, the *Disability Services Act 1986*, the *Health Insurance Act 1973* and the *National Health Act 1953*. Access to DHS's computer centres is strictly controlled and entry is properly authorised.

DHS's data is held in secure data platforms. These are core systems that employ strict security controls. DHS's security system provides protection and control of dataset access and system entry and maintains program integrity. Security features include logon identification codes, passwords and security groupings to ensure that access to information is on a needs-only basis. Only departmental staff with a business need have access to view the data described in this protocol.

Existing security arrangements in DHS automatically log user access to data files.

Personal information extracted for use in this data-matching program which does not lead to a data-match is destroyed as soon as practicable and no later than 90 days after the data-matching has occurred.

4.4 DATA USAGE

The data-matching process will match customer data held in the Medicare Benefits Schedule (MBS) with Centrelink's welfare payment data (social security, family assistance, paid parental leave, student assistance and disability services). DHS will only be data-matching MBS data and not Pharmaceutical Benefits Schedule (PBS) data, with welfare payment data.

However, where MBS data identifies an anomaly in customer claiming, DHS may, where appropriate for investigative purposes, undertake a separate check with a customer's PBS data held by the department under the *National Health Act 1953*.

A range of business rules will be used in conjunction with the data match to only select persons for investigation that are high risk identities.

Data-matching is conducted in accordance with OAIC's Guidelines. Data will also be used pursuant to the obligations under the National Health (Privacy) Rules 2018.

Data identified from the MBS and the PBS will be kept separately and not blended into a singular match record.

5. The Data-Matching Process

This data-matching program aims to identify possible instances of fraud against the Centrelink program. Customers who appear on both the Centrelink and Medicare datasets are considered to be 'matches'.

The following information in relation to customers who appear on both the Centrelink and Medicare databases will be data matched:

- standardised first name
- nickname/alias
- standardised surname
- gender
- date of birth
- address
- email address
- telephone number, and
- Medicare Benefits Schedule Usage (date of last service).

Further detail can be found in the Technical Standards Report at Attachment A.

In undertaking the data-matching program, officers in the Fraud Investigation Branch in DHS will match customer data held in the Medicare databases with Centrelink's welfare payment data (social security, family assistance, paid parental leave, student assistance and disability services) using various combinations of the above mentioned information.

For the purposes of the data-matching program, DHS will only view those Medicare records with a matching Centrelink record for that person, and not all Medicare records.

Where matched data identifies some anomaly in customer claiming, officers in the Fraud Investigation Branch will investigate further. Data will be used for individuals who are flagged by the use of high-risk matching profiles. Only cases that merit further examination would be progressed through to intelligence assessment and subsequent investigation.

If evidence is collected which identifies that fraud has occurred, recipients may be interviewed and provided with an explanation of the data-matching that has occurred. They will also be given an opportunity to respond to any allegations.

6. Action resulting from the Data-Matching Program

6.1 INVESTIGATIVE ACTION

When a 'match' is identified, it will then have a set of high-risk profile rules applied to it. If it meets the high-risk criteria, it will be referred for further intelligence analysis.

A decision to investigate a case depends on the supporting intelligence that is uncovered during the analysis phase of individual data-matches. This will include seeking specific transaction data on individuals from Medicare.

When an intelligence analyst has established that fraud is likely to have been committed, the case will be assessed against the fraud investigation selection criteria. If a case meets the criteria, an Intelligence Analyst will prepare an Intelligence Assessment report and send it to the Operational Management Committee for acceptance.

A review is then loaded on the Integrated Review System (IRS), which is aligned to the recipient record, and an investigation record is created on the Investigation Management System (IMS). Investigators use IRS and IMS to record the outcome of their investigations. IRS generates enterprise-wide management information and is the single repository of the outcome of all review and compliance activity.

There are three main outcomes of an investigation. These are:

- brief referral to the Commonwealth Director of Public Prosecutions
- administrative action – raising a debt and/or reducing, suspending or cancelling a customer's payments and/or benefits, and
- investigation does not proceed due to lack of evidence.

Investigations in DHS operate under the provisions of Part 1C of the *Crimes Act 1914* and the Australian Government Investigation Standards (AGIS). Any person suspected of committing fraud against DHS is given the opportunity to participate in a recorded interview and provide their response to allegations.

Upon finalisation of an investigation, record correction is undertaken. This may include:

- correction of legitimate record
- quarantining known false identity records
- linking known false identity records to the individual concerned, and
- steps to protect an identity fraud victim from unauthorised access.

6.2 ADMINISTRATIVE ACTION

Matters that do not meet the fraud investigation selection criteria (or do not progress as investigations for other reasons) but may require some corrective treatment, will be referred to the relevant business areas for appropriate intervention. These business areas have responsibility for notifying the individual of any discrepancies and providing the individual with an opportunity for record correction.

Administrative action may include the reduction, suspension or cancellation of benefits and also includes actions taken to recover any overpaid amounts. Any such decision will be notified to the recipient in writing together with their review rights.

Customers have the right to appeal administrative action taken against them by asking that an Authorised Review Officer (ARO) reviews the debt. If a customer does not agree with the ARO's decision a customer can appeal to the Administrative Appeals Tribunal. This information is available to the recipient within correspondence sent to them during the process. While a review is being conducted, debt repayments can be paused.

If anomalies are identified there are several layers of assurances applied after a data match to ensure that appropriate treatment occurs.

Any matters containing identity anomalies that may need correction, updating or review will be referred back to the Medicare program for their consideration and appropriate action.

No other entities will use the results of the data-matching program.

7. Time Limits applying to the Data-Matching Program

The first data-matching exercise is intended to be conducted as soon as practicable and to occur on a regular basis as required.

Any information that has not led to a data-match, or has resulted in a data-match requiring no further action, will be destroyed where practicable within 14 days, or at least within 90 days after the completion of the data-matching cycle, in line with Guideline 7.4 of the Guidelines.

DHS does not intend to create a permanent register or database on data-matched or non-matched selections as part of this protocol.

8. Public Notice of the Data-Matching Program

The Program Protocol will be published on the DHS website.

The data-matching program will also be notified in the Australian Government Gazette before the commencement of the program.

9. Reasons for Conducting the Program

9.1 RELATIONSHIP WITH THE AGENCY'S LAWFUL FUNCTIONS

The data-matching program is related to DHS's lawful function of limiting payments and benefits to those eligible under relevant legislation. The *Social Security Act 1991,* the *Social Security (Administration) Act 1999*, *A New Tax System (Family Assistance) Act 1999*, *A New Tax System (Family Assistance) (Administration) Act 1999,* the *Paid Parental Leave Act 2010*, the *Student Assistance Act 1973* and the *Disability Services Act 1986* provide eligibility criteria that must be met to enable payments to be made.

These requirements are given to recipients through written advice authorised under different sections of these Acts for different payment types.

9.2 SOCIAL CONSIDERATIONS

Welfare is often topical and of interest to the media and the general public. There are some key social issues associated with the data-matching program:

- that only persons entitled to receive payments and benefits from DHS do so and they receive correct entitlements
- the desire of taxpayers for the income support system to ensure integrity in its payments, services and recovery processes, and
- an individual's right to privacy is protected.

Aligned to those issues is a concern for social justice. In particular, there is strong support in the community for an income support system that directs available funds and services to those most in need of assistance. The program helps to achieve this in two ways:

- by strengthening controls in DHS's payment systems, it reduces the expenditure associated with its programs (which allows government funds to be directed to other priorities), and
- the existence of effective controls in payment systems soon becomes 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 program which is conducted in accordance with OAIC's Guidelines.

10. Legal Authority

10.1 MEDICARE

Paragraph 130(7)(a) of the *Health Insurance Act 1973* and paragraph 135A(7)(a) of the *National Health Act 1953* authorise protected information to be recorded, divulged or communicated where a delegate certifies in writing that it is desirable for the purposes of the administration of an Act administered by the Minister for Social Security, such as the social security law, family assistance law and Acts relating to paid parental leave, student assistance and disability services.

On this basis, DHS's collection of the information is authorised under APP 3.1, as the information is reasonably necessary for, or directly related to, DHS's functions and activities.

APP 6.2(b) does not limit the use or disclosure of personal information by DHS where that use or disclosure is required or authorised by or under law. Where the information used in the data-matching program is authorised by DHS under paragraph 130(7)(a) of the *Health Insurance Act 1973* or paragraph 135A(7)(a) of the *National Health Act 1953*, APP 6 does not limit its use.

There are limited circumstances in which Centrelink officers can receive protected information relating to health and/or professional services a customer may have received. Protected information may be disclosed to the Centrelink program where it is necessary in the public interest under section 130(3)(a) of the *Health Insurance Act 1973* and section 135A(3)(a) of the *National Health Act 1953*.

Public interest disclosure certificates are completed on a case by case basis when deemed to be in the public interest.

10.2 CENTRELINK

Centrelink's collection and use of protected information is authorised by the social security law and other Centrelink legislation under which DHS operates. This is because it is necessary for the proper administration of payments and services under the social security law, family assistance law, and other Centrelink legislation (as set out below).

The following provisions in DHS's Centrelink legislation authorise the collection and use of protected information for the data-matching program:

(a) paragraph 202(2)(d) of the *Social Security (Administration) Act 1999* authorises DHS's involvement in the data-matching as it is for the purposes of the social security law
(b) paragraph 162(2)(d) of the *A New Tax System (Family Assistance) (Administration) Act 1999* authorises DHS's involvement in the data-matching as it is for the purposes of the family assistance law
(c) paragraph 127(2)(d) of the *Paid Parental Leave Act 2010* authorises DHS's involvement in the data-matching as it is for the purposes of the Act
(d) paragraph 351(2)(d) of the *Student Assistance Act 1973* authorises DHS's involvement in the data-matching as it is for the purposes of the Act, and
(e) subsection 28(2A) of the *Disability Services Act 1986* authorises DHS's involvement in the data-matching as it is for the purposes of Part 111 of that Act relating to provision of rehabilitation services, or the administration of the *Social Security Act 1991.*

DHS's collection of information is authorised under APP 3.1 as the information is reasonably necessary for, or directly related to, one or more of DHS's functions or activities. As described above, the use of the information for data-matching is also authorised under APP 6.2(b) as the use is authorised by law.

Medicare only releases sufficient information to Centrelink to allow Centrelink to determine a recipient's correct entitlement and whether administrative action (such as investigation) or other actions (such as referring a matter to the Commonwealth Director of Public Prosecutions) need to be considered.

11. Alternative Methods

Currently, data-matching with Centrelink occurs based on individual risk indicators that may relate to DHS's payments and benefits. This data-matching program aims to build on existing fraud detection methods and current data-matching capabilities by extending the range of information on which investigations are based. Information is being sought outside current data-matching programs and will enable a more informed assessment of potential persons of interest and individual circumstances and how this information may relate to the risk of fraudulent behavior.

The combination of Medicare registration and usage dates, with Centrelink held 'life event' data, provides a unique insight to the use of a claimed identity over time, which cannot be otherwise replicated.

DHS receives tip-offs from members of the public through the Tip-off Recording System. Informants can provide tip-offs to DHS online and via phone.

DHS also has a stand-alone system for staff to report suspected fraud. However, DHS cannot rely on tip-offs from members of the public and staff referrals alone to detect identity fraud.

The addition of Medicare data that is matched (in conjunction with current business processes) will significantly improve efficiencies in flagging incidents of fraud.

12. Pilot/Prior Data-Matching Programs

The current data-matching conducted with Medicare is based on individual risk indicators that may be identified through tactical intelligence or investigation assessments on a person of interest to the department. Matters of interest from a fraud perspective are identified through further intelligence treatment and the investigation of individual cases.

A key objective of the data-matching program is to make more comprehensive and strategic use of Medicare data, where matches are used to add intelligence value to cases suspected of being fraudulent. This will also present the opportunity to identify cases of joint interest to both DHS and the Department of Health.

The data-matching program is considered an enhancement to the current data-matching and case selection process that occurs with Medicare.

The results will be evaluated to determine the effectiveness of the data-matching program and assist in determining the regularity of future data-matching cycles.

13. Costs and Benefits

DHS's risk-based approach uses data from a variety of sources and matches where appropriate to allow a holistic profile of a recipient. Data from both internal and external sources is used in data-matching exercises to identify recipients at risk of incorrect payments or fraudulent activity.

The data-matching program is designed to detect false, manipulated and assumed identities used by customers in submitting multiple claims. It is also designed to detect false information provided by customers relating to employment, medical eligibility and relationship circumstances.

In addition to the quantitative benefits, the matching of Centrelink and Medicare data allows DHS to address issues of non-compliance with customers receiving payments and/or benefits. Over time this will lead to more preventative approaches in addressing fraud, increasing voluntary compliance and reduce debt.

When the costs and benefits (direct savings) are compared, the net benefits of data-matching are significant. As noted in the 2016-17 Annual Report, the net benefit of the department's data-matching under the *Data-Matching Program*[1] was $27.5 million.

[1] NB. Data-Matching conducted as part of the *Data Matching Program (Assistance and Tax) Act 1990* relates only to a subset of all data-matching activities conducted by the department.

13.1 DIRECT COST AND BENEFITS SUMMARY

The following sets out the use and matching of Medicare data to detect cases of identity fraud from the 2013 to 2018 financial years.

• Debts	$4,662,917.98
• Savings (includes payment cancellations and debts)	$5,120,361.98

*Source: MI1204_Report1_Productivity Reports for 30th June for each financial year.

Analysis will be done on the results of this project when completed. This will provide further detail on the cost and benefits of the project. It will also provide intelligence on customers who fail to declare their true identity and the circumstances surrounding such behaviour. It is intended that mitigation and education strategies may be developed based on the intelligence gathered.

14. Evaluation of the program

DHS will evaluate this program after three years of operation and at least every three years while the program continues. As part of the evaluation DHS will document the findings in an evaluation report which will be provided to OAIC and made publicly available.

DHS will also ensure that it’s Privacy Policy and relevant collection notices are updated to reflect any changes to the way personal information is managed as a result of this program.

Australian Government
Department of Human Services

Attachment A
Technical Standards Report

1. Description of Data provided between Centrelink and Medicare

1.1 Data from Medicare to Centrelink

The following data items to be provided to Centrelink by Medicare for record matching purposes:

- Medicare Program Number
- Medicare Identity Number
- Centrelink Customer Reference Number (CRN) / Centrelink Identity
- gender
- name
- date of birth
- date of death
- address
- phone number
- date of service, and
- start and end date, if applicable.

Table 1 – Medicare Identity File

Data item	Description
PGM.ID	Medicare Program Code only
CNPGM.ID	Medicare Program Services number (PIN)
CNSMR.ID	Medicare Program Identifier (Medicare Identity)
ASC.ISS.PARTY.CDE	Other Program codes (including Centrelink)
ASC.ID	Other Program Identifier (including Centrelink CRN)
BIRTH.DTE	Date of birth
DEATH.DTE	Date of death
SEX.CDE	Gender (1 character)
NAME.TITLE	Name title
SURNAME	Surname
GIVEN.NAME.1	First Name
GIVEN.NAME.2	Middle Name
NAME.ETS	End date for name updates
GNAF.PID	Geocoded National Address File (GNAF) identifier
ADR.ID	Address identifier
ADR.LN.1	Raw address line 1 (at least line 1 or 2 has to be completed)
ADR.LN.2	Raw address line 2
UNIT.NUM	Unit Number
STREET.NUM.1	Street Number
STREET.NME	Street Name

LOCALITY	Suburb
STATE.CDE	State
POST.CODE	Postcode
DOS	Date of service
NAME.ETS	End date stamp Names information to identify current name
CNSMR.END.RSN.CDE	Medicare Program Unique Identifier end reason code
CNPGM.STS	Medicare registration date stamp
CNSMR.CHRTC.ETS	End date stamp CNSMR.ID information to identify current version
CNSMR_ADR_EFF_ETS	End date stamp for address information to identify current address
ADR_ETS	End date stamp for address information to identify current address
DVY.POINT.ID	Delivery Point ID (DPID) identifier
CONTACT.TYP.CDE	Contact type (email, phone, mobile
CONTACT.VALUE	Contact details (email address, phone number - not a silent

1.2 Data from Centrelink to Medicare

The following data items to be provided to Medicare by Centrelink for record matching purposes:

- Centrelink Customer Reference Number (CRN) / Centrelink Identity
- gender
- name
- date of birth
- date of death
- address
- email address
- phone number, and
- start and end date, if applicable.

Table 2 – Centrelink Identity File

Data Item	Description
PERSON.ID	Customer Reference Number (CRN) – Centrelink Identity
CUNM.DOB	Date of Birth
CUDD.DEATH.DATE	Date of Death
CUNM.SEX.CODE	Gender
CUNM.SURNAME	Raw Surname
CUNM.1ST.NAME	Raw First Name
CUNM.2ND.NAME	Raw Second Name
CUAD.GEO.GNAF.PERSIST.ID	Geocoded National Address File (GNAF) identifier
CUAD.DLVRY.PNT.ID	DELIVERY POINT ID (DPID) identifier
CUEM.ADDR.ID	Contact address (email address)
CUPH.AUST.AREA.CODE	Phone area code
CUPH.PHONE.NUM	Phone number
CUPH_TYPE_CODE	Phone type (not work or fax)

CUAD.ADDR.1ST.LINE	Address line 1
CUAD.ADDR.2ND.LINE	Address line 2
CUAD.ADS.FLA.NUMER	Flat Number
CUAD.ADS.STR.NUMER	Street Number
CUAD.SUBB.LOC.NAME	Suburb
CUAD.STATE.CODE	State
CUAD.AUS.POSTCODE	Postcode

2. Matching Techniques

2.1 Preparing Medicare data

Medicare data is prepared for record matching by:

- standardising name, address, mobile phone fields
- deleting addresses identifying business, organisational, temporary premises for individuals like hotels, hostels, university, tax agents, aged care facilities, caravan parks, airports
- deleting suburb, street, state, address identified as ‘unknown’
- deleting invalid data before matching like:
  - surnames containing numbers or one letter only
  - names containing repeated letters like ‘ZZZZ’
  - names like ‘baby’, ‘child’, ‘twin’, ‘triplet’, ‘anonymous’
  - customer’s date of birth before 18500101 and child’s date of birth before 19000101, and
- defining last date of Medicare Program service.

2.2 Preparing Centrelink data

Centrelink data is prepared for record matching by:

- standardising name, address, mobile phone fields
- deleting addresses identifying business, organisational, temporary premises for individuals like hotels, hostels, university, tax agents, aged care facilities, caravan parks, airports
- deleting suburb, street, state, address identified as ‘unknown’
- deleting invalid data before matching like:
  - surnames containing numbers or one letter only
  - names containing repeated letters like ‘ZZZZ’
  - names like ‘baby’, ‘child’, ‘twin’, ‘triplet’, ‘anonymous’
  - customer’s date of birth before 18500101 and child’s date of birth before 19000101, and
- for child records in Centrelink, if surname is not recorded, the surname of parents is used as an alias.

2.3 Record matching

Record matching of Centrelink and Medicare information sources is conducted by Centrelink. The output of this matching is provided to Centrelink as ‘matched’ records.

Centrelink identifies customers where there are discrepancies between personal details/circumstances declared to Medicare and personal details / circumstances declared to Centrelink.

This could be:

- variations in name, and
- variations in date of birth.

How Centrelink detects the discrepancies depends on the information gathered. Centrelink may have to use different business rules to obtain an accurate and valid result.

For example, where a Customer Reference Number (CRN), name, address and date of birth are available all items are used in the record matching process.

3. Risks

3.1 Incorrect record matches

Centrelink and Medicare use sophisticated record matching techniques to ensure they identify the correct customers. The techniques use multiple details to obtain a record match.

Very high confidence matches will occur where all fields are matched to a person. Additional manual processes may be undertaken where high confidence record matches do not occur.

Data matching rules and techniques are constantly evolving and being refined to ensure risks are minimised. This is achieved by utilising the learnings of past and present data matching exercises.

4. Data quality controls

When administrative action is proposed, additional checks will take place to ensure the correct customer or partner has been identified.

Centrelink customers will be provided with the opportunity to verify the accuracy of the information before any administrative action is taken.

5. Security features

All departmental core computer systems are strictly controlled with features including:

- system access controls and security groupings
- log in identification codes and password protection, and
- full audit trails of data files and system accesses.

Information about ‘matched’ records is used for intelligence purposes only.