Australian Government

Department of Health and Aged Care

Data Matching Notice

Data Matching for Medicare Compliance Purposes

Contents

The Data Matching Notice

Requirement for Data Matching Notice

This Data Matching Notice (Notice) has been developed to meet the requirements of the *National Health (Data-matching Principles) 2020* (Principles). It is in line with similar practices recommended in the *Guidelines on Data Matching in Australian Government Administration* (Guidelines) developed by the Office of the Australian Information Commissioner (OAIC).

The purpose of the Notice is to provide transparency and public awareness in relation to data matching which is undertaken for a permitted purpose under the *National Health Act 1953* (National Health Act), as part of Medicare provider compliance.

The requirement for the Notice applies to the Chief Executive Medicare (CEM), rather than to any particular government agency. However, this Notice relates only to data matching for Medicare provider compliance undertaken by CEM delegates within the Australian Government Department of Health and Aged Care. To the extent data matching for a permitted purpose is undertaken by CEM delegates within another government agency, each agency is responsible for publishing their own notice and public register.

What is data matching?

Throughout the Notice, the term data matching is used to describe the use of analytical techniques to compare, connect and/or combine data from two separate sources, databases or programs, to analyse results including patterns and anomalies.

In the context of the Notice, data matching refers specifically to matching information under Part VIIIA of the National Health Act for a permitted Medicare compliance purpose (permitted purpose). Data matching is used to identify incorrect claiming, inappropriate practice, or fraud in relation to Medicare programs.

What is Medicare compliance?

Medicare programs are health-related services, benefits, services or facilities including the Medicare Benefits Schedule (MBS), the Pharmaceutical Benefits Scheme (PBS), and other programs set out in the *Human Services (Medicare) Act 1973*. To ensure the sustainability of Medicare into the future, it is critical to protect the integrity of its health payment systems. We have a strong and well-established Medicare compliance program that protects Australia's health payments system through:

- prevention of;
- identification of; and
- taking compliance action;
- in relation to incorrect claiming, inappropriate practice, and fraud by health providers.

This compliance program:

- ensures that public money is not spent on unnecessary services, or lost to waste, inappropriate practice, or fraud; and
- promotes voluntary compliance by demonstrating effective monitoring of claiming practices.

Most health providers claim for services appropriately, however, there are a small proportion that do not. On occasion, claims are also submitted incorrectly by people other than the health provider without their (or the patient's) knowledge.

We conduct and support a variety of compliance activities dependent on the type of non-compliance. These activities include:

- audits;
- letter campaigns;

- practitioner review;
- investigations of suspected fraudulent activity and prosecution of fraud; and
- recovery of debts that have been identified as a result of incorrectly claimed benefits.

Medicare compliance processes incorporate procedural fairness and review rights. Find out more information about these processes such as compliance audits, review and fraud investigations, and compliance education, on the *Health Professional Compliance* internet page.

Why match data?

Objectives of data matching

Historically, we have been reliant on the public and health providers telling us about potentially non-compliant behaviour. This information will continue to be valuable and used in tandem with data matching to efficiently detect incorrect claiming, inappropriate practice, and fraud.

The ability to match information available to us and information provided lawfully by other entities, will enhance our ability to identify behaviour which is not otherwise able to be detected. This can be used for permitted purposes, including compliance audits, review and fraud investigation, as well as analysing Medicare services and educating providers.

It is important to note that:

- Data matching is a compliance identification tool to improve our ability to identify incorrect claiming, inappropriate practice, and fraud.
- Other than this improved ability to identify potential non-compliance, data matching does not expand our powers to conduct compliance activities, nor does it change our approach to conducting compliance activities.
- Data matching does not enable the automation of compliance outcomes or the automatic raising of debts.
- Data matching can only be undertaken if the CEM, or delegate, is satisfied that it is reasonably necessary for a permitted purpose. Examples of the factors which might be considered as part of this are likely to differ on a case-by-case basis but may include consideration of the permitted purposes, whether there are any alternative measures to data matching for those permitted purposes, and any related compliance concerns, risks, or other insight.

For more information, see '*Alternative methods to data matching*'.

Budget measures and management of public resources

Data matching forms part of the 2019-20 Budget Measure: Guaranteeing Medicare – improving quality and safety through stronger compliance. This includes better targeting of investigations into:

- fraud;
- inappropriate practice; and
- incorrect claiming.

This will improve Medicare compliance arrangements and debt recovery practices; and ensure Medicare services are targeted at serving the health needs of Australian patients.

Conducting Medicare compliance data matching is also consistent with our duties and obligations to promote the proper use and management of public resources and recover debts due to the Commonwealth under the *Public Governance, Performance and Accountability Act 2013.*

Other considerations

To ensure Medicare services are targeted and serving the health needs of all Australians, the ability to identify and address incorrect claiming, inappropriate practice or fraud is essential.

Data matching is a tool employed by us to ensure that payments made under a Medicare program were made correctly and to facilitate recoveries where appropriate. This means that more resources will be able to be reinvested in new services and medications for the Australian community, which will improve access to Medicare programs for a greater number of Australians.

Medicare compliance is directly relevant to Australians who receive health services. Fraudulent or incorrect Medicare claims made for a service a patient never received may impact the patient's ability to access Medicare services when needed.

For example, a patient who is provided a GP mental health treatment plan is eligible for Medicare rebates for a set number of individual psychological services per calendar year. Fraudulent claims for these services may falsely count towards the patient's yearly limit of services, which may result in the patient being unable to access their full entitlement when they need to do so.

Broadly these compliance activities are consistent with Australia's international law commitments such as the right of all individuals to enjoy the highest attainable standard of physical and mental health.

Data Matching for Compliance

Legal authority

Part VIIIA of the National Health Act authorises the CEM to match specified types of information for permitted purposes. The National Health Act, the Principles, and the *Privacy Act 1988* (Privacy Act) all contain requirements which are relevant and applicable to data matching.

As the provider compliance function sits with us, CEM delegates undertake data matching for provider compliance purposes. For permitted purposes which are not provider compliance, CEM delegates within Services Australia would be responsible.

The Benefits Integrity and Digital Health Division (BIDHD) is responsible for Medicare provider compliance and BIDHD's Compliance Assessment Branch performs data matching powers of the CEM.

The National Health Act also enables the CEM to authorise a Commonwealth entity to undertake data matching for a permitted purpose on the CEM's behalf.

Permitted purposes

Data matching under the National Health Act is limited to specific permitted purposes, which are listed in section 132A.

a) Each of the following is a permitted purpose for the matching of data:

a) identifying whether a person may have, under a medicare program, claimed or been paid a benefit that exceeds the amount of the benefit that was payable to the person;

b) recovering overpayments of benefits under a medicare program;

c) detecting or investigating contraventions of a law of the Commonwealth relating to a medicare program;

d) detecting or investigating whether a person may have engaged in inappropriate practice;

e) analysing services, benefits, programs or facilities that are provided for under a medicare program, in connection with the purposes mentioned in paragraphs (a) to (d);

f) educating healthcare providers about medicare program requirements.

The data matching process

Data matching involves matching information held by us with information held or provided by other entities for the purposes of health provider compliance.

Data Matching programs involve collecting personal information from someone other than the individual concerned, relevantly:

- data matching input from other source agencies
- data matching output as a result of data matching activities.

Data matching can only occur after a delegate of the CEM is satisfied that the proposed data matching activity is reasonably necessary for a permitted purpose.

We will match:

- Identities and claims information from Medicare programs with data from other Medicare programs, such as the MBS and PBS.
- Identities and claims information from Medicare programs with data from other agencies (source agencies) and *authorised Commonwealth entities* such as the Department of Home Affairs (Home Affairs) or the Department of Veterans' Affairs (DVA).

For examples of the information from source agencies which may be matched, see "*Data matching examples*" below.

We can also match information from other persons or entities if this can be lawfully provided.

Data is transferred from the source agency to us using a secure data transfer connection and held in our secure storage facility.

Different data matching activities may require different datasets. The criteria used to identify a match will depend on the relevant datasets and will evolve as data matching activities progress and key requirements are refined.

For each activity, we will minimise the data required and will only match information that is essential and relevant to the permitted purpose. Partial matches will be manually reviewed or excluded where necessary to ensure data quality. Data matching will be conducted based on pre-determined key data fields or variables.

Wherever possible:

- predefined variables will be used, or existing data will be validated (such as by seeking yes/no responses, or other set options, instead of new information);
- de-identified data will be used; and

- identifiers will be used instead of names or other personal information (see *'Privacy considerations'* below).

What happens after data matching?

Once at least two different data sets have been matched, analysis is conducted on the combined dataset to flag data that may require further assessment.

Where we identify an anomaly in the data, our data analysts verify and validate the information and identify cases that merit further examination. These cases will then progress to our compliance officers. This process typically involves further assessment and manual review, and in some cases, consultation with health professional bodies and stakeholder groups.

If indicated, a matter may be referred for potential compliance action in line with existing compliance processes (including, where relevant, consideration of information submitted by providers). The Department's '*How we ensure Medicare compliance*' web page provides more information on the kind of Medicare compliance actions that may be taken as a result of data matching. In limited cases relating to payments made through the Practice Incentive Program, data matching is used to confirm payment eligibility. Until this is confirmed payment to practices may be withheld. For more information, see '*What is Medicare compliance?*' above.

Data matching examples

Here are some practical examples of what can be identified using data matching:

- **MBS/PBS:** matching pharmaceutical benefit dispensing data to Medicare data will assist in identifying whether corresponding medical consultations and pathology services have been provided to meet pharmaceutical benefit requirements. Patterns outside the norm may be indicative of fraud or inappropriate practice.
- **MBS/Home Affairs:** matching the dates of MBS claims made by a health provider, to Home Affairs records can help determine if a health provider or patient was outside of Australia at the time of the MBS service. This will assist in identifying instances where a health provider may have fraudulently claimed Medicare benefits for services which were not validly provided. Without data matching, we are unable to confirm routinely if health providers are outside of Australia when billing Medicare for services.
- **MBS/DVA:** matching the dates of claims made for services, to identify instances where a health provider is claiming both Medicare and DVA benefits for the same service when they are only entitled to claim one. Without data matching, we have no visibility of when a claim is made through DVA for a service that has also been claimed through Medicare.

Data matching may also assist the detection of:

- when a service has been claimed for payment twice under two separate programs, where only one payment should have been claimed ('double dipping');
- health providers practising outside the conditions on their professional registration, which may represent a health or safety risk to patients;
- when health providers have claimed MBS benefits for medical devices which are not eligible for a Medicare rebate; and
- fraud, where a claim is made for a service or benefit that was never provided.

Data Sources

The National Health Act enables data matching using the data sources described below. A *Public Register* is published on our website and provides details of the kinds of data matching input collected from sources agencies.

MBS and PBS data are sourced from Services Australia. We are already able to access MBS data separately to PBS data, in order to undertake Medicare provider compliance functions.

Other Medicare information

Information may be sourced from Services Australia or other Commonwealth agencies for Medicare programs other than the MBS and PBS.

Other Commonwealth entities as information sources

Commonwealth entities and agencies may share data with us for data matching, provided it is lawful for them to do so. Most data for data matching for permitted purposes will be sourced from:

- Services Australia
- DVA
- Home Affairs.

Information may also be sourced from other agencies such as the Therapeutic Goods Administration.

Before data matching with data from a Commonwealth entity, we will put in place an agreement with the other entity, to establish agreed steps, standards and procedures for any data sharing and use.

My Health Records may not be provided or used for data matching.

Non-Commonwealth information sources

The Australian Health Practitioner Regulation Agency, private health insurers and other entities may provide data to us on a voluntary basis, provided it is lawful for them to do so.

Agencies involved in the data matching

Department of Health and Aged Care

We are the key data matching agency for Medicare provider compliance and the primary user agency of the results of the data matching.

Authorised Commonwealth entities

In certain circumstances, it may be appropriate for us to disclose data to another Commonwealth entity and for a delegate of the CEM to authorise that entity to match that disclosed data with its own data, on behalf of us ('authorised Commonwealth entities').

For example, when an authorised Commonwealth entity holds the larger dataset it may be more secure for that entity to conduct the data matching on our behalf. The relevant results of the data match are then securely transferred to us for evaluation and further consideration. Authorised Commonwealth entities may only match this data for permitted purposes (which relate to Medicare compliance), not their own purposes.

Authorised Commonwealth entities who have matched data on behalf of us are identified on our Public Register found on the *Data Matching for Medicare Compliance Purposes internet page.*

Disclosure

In limited circumstances, we may be permitted or required by law, to disclose information related to data matching. A key example is when a concern has been identified which is relevant to the functions of another agency.

For example, if we identify as a result of data matching, potential fraud relating to the responsibilities of another agency such as DVA or Services Australia, we may provide that information to those agencies for their consideration and potential action in accordance with their legislative obligations.

Disclosure may occur where it is authorised by the relevant secrecy provisions and the Australian Privacy Principles (APPs) including when:

- it forms part of our functions, powers or duties;
- it is certified as being in the public interest; or
- it is to an authority prescribed under the *Health Insurance Regulations 2018* or *National Health Regulation 2016*, in the relevant circumstances.

We will not disclose personal information to overseas recipients as part of our data matching activities.

Data quality

No two data matching activities will be the same. Each activity is likely to:

- match different kinds of information;
- consist of different types of file transfers; and
- be subject to different data quality measures.

More detailed information about data matching activities is located on our Public Register found on the *Data Matching for Medicare Compliance Purposes* internet page.

Technical standards

To meet the CEM's legislative obligations, we will prepare, maintain and comply with technical standards to govern the conduct of data matching it undertakes. Technical standards must include:

- a description of the data supplied by source entities;
- the specification of the relevant data matching algorithm;
- a description of any identified risks for the data matching program and how these will be addressed; and
- description of controls to be used to ensure the integrity of the information and system for data matching and relevant system security features to control and minimise access to personal information.

The technical standards ensure that data matching is conducted subject to specifications which have been considered, documented and complied with. This promotes clarity and consistency in data matching.

Kinds of files transferred for data matching

The structure and content of files will vary depending on the information being transferred and the source of the information. Files will be securely transferred, typically in a tabular format, containing the minimum necessary information to conduct the match, inform compliance activities and ensure data quality.

Type of information

Most data matches will use data taken from either MBS or PBS claims information. This is generated or collected at the time a claim is made and may include personal information (such as patient name, sex, date of birth) and administrative information (such as date and time of the service or claim). DVA claims contain similar information.

When matching MBS data with PBS data, unique patient identifiers are used for the match, instead of names or other recognisable personal information (see *'Privacy considerations'* below). In some instances, when data is matched with data from another Commonwealth agency, a set of personal details is securely provided to act as a reference for the other agency to provide relevant matching records from their database. Personal identifiers will then be allocated and may be used after the initial match.

Measures taken for quality and integrity of data

Data quality is achieved by checking that information is complete, accurate and up to date. Effective data quality practices, programs and tools are in place to ensure high data quality, including data reconciliation and quality assurance checks.

Data fields and data subjects will be minimised so that only data which is reasonably necessary to be matched will be matched. Unnecessary data fields and data subjects will not be shared or used for matching, and data fields and data subjects will be regularly evaluated to ensure they remain relevant and necessary. Further detail in relation to the data quality and minimisation methods are included above in the *‘The data matching process’*.

Data handling

Privacy considerations

In addition to the data matching legislative obligations, we comply with the Privacy Act, the APPs, the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (the Code), and other relevant obligations in respect of the collection, use and disclosure of personal information. Safeguards to protect personal information are built into data matching activities. This includes the data quality and minimisation requirements described above and the data safeguards described below.

We consulted with the OAIC throughout the development of the data matching legislation, and engagement with the OAIC will continue throughout the data matching process.

Our *Privacy Policy* sets out how we comply with the Privacy Act.

Where possible, names are replaced with identifiers (a unique combination of letters or numbers used to verify an individual’s identity without identifying the individual). This also reduces the likelihood of partial matches which might be due to a name change or spelling error.

Data governance

In addition to the provisions within the legislation, we have developed robust, internal governance arrangements to ensure the secure and appropriate handling of data and have implemented consistent procedures, including approval processes for data matching.

Data access safeguards

All our staff are required to have the appropriate Australian Government security clearance for their position. Data is subject to security controls, with access restricted to our staff with the appropriate security clearance, delegation and the ‘need to know.’

All our computer systems are monitored and restricted with security features including:

- access controls and security groupings;
- uniquely identifiable login codes each with password protection; and
- audit trails of access to data files and systems.

Our staff are also subject to relevant secrecy provisions included in the *Health Insurance Act 1973* and the National Health Act, which require officers not to divulge or communicate information obtained as part of their duties, powers or functions, unless permitted by a relevant exception. Penalties apply for breaches of the secrecy provisions.

Data matching may only occur in secure IT environments. As a Commonwealth agency, we must comply with the Australian Government Protective Security Policy Framework and the Australian Government Information Security Manual.

Time limits and data destruction

Data matching will operate on an ongoing basis. However, specific data matches may be one-off or undertaken at regular intervals throughout the year, depending on the potential compliance concern that is being investigated

All information and records are managed in accordance with the provisions of the *Archives Act 1983*, including provisions relating to destruction and retention.

Data matched under the National Health Act or data obtained for matching but not matched will be destroyed within 90 days after we have identified that the data is no longer required for the purpose for which it was obtained or matched. This only applies to copies of data for matching and not the original copy of the data.

We do not use data matching to create permanent registers or databases of matched data. Note that there are existing restrictions on the period for which identified, unmatched MBS and PBS data may be kept.

Public notification of data matching

Our website

A dedicated page, *Data Matching for Medicare Compliance Purposes*, can be found on our website and provides an overview and description of data matching.

Public Register

Also published on our website is a Public Register which provides details for each data matching activity that has been undertaken including:

- a description of the kinds of information matched and the datasets from which the information was taken;
- each permitted purpose for which the information was matched;
- description of information provided to the CEM for data matching and the name of the source agency or entity (excluding individuals);
- the name of the authorised Commonwealth entity (if any) which matched the information
- the name of an entity (if any), such as a private company, which is delegated the data matching powers; and
- optionally, other information about the matching of information may be included.

The data matching Public Register will be updated on an ongoing basis and is available on the *Data Matching for Medicare Compliance Purposes* internet page.

Alternative methods to data matching

We already undertake compliance activities based on tip-offs or analytics. However, it is difficult or impossible to identify types of non-compliance such as ‘double dipping’ without data matching. Data matching enables a broader range of claims to be checked equally, fairly, and efficiently to identify a greater range of non-compliance.

Prior to data matching, a large number of our compliance activities were reliant on tip-offs or individual investigations, which are resource-intensive, and risk being compromised through the provision of incorrect or irrelevant information. Data matching enables more efficient and accurate identification of potential non-compliance.

Review of Data Matching

Given the new and evolving nature of data matching, all aspects of data matching will be subject to ongoing review and amendments. The CEM must, within three years after the commencement of data matching, evaluate the privacy practices relating to data matching, prepare a report of the evaluation and give a copy of the report to the Australian Information Commissioner. This is to ensure that there is a privacy self-evaluation, and that the Australian Information Commissioner has visibility over this evaluation. We may choose to undertake evaluations in an ongoing capacity as required and will consider the subject and any findings of the initial evaluation when determining the content and frequency of any future evaluations.

Oversight of Data Matching

The Australian Information Commissioner, supported by the OAIC, has oversight of data matching undertaken in accordance with the National Health Act. The Australian Information Commissioner is responsible for the functions and duties under the Privacy Act and other laws and has a range of guidance, regulatory and enforcement powers.

The Privacy Act empowers the Australian Information Commissioner to undertake an assessment in relation to data matching undertaken in accordance with the National Health Act, and the handling of information for data matching, including whether we have complied with relevant legislative and privacy obligations. The Principles require us to keep records of data matching sufficient to enable assessment by the Australian Information Commissioner.

Privacy Complaints

A breach of the data matching provisions in the National Health Act, in relation to an individual's personal information, is an interference with the privacy of the individual for the purposes of the Privacy Act. It is your right as an individual, to make a complaint if you think we, or another APP entity subject to the Privacy Act, has mishandled your personal information.

You can also ask for your personal information to be corrected if it is held by us or used for data matching by us and you believe it is incorrect.

If you believe we have breached the Privacy Act or the Code or mishandled your personal information or your personal information is incorrect, please contact our Privacy Officer. Further information about how to make a complaint, request access to, or correction of your personal information can be found in our *Privacy Policy*. Contact details can be found on the *Departmental privacy enquiries* internet page.

You will need to submit your complaint to us or the relevant APP entity before making a complaint to the Australian Information Commissioner. If you have not received a response within 30 days, or you are not happy with our response you can then make a complaint to the Australian *Information Commissioner* at the OAIC.

Further Information

This Notice is provided for general information only. Further details of specific data matching activities are subject to change and will be recorded on our Public Register available on the *Data Matching for Medicare Compliance Purposes* internet page.

The legislative basis for data matching is Part VIIIA of the *National Health Act*.

We will update this Notice periodically to ensure it reflects current data matching practices.

Contact

You may contact us about data matching for compliance purposes at *medicareproviderdatamatching@health.gov.au*

Health.gov.au

All information in this publication is correct as at July 2022