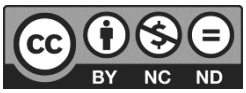
The Auditor-General
Audit Report No.27 2013–14
Performance Audit

Integrity of Medicare Customer Data

Department of Human Services

Australian National Audit Office

ISSN 1036–7632
ISBN 0 642 81442 2 (Print)
ISBN 0 642 81443 0 (Online)



Australian National Audit Office

Canberra ACT
24 April 2014

Dear Mr President
Dear Madam Speaker

The Australian National Audit Office has undertaken an independent performance audit in the Department of Human Services titled *Integrity of Medicare Customer Data.* The audit was conducted in accordance with the authority contained in the *Auditor-General Act 1997*. Pursuant to Senate Standing Order 166 relating to the presentation of documents when the Senate is not sitting, I present the report of this audit to the Parliament.

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's website—http://www.anao.gov.au.

Yours sincerely

Ian McPhee
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits, financial statement audits and assurance reviews of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:

The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Phone: (02) 6203 7505
Fax: (02) 6203 7519
Email: publications@anao.gov.au

ANAO audit reports and information about the ANAO are available on our website:

http://www.anao.gov.au

Audit Team

Kylie Jackson
Clifford Lloyd
Fei Gao
Fiona Knight

Contents

Tables

Figures

Abbreviations

ANAO	Australian National Audit Office
BSB	Bank State Branch
CDMS	Consumer Directory Maintenance System
DIBP	Department of Immigration and Border Protection
ICT	Information and Communication Technology
IHI	Individual Healthcare Identifiers
IPP	Information Privacy Principle
ISM	Information Security Manual
OAIC	Office of the Australian Information Commissioner
PIN	Personal Identification Number
TSR	Technical Standards Report

Glossary

Consumer Directory	The database which is the main repository for Medicare customer data.
Duplicate record	A record in the Consumer Directory for a customer who is enrolled more than once in Medicare.
False positive	A result which indicates a given condition has been fulfilled, when it actually has not been fulfilled.
Intertwined record	A record in the Consumer Directory which is shared by two different customers.
Medicare Data Warehouse	A data repository which contains a copy of Medicare customer data that is used for statistical and performance reporting purposes.
Service Delivery Brand	The Department of Human Services comprises three service delivery brands—Centrelink, Medicare and Child Support.

Summary and Recommendations

Summary

Introduction

1. Medicare is Australia's universal healthcare system, which provides people with access to free or subsidised health and hospital care, with options to also choose private health services. Medicare is one of a range of Australian Government health programs administered through the Department of Human Services (Human Services).[1]

2. In its 2012–13 Annual Report, Human Services reported that as at 30 June 2013, there were 23.4 million people enrolled in Medicare, including 618 533 new enrolments. For an individual to enrol in Medicare, they need to reside in Australia and be either an Australian or New Zealand citizen[2]; a permanent resident visa holder; or an applicant for a permanent resident visa (excluding a parent visa). Australia has Reciprocal Health Care Agreements with 10 countries and visitors from these countries may also be eligible to enrol.[3] Some eligibility types, for example, visitors from Reciprocal Health Care Agreement countries, are only eligible to use Medicare for a limited period of time.

3. In 2012–13, Human Services processed payments totalling $18.6 billion for over 344 million Medicare services. Expenditure under Medicare is expected to continue to grow, with payments estimated to reach $23.7 billion by 2016–17.[4]

4. In administering Medicare, Human Services collects personal information from customers at the time of their enrolment and amends this

1 Medicare is administered by Human Services on behalf of the Department of Health. Medicare was previously administered by Medicare Australia. Prior to 1 October 2005, Medicare Australia was known as the Health Insurance Commission. In this report, Medicare Australia and the Health Insurance Commission are referred to as Human Services. The Department of Health is responsible for Medicare policy.

2 Residents of Norfolk Island are not entitled to enrol in Medicare. Norfolk Island, which is part of the Commonwealth of Australia, is the only self–governing Australian external territory.

3 These are visitors who are residents of the United Kingdom, the Netherlands, Sweden, Slovenia, Norway, Finland and Belgium. Visitors from Italy and Malta who are both citizens and residents of those countries are eligible for a Medicare card for the six month period following their arrival in Australia. Visitors from the Republic of Ireland and New Zealand are not enrolled in Medicare but can access public hospital services as a public patient under the reciprocal agreements.

4 Australian Government, *Budget Paper No. 1: Statement 6: Expenses and Net Capital Investment* [Internet], available from < http://www.budget.gov.au/2013-14/content/bp1/html/bp1_bst6-01.htm> [accessed February 2014].

information to reflect changes in their circumstances.[5] The main repository for this data is the Medicare customer record database, the Consumer Directory.

5. Maintaining the integrity of customer data assists to mitigate key risks associated with Medicare including access to benefits by ineligible people who are enrolled without an entitlement or who are enrolled for a period beyond their entitlement. There is also a risk that ineligible people may obtain an active Medicare card and use it fraudulently to access services and/or make fraudulent claims. In addition, the fraudulent use of Medicare cards as a form of identification is a risk to Medicare and the broader community.[6]

6. Customer data integrity assists in mitigating these risks and contributes to the effective and efficient administration of Medicare. To maintain data integrity, Human Services has implemented both 'upstream' controls at the enrolment stage, and post-enrolment measures to manage updates to its records arising from changed customer circumstances. The department has also implemented measures to protect the privacy and security of customer data.

Audit objective, criteria and scope

7. The objective of the audit was to examine the effectiveness of the Department of Human Services' management of Medicare customer data and the integrity of this data.

8. To assist in evaluating the department's performance in terms of the audit objective, the ANAO developed the following high level criteria:

- Human Services has adequate controls and procedures for the collection and recording of high quality customer data;
- Medicare customer data as recorded on Human Services systems is complete, accurate and reliable; and
- customer data recorded on Human Services systems is subject to an effective quality assurance program and meets relevant privacy and security requirements.

---

5 Enrolment information can be amended on the advice of a customer or their agent, or through data matching.

6 For example, a range of businesses rely on Medicare cards to help satisfy personal identity requirements, including banks and telecommunications companies. Human Services advised the ANAO that it does not endorse this practice.

9. The audit scope focused on the integrity of Medicare customer data and included related testing of all Medicare customer records. It did not examine Healthcare Provider Information, the allocation or management of Individual Healthcare Identifiers (IHI) or the operation of Personally Controlled Electronic Health Records.

10. The audit also considered the extent to which Human Services had implemented the six recommendations from ANAO Performance Audit Report No.24 of 2004–05 *Integrity of Medicare Enrolment Data.*

Overall conclusion

11. Medicare has been in place for 30 years[7] and is accessed by almost all Australians and some visa holders and visitors. In 2012–13, Human Services reported over 23 million people enrolled in Medicare, including 618 533 new enrolments.[8]

12. The department's administration of Medicare is supported by a long-established database, the Consumer Directory, which contains all Medicare customer records. As the repository of a large and evolving data set incorporating, on an ongoing basis, both new enrolments and changes to customer information, the Consumer Directory requires active management to maintain the integrity, security and privacy of customer data; essential prerequisites for the effective administration of Medicare.

13. Human Services' framework for the management of Medicare customer data, including procedures and input controls for the entry of new enrolment information and changes to customer information, has not been fully effective in maintaining the integrity of data in the Consumer Directory. ANAO analysis of the department's Medicare customer data holdings identified[9]:

- at least 18 000 possible duplicate enrolments—an ongoing data integrity issue in the Medicare customer database[10];
- active records for customers without an entitlement as well as inactive records and some with unusual activity; and

7 Medicare came into effect in February 1984. Its predecessor, Medibank, commenced in July 1975.

8 In the same year, Human Services processed $18.6 billion in payments for over 344 million services.

9 There were a total of 29.3 million Medicare customer records as at 16 September 2013, when reviewed by the ANAO.

10 Duplicate enrolments were also identified in the ANAO's 2004–05 performance audit discussed in paragraphs 10 and 18.

- records which had customer information inconsistently, inaccurately and incompletely recorded.

14. In addition, the department advised the ANAO of instances where the records of two different customers are combined ('intertwined records')[11], giving rise to privacy and clinical safety[12] risks.

15. While the number of compromised records held in the database is not significant given the scale of the department's data holdings, the data integrity issues referred to above indicate that departmental procedures and key elements of the data input control framework require management attention to improve operational efficiency, better protect customer privacy and clinical safety, and reduce the risk of fraudulent activity. The extent of the data integrity issues highlighted by the audit and the length of time these issues have been evident also indicate a need for the department to periodically assess the underlying causes of data integrity issues and implement necessary treatments.

16. The audit identified that additional attention should be given to: the tightening of data input controls, including the full and accurate completion of mandatory data fields in accordance with system and business rules; the adequacy and consistency of staff training and written guidance; addressing duplicate and 'intertwined records'; and undertaking data integrity testing on a targeted risk basis. Further, Human Services' procedures for managing the security of Medicare customer data do not comply fully with some mandatory requirements of the Australian Government's Information Security Manual (ISM)[13]; significantly reducing the level of assurance of the relevant systems' ability to withstand security threats from external and internal sources. The department should implement whole-of-government requirements in relation to system security.

17. Positive elements of Human Services' approach to managing Medicare customer data include: unique customer reference numbers within the

11 These are known as 'intertwined' records and occur when two customers are incorrectly enabled to use the same Medicare enrolment identifier. Human Services advised the ANAO that since 2011–12, 34 of these records have been brought to its attention.

12 If one of the affected customers requested a Personally Controlled Electronic Health Record, the record would contain both customers' health information and consequently, could not be relied on by a healthcare provider.

13 The ISM is issued by the Australian Signals Directorate. In May 2013, the Defence Signals Directorate was renamed the Australian Signals Directorate.

Consumer Directory, which have a high degree of integrity[14]; a well-developed privacy framework which contributes to maintaining the confidentiality of sensitive Medicare customer records; and a Quality Framework comprising a daily program of random checks on completed transactions by customer service officers. As discussed however, a fully effective approach to managing the integrity of data holdings requires that attention be given to the development and consistent implementation of the full suite of procedures and controls.

18. The ANAO last examined the integrity of Medicare enrolment data in 2004–05, making six recommendations.[15] Human Services could demonstrate implementation of two recommendations[16] but could not demonstrate implementation of the remainder, which were aimed at addressing data integrity issues, including duplicate enrolments, prior to the migration of Medicare customer data to the Consumer Directory. As discussed, the ANAO's analysis in this audit indicates that the issue of duplicate enrolments has persisted[17]; and, more broadly, the department has foregone an opportunity to enhance its performance by implementing a number of the earlier ANAO recommendations targeted at improving data integrity.[18]

19. The ANAO has made five recommendations in the current audit aimed at enhancing the management and integrity of Medicare customer data by Human Services. The recommendations relate to improving training and guidance for customer service officers, addressing data integrity issues and their causes, and complying with the mandatory requirements of the ISM.

14 Only one duplicate Medicare Reference Number was identified by the ANAO. Human Services investigated this duplicate Medicare Reference Number and found that it had been mistakenly issued by a customer service officer to two different family members sharing the same Medicare card in 1996, using the Medicare Enrolment File (the predecessor of the Consumer Directory). Human Services advised the ANAO that duplicate Medicare Reference Numbers cannot be issued using the Consumer Directory.

15 ANAO Audit Report No.24 2004–05 *Integrity of Medicare Enrolment Data.*

16 Relating to improving its use of Fact of Death Data to automatically update Medicare customer records and preparing a Technical Standards Report as required by the Privacy Commissioner.

17 Refer to paragraph 13.

18 The ANAO recently examined the risks of delaying or not implementing audit recommendations in ANAO Audit Report No.25 2012–13 *Defence's Implementation of Audit Recommendations*, p. 13 and 16 and ANAO Audit Report No.53 2012–13 *Agencies' Implementation of Performance Audit Recommendations*, p. 16.

Key findings by chapter

Data collection and recording (Chapter 2)

20. Medicare customer data, with the exception of claims, is captured mainly when customers enrol in Medicare and when they amend their details. Customer service officers are mostly responsible for entering and updating customer information in Medicare's customer record database, the Consumer Directory. The collection of accurate, complete and reliable customer data supports the efficient and effective administration of Medicare.

21. Customers enrol in Medicare using one of three main forms. There is an opportunity for Human Services to improve the efficiency of the enrolment process by amending the *Medicare Enrolment Application* form to better specify the documentation that visitors are required to provide in support of their enrolment.

22. There are a range of channels for customers to amend their data, including over–the–phone, in–person, in–writing and through self–service options such as Medicare Online Services and the Medicare Express Plus mobile phone application. Customers would benefit from Human Services listing all of these channels on its webpage, *Keeping up to date with Medicare*.[19]

23. To assist customer service officers to enrol customers and amend their personal information, Human Services provides training and guidance on its intranet. While the online training covers the essentials of enrolling customers, it does not include complex enrolment examples. Further, there are inconsistent instructions in and between the training and guidance. For these reasons, Human Services should review its staff training and guidance, in respect to enrolling customers and amending their information, for completeness and consistency.

24. As a further means of collecting and amending customer information, Human Services conducts data matching with other Australian Government departments and state and territory agencies. Customer records are updated with dates of death using an automated process of matching a Fact of Death Data (FODD) file on a monthly basis, compiled from state and territory

19 Department of Human Services, *Keeping up to date with Medicare* [Internet], available from <http://www.humanservices.gov.au/customer/news/keeping–up–to–date–with–medicare> [accessed January 2014].

registries of births, deaths and marriages. This process was introduced by Human Services in 2005 in response to Recommendation No. 5 of the ANAO's performance audit discussed at paragraph 18.

25. When customer information is recorded—at the time of enrolment and if subsequently amended—it is subject to system controls, including address matches with the Postal Address File[20]; BSB validation checks; and field controls. These controls are intended to ensure that data is complete, accurate and reliable. The ANAO's testing of mandatory customer data, which is discussed in paragraphs 33 to 36, indicate that some of these controls are not operating effectively.

26. To further support the collection and amendment of Medicare customer data, Human Services has a Quality Assurance Framework that includes a daily check of randomly selected completed transactions. In 2012–13, 26.8 per cent of these daily checks of Medicare transactions were of customer enrolments and information amendments. The results of these daily checks are reported to the Human Services Executive and stakeholders on a monthly basis and a sample are also reviewed annually for accuracy. For the enrolments and data amendments checked in 2012–13, Human Services reported a 96.3 per cent accuracy rate, which was slightly below the key performance indicator of 98 per cent.

Integrity of unique customer reference numbers (Chapter 3)

27. Unique customer reference numbers are used to identify individual customers and to protect their privacy and clinical safety. Customers enrolled in Medicare are assigned four unique reference numbers in Human Services' records:

- Consumer IDs: record identifier;
- Personal Identification Numbers (PIN): Medicare enrolment identifier;
- Medicare Reference Numbers: card identifier; and
- IHI: identifier within the 'eHealth' environment.[21]

20 The Postal Address File is Australia Post's delivery database which contains details on every delivery point in Australia.

21 The Australian Government's 'eHealth' initiative is the electronic collection, management, storage and sharing of healthcare data.

28. These numbers are used to identify customers and their records and link their information between Human Services' various Medicare databases. The ANAO tested all 29.3 million Medicare customer records in the Consumer Directory. No duplicate unique reference numbers were identified apart from one Medicare Reference Number shared by two different records. Human Services investigated this duplicate Medicare Reference Number and found that it had been mistakenly issued by a customer service officer to two different family members sharing the same Medicare card in 1996, using the Medicare Enrolment File (the predecessor of the Consumer Directory).[22] The testing indicates that unique customer reference numbers have a high degree of integrity.

29. Duplicate customer enrolments mean that customers have more than one of each of these unique customer reference numbers. Consequently, customer information is fragmented across more than one record, posing a risk to the accuracy, completeness and reliability of their personal and health information.

30. Duplicate customer records have been an ongoing data integrity issue in Medicare customer record databases. The ANAO's 2004–05 performance audit recommended that Human Services address duplicate enrolments prior to migrating Medicare customer data to the Consumer Directory (Recommendation No. 3). Human Services advised that it implemented this recommendation but this could not be verified by the ANAO without supporting documentation.

31. The ANAO's testing of all 29.3 million Medicare customer records[23] used varying matching criteria which identified at least 18 000 possible duplicate records.[24] Testing included matches based on names, name initials, dates of birth, addresses and gender as well as varying combinations of these criteria, for example, matches on name and address with a different birth day

22 Human Services advised the ANAO that duplicate Medicare Reference Numbers cannot be issued using the Consumer Directory.

23 There are approximately 29.4 million records in the Consumer Directory, of which 29.3 million are Medicare customer enrolments. The Consumer Directory also includes Australian Organ Donor Register records. Customers who do not provide their consent to link their Australian Organ Donor Register enrolment to their Medicare enrolment will have two records and consequently, two Consumer IDs.

24 These records matched on first name initial, family name, address and date of birth, or first name, family name, address but with a different birth day, month or year. Further, for each match (there are 8797 matches) one of the records appeared to be active while the other record appeared to be inactive suggesting that they were duplicate enrolments.

or month. As part of a continuous improvement approach to managing data in the Consumer Directory, Human Services should consider ways to: better identify duplicate enrolments which take into account these types of variances; investigate the underlying causes of duplicate enrolments; and apply appropriate treatments to address duplicate enrolments.

32. Data integrity can also be weakened by intertwined records, which are single records shared by more than one customer. Intertwined records are created when customer service officers incorrectly enable two customers to use the same PIN—customers' unique Medicare enrolment identifiers. Human Services advised that it has recorded 34 intertwined records since 2011–12, when it commenced recording identified instances. These records pose a risk to the privacy and clinical safety of affected customers as their recorded health information does not accurately reflect their individual circumstances. Human Services has established a working group to address intertwined records. The department should also introduce guidelines to ensure risks are mitigated when these types of records are resolved—which could form part of the work of this group.

Integrity of customer data (Chapter 4)

33. To assist with recording accurate and complete customer data, there are controls in the Consumer Directory including mandatory fields and system rules. Mandatory personal data fields include family name, first name[25], date of birth and most address fields. Mandatory eligibility fields include eligibility document type, a document reference date or number, and an entitlement end date for relevant entitlement types. The ANAO tested these mandatory fields and identified not all mandatory fields had been completed. Further, the ANAO's testing found Medicare customer data which was inconsistently and inaccurately recorded, and which contravened system and business rules.

34. One consequence of errors or omissions in customers' personal data is that existing customer records may not be identified in the customer enrolment search which could result in duplicate enrolments.

35. Of greatest concern are the consequences of incomplete, inaccurate and unreliable eligibility data, which can include payments to ineligible persons. The

25 If the customer has only one name and the 'Only name' indicator is selected on the customer's record, the first name field is not mandatory.

ANAO identified some active customer records with invalid entitlement types which had recent associated claims. Further, some customer records did not:

- contain sufficient information to support customers' eligibility for Medicare. For example, there were 34 129 records for permanent resident visa holders which did not have reference to at least one of the eligibility documents required to support enrolment recorded; and
- reflect an entitlement period consistent with the customer's entitlement type, including not having an entitlement end date recorded despite the customer having a limited entitlement. For example, there were 2743 records for visitors which had no eligibility end date recorded.

36. Human Services should implement controls to ensure that: all mandatory data fields are completed; recorded data is consistent with business and system rules; and customer access to Medicare benefits is consistent with their entitlement. Human Services should also review all customers accessing benefits without a valid entitlement type, to confirm their eligibility.

37. The ANAO tested date of death data and found 40 541 records for customers over 85 years old which did not have an associated claim in the 12 months prior to testing.[26] The absence of claiming activity on these records suggests that these customers may be deceased. The ANAO also identified a customer aged approximately 143 years old who had made a claim in the six months prior to testing. Human Services' investigation of this record showed that the affected customer's date of birth had been incorrectly recorded and the department advised the ANAO that it has subsequently corrected the record. Human Services does not currently undertake data integrity testing. The department should undertake some risk–based, targeted data integrity testing to assist with the identification of records that require review.

38. The ANAO's testing of customer data also provided some insight as to whether Human Services had implemented recommendations made in the ANAO's 2004–05 performance audit discussed in paragraph 18. In particular, the ANAO's testing indicated:

---

26 According to the Australian Bureau of Statistics, in 2012 the average life expectancy for a male and a female at birth was 79.9 years and 84.3 years, respectively. Source: Australian Bureau of Statistics, *1.1 DEATHS, Selected summary statistics — 2002, 2011 and 2012* [Internet], ABS, available from <http://www.abs.gov.au/ausstats/abs@.nsf/mf/3302.0> [accessed November 2013].

- Recommendation No. 1—to cleanse customer data prior to its migration to the Consumer Directory—was not implemented although some of the records relevant to this recommendation have been corrected by Human Services.
- Recommendation No. 2—to apply the Consumer Directory business rules to customer data prior to its migration—was not implemented.
- Recommendation No. 4—to review Human Services' approach to consolidating and migrating customer data to the Consumer Directory—was not implemented.

39. Human Services could not demonstrate implementation of the ANAO's recommendations aimed at improving the integrity of customer information prior to its migration to the Consumer Directory; foregoing an opportunity to address data integrity issues that persist to the present day.

Privacy of customer data (Chapter 5)

40. Human Services has legislative obligations to protect the privacy of customer data and has a well-developed framework to meet its obligations. The central element of its framework is the 'Operational Privacy Policy' which sets out relevant privacy requirements for all staff in an accessible form and provides links to appropriate supporting documentation on protecting privacy. There are policies and processes in place as well as guidance to assist staff to understand their privacy responsibilities, including reporting privacy incidents and complaints, and completing privacy awareness training.

41. Human Services has adopted better practice in requiring Privacy Impact Assessments for new projects. There is an opportunity, however, for Human Services to more consistently apply this requirement to fully realise the benefits of this approach.

42. Human Services is required to comply with the Privacy Commissioner's *Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs*, including the submission of a Technical Standards Report which outlines its management of Medicare customer databases. In 2009, Human Services implemented Recommendation No. 6 of the 2004–05 ANAO audit—to produce and submit a Technical Standards Report—approximately four years after the ANAO's report was tabled. The guidelines also require that Human Services lodge variation reports to the Technical Standards Report. The current Technical Standards report does not reflect current arrangements and

there is an opportunity for Human Services to implement a process to review and update this report and to lodge variation reports in a timely manner.

Security of customer data (Chapter 6)

43. Human Services is subject to the requirements of the Australian Government's Information Security Manual (ISM), issued by the Australian Signals Directorate, which outlines standards to assist agencies in applying a risk–based approach to protecting their data and ICT systems.

44. Human Services undertakes security initiatives outlined in the ISM but falls short of complying fully with the standards outlined. In particular, Human Services is not compliant with two of the mandatory requirements of the ISM. The department has not completed all of the mandatory security documentation required by the ISM for the systems that record, process and store Medicare customer data. Further, it has not completed the certification and accreditation processes for these systems or most of the infrastructure that supports them, as required by the ISM. Fulfilling these requirements would assist Human Services to identify and mitigate risks to the security and confidentiality of Medicare customer data.

45. There is also scope for Human Services to improve its implementation of:

- risk management activities for ICT systems and services by ensuring that controls and treatments to mitigate risks are in place;
- active security monitoring by addressing identified vulnerabilities associated with new ICT systems and taking a risk-based approach to monitoring potential threats to systems; and
- user access management by monitoring and reporting on access to the Medicare Data Warehouse which contains a copy of Medicare customer data.

46. Human Services has also identified areas for improvement in its self–assessment against the Australian Government's *Protective Security Policy Framework*[27] and is taking action to meet its security awareness and training

27 The *Protective Security Policy Framework* is issued by the Attorney–General's Department. It requires that agencies undertake an annual self–assessment of 33 mandatory components.

responsibilities. Further, the department is undergoing an organisation-wide process to develop business continuity plans which address identified critical functions. There would also be benefit in Human Services completing disaster recovery plans in relation to its identified critical functions.

Summary of agency response

47. Human Services provided the following summary comment to the audit report:

> The Department of Human Services welcomes this report and agrees with the five ANAO audit report recommendations. The department recognises that the audit highlights several opportunities to further strengthen and enhance the management and integrity of the Medicare customer data and is strongly committed to ensuring the ongoing completeness, accuracy and reliability of customer records.
>
> The department also notes acknowledgement by the ANAO of its well-developed Privacy and Quality Assurance Frameworks, and the high degree of integrity in the unique customer reference numbers within the Consumer Directory.

48. Human Services' full response is included at Appendix 1.

Recommendations

Recommendation No.1

Para 2.53

To better support customer service officers who enrol Medicare customers and update their information, the ANAO recommends that Human Services review its eLearning training and eReference guidance for consistency and completeness.

Human Services' response: *Agreed.*

Recommendation No.2

Para 3.44

To better manage duplicate and intertwined records and improve the integrity of its customer data, the ANAO recommends that Human Services:

- consider ways to better identify duplicate customer enrolments;
- investigate the underlying causes of duplicate enrolments with a view to informing approaches to their prevention; and
- develop and implement guidelines for resolving intertwined records.

Human Services' response: *Agreed.*

Recommendation No.3

Para 4.33

To further improve the completeness, accuracy and reliability of Medicare customer data, the ANAO recommends that Human Services undertake targeted, risk-based data integrity testing of Medicare customer records.

Human Services' response: *Agreed.*

Recommendation No.4

Para 4.66

To ensure that only those customers eligible to receive Medicare benefits can access them, the ANAO recommends that Human Services review existing entitlement types and implement controls where relevant, to:

- prevent instances of customers being enrolled under invalid entitlement types and accessing Medicare benefits without an entitlement; and
- ensure mandatory data fields are completed, and that data entries are consistent with business and system rules.

Human Services' response: *Agreed.*

Recommendation No.5

Para 6.17

To ensure compliance with the mandatory requirements of the Information Security Manual, the ANAO recommends that Human Services:

- undertake a review of existing documentation and finalise all mandated security documents; and
- complete the mandated certification and accreditation processes for the systems that record, process and store Medicare customer data and the ICT infrastructure that supports them.

Human Services' response: *Agreed.*

Audit Findings

1. Introduction

This chapter describes how Medicare customer data is collected, recorded and updated. It concludes by outlining the audit objective, criteria, scope and methodology and the structure of the remaining chapters.

Medicare

1.1 Medicare is Australia's universal healthcare system, which provides people with access to free or subsidised health and hospital care, with options to also choose private health services. Medicare commenced 30 years ago[28] and is one of a range of Australian Government health programs administered through the Department of Human Services.[29]

1.2 In its 2012–13 Annual Report, Human Services reported that as at 30 June 2013, there were 23.4 million people enrolled in Medicare, including 618 533 new enrolments. In 2012–13, Human Services processed payments totalling $18.6 billion for over 344 million Medicare services. Expenditure under Medicare is expected to continue to grow, with payments estimated to reach $23.6 billion by 2015–16.[30]

1.3 In December 2009, the Australian Government announced the integration of Medicare Australia, together with Centrelink, CRS Australia and Australian Hearing into the Department of Human Services.[31] The aim of this integration was to enable more efficient and effective delivery of government services and give customers more convenient access to services.[32]

---

28 Medicare came into effect in February 1984. Its predecessor, Medibank, commenced in July 1975.

29 Medicare is administered by Human Services on behalf of the Department of Health. Medicare was previously administered by Medicare Australia. Prior to 1 October 2005, Medicare Australia was known as the Health Insurance Commission. In this report, Medicare Australia and the Health Insurance Commission are referred to as Human Services. The Department of Health is responsible for Medicare policy.

30 Australian Government, *Budget Paper No. 1: Statement 6: Expenses and Net Capital Investment* [Internet], available from <http://www.budget.gov.au/2013-14/content/bp1/html/bp1_bst6-01.htm> [accessed February 2014].

31 On 1 July 2011, Medicare Australia was integrated into the Department of Human Services under the *Human Services Legislation Amendment Act 2011.* The department is now responsible for payments and services previously delivered by Medicare Australia.

32 Department of Human Services, *Service Delivery Reform: Transforming government service delivery An update on progress and overview of the reform program* Available at: <http://www.humanservices.gov.au/spw/corporate/about–us/resources/service–delivery–reform–overview.pdf> [accessed 1 November 2013].

1.4 Medicare operates through a network of service centres around Australia which are often co–located with other services such as Centrelink and Child Support. Medicare is collecting customer data, including claims, in a wider variety of ways with the introduction of Medicare Online Services[33] in February 2011 and the release of the Medicare Express Plus mobile phone application[34] in August 2013.

Medicare eligibility

1.5 To be able to claim or receive Medicare benefits, a person must first be enrolled in Medicare.[35] Australian and New Zealand citizens living in Australia, except Norfolk Island residents, are eligible to enrol in Medicare.[36] Permanent resident visa holders and applicants for permanent resident visas (excluding a parent visa), who live in Australia, are also eligible to enrol in Medicare. Visitors from countries with which Australia has a Reciprocal Health Care Agreement (visitors) in place may also be eligible.[37]

Enrolment

1.6 Applications for Medicare enrolment can be submitted in person at a Human Services shop–front or through the mail. The customer service officer processing the application confirms the appropriate proof of identity documentation was provided with the application, or seeks additional information, where necessary. Three forms can be used for enrolling in Medicare:

1. *Medicare enrolment application* form;

33 Medicare Online Services allows customers to access some Medicare services over the internet. Services include claiming for a limited range of items; updating some personal data such as address and bank account details; and viewing claims history.

34 The Medicare Express Plus mobile phone application allows users to view their Medicare claim history for up to three years and update their contact and bank account details as well as claim Medicare benefits.

35 Refer to Sections 6 and 7 of the *Health Insurance Act 1973* which describes Medicare eligibility in terms of how 'certain persons' and 'certain prescribed persons' are to be treated as eligible persons. Section 7 describes agreements for reciprocal treatment of visitors to Australia and other countries.

36 Norfolk Island, which is part of the Commonwealth of Australia, is the only self–governing Australian external territory.

37 These are visitors who are residents of the United Kingdom, the Netherlands, Sweden, Slovenia, Norway, Finland and Belgium. Visitors from Italy and Malta who are both citizens and residents of those countries are eligible for a Medicare card for the six month period following their arrival in Australia. Visitors from the Republic of Ireland and New Zealand are not enrolled in Medicare but can access public hospital services as a public patient under the reciprocal agreements.

2. *Newborn Child Claim for Paid Parental Leave, Family Assistance and Medicare* form; and,
3. *Aboriginal and Torres Strait Islander Medicare enrolment and amendment form.*

1.7 Once enrolled in Medicare, customers are issued with a Medicare card. There are three different types of Medicare cards which are issued based on customers' circumstances (refer to Table 1.1).

Table 1.1: Types of Medicare cards

Type of card	Customer circumstances	Card duration period
Green Medicare card	Australian citizens and permanent resident visa holders	Five years
Blue Medicare card	Permanent resident visa applicants	12 months, with automatic card replacements every 12 months for the first three years
Yellow Medicare card	Visitors	Duration of the visitor's visa

Source: ANAO analysis.

1.8 Customers with a limited eligibility type, for example, visa applicants or visitors, have an eligibility start date and end date recorded on their customer records.

Updating customer information

1.9 Customers' personal information should be updated if their circumstances change. Customers can contact Human Services to update personal information, for example, changes to addresses and bank accounts, over the phone, in–person at a Human Services shopfront or in–writing. Medicare Online Services and the Medicare Express Plus mobile phone application also allow customers to update their address, contact and bank account details. Changes to a customer's name, date of birth[38] or gender must be done in person at a Human Services shop–front and customers are required to provide appropriate supporting documentation.[39]

38 Changes to a person's date of birth are made to correct errors in the original collection and recording of Medicare customer data. It requires appropriate supporting documentation.

39 Appropriate documentation can include a driver's licence, birth certificate and marriage certificate.

1.10 Human Services also undertakes data matching with a number of government agencies to update customer records using those agencies' data including with the Department of Immigration and Border Protection's (DIBP) settlement data for permanent resident visa applicants. In addition, Human Services is an approved recipient agency of the monthly Fact of Death Data (FODD) file, which is compiled by the Australian Institute of Health and Welfare on behalf of the eight Australian registries of births, deaths and marriages.

The Consumer Directory and Medicare Data Warehouse

1.11 There are two central repositories of Medicare customer data: the Consumer Directory and the Medicare Data Warehouse.

1.12 The Consumer Directory is the central database that stores Medicare customer data, including name, date of birth, contact details and bank account details.[40] The Consumer Directory was established in 2005 and replaced the Medicare Enrolment File. Medicare customer records are created and updated in the Consumer Directory database through an interface—the Consumer Directory Maintenance System (CDMS).[41]

1.13 The Medicare Data Warehouse, introduced in 2002, is used for internal and external reporting of Medicare performance and statistics. It contains a copy of Medicare customer data from the Consumer Directory, which is updated daily. Human Services intends to decommission the Medicare Data Warehouse by the third quarter of 2014 and replace it with a single Human Services Enterprise Data Warehouse platform, which will also support the Centrelink and Child Support service delivery brands[42] and the Data-matching Agency.[43] Human Services advised the ANAO that the data associated with each of the service delivery brands will be maintained separately within the new platform.

---

40 From the commencement of Medicare in 1984 through to 2005 and the introduction of the Consumer Directory, the Health Insurance Commission established and maintained the Medicare Enrolment File which was a database designed to receive, store and analyse Medicare enrolment data.

41 Some data, such as data received from data matching activities, is directly recorded in the Consumer Directory.

42 The Department of Human Services includes three service delivery brands: Centrelink, Medicare and Child Support.

43 The Data–matching Agency is a virtual agency located within Human Services that uses data supplied by other Australian Government agencies (such as the Australian Taxation Office) to verify the accuracy of customer data.

The importance of Medicare customer data integrity

1.14 Once a customer is enrolled, the customer can access Medicare benefits and their Medicare card can be used as proof of identity. To support the integrity of Medicare, Human Services requires a robust enrolment process which focuses on: allowing only eligible persons to be enrolled; avoiding duplicate enrolments; and collecting customer data that is complete, accurate and reliable. Effective processes and controls for amending customer data can also assist with maintaining data integrity.

1.15 Customer data integrity assists with the effective and efficient administration of Medicare. Redundant, inaccurate and unreliable data leads to inefficient service delivery and work practices. This can, in turn, impact on customers by causing delays or enable inappropriate access to Medicare.

1.16 Medicare customer data needs to be complete, accurate and reliable as it:

- underpins the Medicare claims processing system;
- assists to prevent identity fraud[44] and fraudulent claims;
- contributes to the efficient operation of the Consumer Directory; and
- mitigates the risk of compromising customer privacy and clinical safety.

ANAO audits of Medicare

1.17 This audit is part of the ANAO's wider coverage of Human Services' management of risks to Medicare. It complements the ANAO's performance audit on *Medicare Compliance Audits* (scheduled to be presented to the Parliament in the second quarter of 2014) which assesses Human Services' management of risks related to health professionals' Medicare Benefit Schedule (MBS) claiming at the post–payment stage. In contrast, this audit examines the department's management of risks at Medicare's entry point, when customers are enrolled.

---

44 Medicare customer data is used to produce Medicare cards which are commonly used to support proof of identity when obtaining a drivers licence or opening a bank account. In early 2013, Medicare cards were accepted as a verification document in the Document Verification Service which aims to reduce the risk of a stolen identity being used and allows for real–time checks of whether Medicare cards are accurate and up–to–date.

1.18 ANAO Audit Report No.24 2004–05 *Integrity of Medicare Enrolment Data* was undertaken when the then Health Insurance Commission was planning the migration of its customer data from the Medicare Enrolment File to its new database, the Consumer Directory. This audit includes an assessment of whether Human Services adequately implemented the agreed recommendations from that audit.

1.19 In 2010–11, the ANAO reported on a cross–agency audit of the effectiveness of Australian Government agencies' management and implementation of measures to protect and secure their electronic data in accordance with Australian Government protective security requirements: ANAO Audit Report No.44 2010–11 *The Protection and Security of Electronic Data Held by Australian Government Agencies.* Medicare Australia was one of the agencies included in the audit, which identified scope for agencies to enhance security measures and highlighted several areas of better practice along with four recommendations aimed at improving approaches to the protection and security of electronic data.

1.20 The ANAO is currently undertaking a further cross–agency audit *Cyber Attacks: Securing Agencies' IT systems*, scheduled to be presented to the Parliament in mid–2014. Human Services is one of the agencies included in this IT–focused audit, which examines compliance with key controls in the Australian Government's Information Security Manual (ISM).[45]

Audit objective, criteria, scope and methodology

Objective

1.21 The audit objective was to examine the effectiveness of the Department of Human Services' management of Medicare customer data and the integrity of this data.

45 The Australian Signals Directorate issues the Australian Government ISM, which is the standard for security of Australian Government and some state and territory agencies' ICT systems.

Criteria

1.22 To assist in evaluating the department's performance in terms of the audit objective, the ANAO developed the following high level criteria:

- Human Services has adequate controls and procedures for the collection and recording of high quality customer data;
- Medicare customer data recorded on Human Services systems is complete, accurate and reliable; and
- customer data recorded on Human Services systems is subject to an effective quality assurance program and meets relevant privacy and security requirements.

Scope

1.23 This audit focused on the integrity of Medicare customer data. It did not examine Healthcare Provider data, the allocation or management of Individual Healthcare Identifiers (IHI) or the operation of Personally Controlled Electronic Health Records.

1.24 The audit considered the extent to which Human Services has implemented the six recommendations from ANAO Performance Audit Report No.24 of 2004–05 *Integrity of Medicare Enrolment Data.*

Methodology

1.25 The audit was conducted by:

- examining training and guidance material for Human Services staff in relation to recording Medicare enrolments and protecting the privacy of customer data;
- reviewing Human Services' documentation including:
  - system documentation for the Consumer Directory, MyGov[46], Medicare Online Services and the Medicare Express Plus mobile phone application;
  - security and privacy policies and reporting; and

46 MyGov is a single log-on account for customers' to access their DHS online accounts.

- interviewing relevant Human Services staff, including customer service officers.

1.26 The ANAO also tested extracts of approximately 29.3 million customer records for completeness, accuracy and reliability. A description of the methodology for the data integrity testing is included in Chapter 3.

1.27 The audit fieldwork was mainly conducted between July 2013 and October 2013. The audit was conducted in accordance with ANAO Auditing Standards at a cost of $486 336.

Structure of chapters

1.28 The remaining chapters are:

- Data Collection and Recording (Chapter 2);
- Integrity of Unique Customer Reference Numbers (Chapter 3);
- Integrity of Customer Data (Chapter 4);
- Privacy of Customer Data (Chapter 5); and
- Security of Customer Data (Chapter 6).

2. Data Collection and Recording

This chapter examines the collection and recording of Medicare customer data. It also discusses the training and guidance provided to customer service officers regarding the enrolment and amendment of customer data.

Introduction

2.1 Human Services collects personal information from customers when they first enrol in Medicare and continues to collect personal information from enrolled customers. Generally, information collected after a customer's enrolment relates to a change in circumstances, such as a change in their address, name, family circumstances and medical history.

2.2 Customers can advise Human Services of changes to their personal information and Human Services will update the customer record, or a customer can record changes to some of their personal information, such as address or bank account details, through self–service channels. Human Services provides training and guidance to customer service officers to assist them to enrol customers and amend their information.

Collecting customer data at enrolment

2.3 Depending on a customer's circumstances, there are three forms used to enrol in Medicare (refer to Table 2.1): *Medicare enrolment application* form; *Newborn Child Claim for Paid Parental Leave, Family Assistance and Medicare* form; and *Aboriginal and Torres Strait Islander Medicare enrolment and amendment form.*

Table 2.1: Medicare enrolment forms

Form	Customers who use form
Medicare enrolment application form	Migrants living in Australia Permanent resident visa applicants who are living in Australia Visitors to Australia Australian citizens returning to live in Australia New Zealand citizens living in Australia Permanent resident visa holders returning to live in Australia
Newborn Child Claim for Parental Leave, Family Assistance and Medicare form	Newborn children born in Australia[1]
Aboriginal and Torres Strait Islander Medicare enrolment and amendment form	Aboriginal and Torres Strait Islanders

Source: ANAO analysis.

Note 1: Parents can also use a *Medicare enrolment application* form to enrol their child in Medicare if they do not have access to the *Newborn Child Claim for Parental Leave, Family Assistance and Medicare* form. If they use the *Medicare enrolment application* form, however, they are required to provide proof of the child's birth, such as a birth certificate.

2.4 These forms are used to collect customer data for enrolment purposes including name, gender, current address, date of birth, telephone number, Aboriginal and Torres Strait Islander origin indicator and details of other applicants. There are some minor differences between the data collected on the forms. For example:

- the *Newborn Child Claim for Paid Parental Leave, Family Assistance and Medicare* form includes a declaration to be completed by the attending midwife or Doctor to confirm the child's birth; and
- the *Aboriginal and Torres Strait Islander Medicare enrolment and amendment form* can be used to collect the signature, name and organisation name of a customer's referee, as Aboriginal and Torres Strait Islanders can use a referee to establish their identity for the purpose of enrolment.

2.5 The information collected on these forms is necessary for the purposes of enrolling customers in Medicare, and contributes to a complete customer record. The suite of forms aims to capture the key data required for the enrolment of each category of applicant. Further, the forms have been adapted where necessary to facilitate the collection of enrolment information—as with the use of referees for Indigenous customers without access to written data on

their identity. There is, however, opportunity to improve the *Medicare enrolment application* form (refer to paragraphs 2.7 to 2.9).

Documentation to support enrolment

2.6 Customers, enrolling in Medicare, are required to provide documentation to support their enrolment, with the exception of applications for newborn children using the *Newborn Child Claim for Paid Parental Leave, Family Assistance and Medicare* form. Table 2.2 outlines the documentation required to support applications using the *Medicare enrolment application* form.

Table 2.2: Eligibility documentation required for Medicare enrolment

Circumstance	Documentation required
Permanent resident visa holder	Current passport; and valid visa or original visa grant letter.
Applicant for a permanent resident visa[1]	Current passport or travel document; and Valid visa or original visa grant letter; and Evidence of relationship with a spouse, parent or child who is an Australian citizen or permanent visa holder, where necessary.
Visitors from a country which has a Reciprocal Health Care Agreement	Current passport and valid visa.
Australian citizens and permanent resident visa holders who have returned to live in Australia[2] and New Zealand citizens living in Australia	Passport; and Completed statutory declaration; and Any two residency documents.[3]

Source: Department of Human Services, *Medicare enrolment application*, Human Services, Canberra.

Note 1: This does not include applicants for a parent visa. Applicants must also have a visa authorising their stay in Australia; and, have permission to work, or their parent, spouse or child is an Australian citizen or holds an Australian permanent resident visa. Holders of visa subclasses 309 and 310 are only required to provide their passport and visa.

Note 2: These requirements are for Australian citizens who have been living overseas for more than five years and for permanent resident visa holders who were previously enrolled in Medicare, have been living overseas and have returned to Australia to live.

Note 3: The form specifies documents required to provide evidence of the applicant's residence overseas and return to Australia. They include property sale/purchase agreements, lease agreements and evidence of employment or education institute enrolment.

2.7 The *Medicare enrolment application* form, which is used to enrol a number of different eligibility types, states that visitors require a current passport and valid visa to enrol in Medicare. The form also states that

additional documentation may be required, however, it does not indicate the type of information required.[47]

2.8 Visitors are required to provide evidence of their health insurance program enrolment from the relevant country, which is not stated on the form. This could lead to a delay in some customers having their enrolment processed if they did not provide the appropriate documentation with their enrolment application. Further, it is an inefficient use of customer service officers' time as they are required to review the application twice.

2.9 There would be benefit in Human Services reviewing its enrolment form and including more data about the documentation required to enrol in Medicare to avoid any unnecessary delays or additional work.

Enrolling a customer in Medicare

2.10 Enrolments are generally processed by Tier 1 customer service officers, who are located in service centres. Complex enrolments[48] are escalated to Tier 2 customer service officers, who also provide technical support to Tier 1 staff by managing their phone–based and email queries.

2.11 There are two key steps for enrolling customers in Medicare:

- complete a search to confirm that the customer does not already have a customer record in the Consumer Directory; and
- record the customer's personal and eligibility data.[49]

Searching for customers' existing records

2.12 Before enrolling a new customer, customer service officers are required to confirm that the customer does not already have a customer record. Customer service officers can search using: family name, first name, middle

47 Reciprocal Health Care Agreements are negotiated with countries which have a healthcare system of a similar standard as Australia and which have approximately the same number of people visiting Australia as Australians visiting that country. Citizens and residents of Belgium, the Netherlands, Italy, Sweden, and Slovenia are required to provide proof of their enrolment in their respective countries' health insurance programs. Visitors who are residents of Norway and Finland are also required to provide evidence of their health insurance enrolments. Human Services advised it is reviewing these requirements.

48 A complex enrolment is any enrolment where there is uncertainty regarding the eligibility or documentation of a person seeking Medicare enrolment.

49 The other step in enrolling a customer is to record the customer's group details and associate them with a Medicare card. A group refers to the group of customers associated with one card, for example, a family.

name, gender, date of birth, age or age range and postcode or postcode range. At a minimum, customer service officers are required to include family name, gender and date of birth in their search.

2.13 The CDMS searches for possible name matches using current data and does not include historical customer data. Where matching records have been identified, these will be listed for the customer service officer to review. Customer service officers can then either select one of the matched records presented or proceed with the enrolment of a new customer.

Searches including data from the Department of Immigration and Border Protection

2.14 Human Services and DIBP had a Memorandum of Understanding, which expired on 30 June 2013, for the exchange of data about:

- permanent resident visa holders;
- permanent resident visa applicants who are living in Australia; and
- applicants for a permanent resident visa under permanent protection.

2.15 Human Services and DIBP have since entered into an overarching Head Agreement, which requires the development of supporting service schedules to replace expired Memorandums of Understanding. Human Services and DIBP are in the process of negotiating these schedules, including one to replace the exchange of data regarding permanent resident visa holders and applicants, who may be eligible for Medicare. To ensure that agreed arrangements are in place to support the continued exchange of this data, Human Services would benefit from seeking to expedite the finalisation of this schedule.

2.16 When conducting a customer search, customer service officers can specify they want to search the DIBP Immigration Client Holding Database for that customer's record to allow them to link the DIBP record to the Human Services record.[50]

2.17 If a record matching the customer's details is returned in the search results, the customer service officer can select the DIBP customer record to

50 Human Services' guidance states that it has entered into an agreement with DIBP to exchange data in relation to customers who have applied for permanent resident visas or who hold permanent resident visas and where possible, the data provided electronically by DIBP should be used to enrol that customer.

link. By linking the records, the Human Services customer record is populated with the customer's data from the DIBP record, including family name, first name, middle name (if applicable), gender, year of birth, entitlement type, entitlement start date and entitlement end date, if applicable.

2.18 The presence of the customer's record in the DIBP database does not mean the customer is eligible for enrolment in Medicare. Customer service officers are required to confirm the customer's eligibility for enrolment and record their eligibility documentation.

Recording a customer's personal and eligibility information

2.19 After undertaking the customer record search, the customer service officer completes recording the customers' personal data and banking details. Once a customer's details are recorded, the customer service officer is required to record the customer's eligibility for Medicare.

2.20 Medicare categorises the documents it receives from customers to support their enrolment into two categories:

- Eligibility: includes documents used to confirm a customer's eligibility for enrolment in Medicare such as birth certificate, passport and visa.
- Residency: includes documents used to confirm the end of a customer's residency in another country and the commencement of the customer's residency in Australia. For example, property sale and purchase documents, lease agreements, gas or electricity bills and evidence of employment or termination of employment.

2.21 After recording these documents, the customer service officer selects the customer's entitlement type from a drop–down list, for example, Australian citizen, visitor or permanent resident visa holder or applicant. The customer service officer is also required to record the country of relevance (for example, the issuing country for the customer's birth certificate) and the entitlement start date.[51] End dates are recorded where the customer's eligibility type entitles them to Medicare benefits for a limited period of time.

51 For Australian citizens born before the introduction of Medicare, customer service officers are instructed to enter an eligibility start date of 01/02/1984.

Controls for recording customer information

2.22 There are system–level controls in the CDMS aimed at ensuring that mandatory customer information is recorded and that information is accurate. There are three key types of controls: address check, BSB check and field controls.

Address check

2.23 The address entered by the customer service officer is automatically checked against the Postal Address File.[52] This check is undertaken so that correspondence from Human Services, including letters containing Medicare cards, are sent to a correct address. A message is generated if the address cannot be verified against the Postal Address File and the officer is required to check that the address that has been recorded is correct.

BSB check

2.24 For the accurate recording of bank account details, recorded BSB numbers are checked against a list of valid BSB numbers and an error message is generated where the BSB number recorded cannot be matched to the list.[53] The combination of the recorded BSB and account number is also checked and an error message is generated where the combination is invalid.

Field controls

2.25 As previously discussed (refer to paragraph 2.21), some fields in the CDMS have a corresponding drop–down list from which customer service officers are required to select a data entry. For example, there are drop-down lists for customer eligibility type, eligibility documentation provided and residency documentation provided. Drop–down lists assist with the consistent recording of data entries.

2.26 Certain fields for customer data are mandatory which means the fields must contain an entry. Error messages should be generated when mandatory fields are not completed. Analysis of these mandatory fields is discussed further in Chapters 3 and 4.

---

52 The Postal Address File is Australia Post's delivery database which contains details on every delivery point in Australia.

53 The BSB list is updated monthly using a file provided by the Reserve Bank of Australia.

Updating customer information

2.27 Information on a customer's record may need to be updated for a range of reasons including changes to personal information or entitlement type, or to record a date of death. The use of effective mechanisms to update information help maintain the accuracy and currency of customer data—contributing to the integrity of Medicare customer data.

2.28 The Human Services webpage, *Keeping up to date with Medicare*, advises customers they can amend their details in–person at a Human Services service centre and through their Medicare Online Services or Medicare Express Plus mobile phone application accounts.[54] However, it does not provide information about updating personal information via mail, over-the-phone or using the *Bank Account Details Collection* form. Customers would benefit from being made aware of all channels available to them to update their personal data. The ANAO suggests that Human Services review the *Keeping up to date with Medicare* webpage and consider listing all channels available to customers to change their personal details.

2.29 Medicare customers can amend their personal information by:

- making a written or verbal request to Human Services which is actioned by a customer service officer; or
- using a self–service channel to amend their contact, address and bank information.[55]

2.30 Amendments are made in the same CDMS fields used for enrolling a customer. Consequently, changes to customer data are subject to the same system controls, which are an address and BSB check, and field controls. Amendments to some data fields generate additional mandatory fields. For example, if a customer's gender is changed, then the Gender Change Reason field becomes a mandatory field.

---

54 Unless the customer lives in a remote location or is unable to visit a Medicare Services Centre, in which case the webpage advises that the customer can post a request to Human Services for their data to be updated, with certified copies of the relevant documentation. Source: Department of Human Services, *Keeping up to date with Medicare* [Internet], available from <http://www.humanservices.gov.au/customer/news/keeping–up–to–date–with–medicare> [accessed January 2014].

55 The functionality offered by the two applications is different. Customers can update more information through Medicare Online Services than through the Medicare Express Plus mobile phone application. For example, customers can update the language they speak at home and their Indigenous or Torres Strait Islander status through Medicare Online Services but not through Medicare Express Plus. Customers cannot use Medicare Online Services to update their South Sea Islander status.

Tell Us Once

2.31 Human Services is introducing a 'Tell Us Once' initiative, scheduled to be completed by 2014–15. This initiative allows customers, when they advise one of the Human Services service delivery brands of a change to their personal information, to provide consent for this change to be applied to their other Human Services service delivery brand customer records. This information is limited to: name, date of birth, gender, residential and postal addresses, email address, phone number and bank account details.

2.32 While the three Human Services service delivery brands store customer records in different databases, customer service officers will use common software to make changes to customer information. This software will then separately update those service delivery brand records that the customer has nominated to be changed.

Date of death data

2.33 Deactivating cards following a customer's death mitigates the risk of fraudulent use of Medicare cards for identity purposes or the use of Medicare cards by ineligible persons to access Medicare benefits.

2.34 Human Services accepts date of death notification from a range of sources including hospitals, family members, nursing homes, estate executors and next of kin. There are a number of ways to notify Human Services of a customer's death:

- completed *Notification of deceased person* form;
- in–person at a Service Centre or over the phone after a Human Services customer service officer has conducted a security check and either, established the informant's relationship to the deceased or established their authority to notify Medicare of the date of death; and
- signed written advice which includes the date of death, identity of the informant and their relationship to the deceased.

2.35 Human Services also conducts automated data matching with the FODD file containing all dates of death notified in the preceding month to the state and territory registries of births, deaths and marriages.

2.36 Where there is an exact match, the Consumer Directory record is automatically updated with the date of death recorded on the FODD file.

Records identified as possible matches are checked manually by a Tier 2 customer service officer team on a daily basis.

2.37 Human Services advised that its automatic data matching consistently returns an exact match rate of around 90 per cent. The introduction of an automated data matching process was recommended by the ANAO in its 2004–05 audit report—in part to address a back–log of FODD files requiring manual processing (Recommendation No. 5). Its introduction, in 2005, has improved the efficiency of Human Services' processing of date of death data and improved the quality of Medicare data by deactivating records which should no longer be active.

Quality assurance

2.38 Human Services has a Quality Framework which provides guidance to staff on quality assurance and quality control procedures.[56] This is in–part aimed at supporting the integrity of customer data as well as the integrity of payments.

2.39 Included in the framework is a daily program of random checks on completed transactions by customer service officers, including enrolments and customer information amendments.[57] In 2012–13, 26.8 per cent of the Medicare transactions sampled by Human Services were customer enrolments and data amendments. These daily checks are used to report on the accuracy of processing to the Human Services Executive and stakeholders on a monthly basis. For the enrolments and information amendments checked in 2012-13, Human Services reported a 96.3 per cent accuracy rate, which was slightly below its key performance indicator of 98 per cent.

2.40 A sample of these daily checks is assessed by Data Quality Officers on an annual basis as part of a process called, 'Aim for Accuracy'. Feedback on identified errors is provided to customer service officers and quality control checkers. This feedback facilitates improvement and learning as an ongoing process and contributes to improving the accuracy and reliability of Medicare customer data.

---

56 New staff have their work reviewed and corrected with the guidance of a mentor until they are deemed capable. This training process is regarded as a form of quality assurance and is a safeguard to improve the quality of the business process.

57 A range of Medicare transactions are checked as part of this process which includes customer claims, bulk billing and enrolment.

2.41 The Quality Framework also includes:

- an annual action plan for quality continuous improvement for Medicare which includes end of year status reports;
- a monthly Human Services Quality Assurance Framework Forum which considers reports on accuracy of processing, and reviews and assesses quality assurance initiatives; and
- research papers which analyse specific errors and produce recommendations to reduce their occurrence.

Training and guidance for Human Services staff

2.42 To effectively enrol customers and update their information, customer service officers require an appropriate understanding of eligibility requirements and how to use the CDMS. Providing training and guidance to a geographically dispersed workforce like Human Services' can be challenging. Human Services uses the intranet to provide training and guidance on enrolling customers and amending their data which aims to support customer service officers to record customer information accurately and completely.

Training for enrolling customers and updating their data

2.43 Human Services has eLearning modules available on its intranet, including eight modules for enrolling customers and six modules on amending customer data.

2.44 The eLearning modules provide straightforward examples of enrolments for Australian citizens, newborn Australian citizens, visitors, permanent resident visa holders and permanent resident visa applicants. However, they do not explain the complex variations to these examples.

2.45 Further, information in some eLearning modules is inconsistent with the guidance provided to staff on Human Services' intranet. There are also instances where the various eLearning modules do not always provide consistent guidance on recording eligibility data.

2.46 The eLearning modules are the only nationally available training on enrolling customers and amending their information as customer service officers do not undertake this type of training as part of their induction. Human Services advised that it prefers nationally consistent training, but in some circumstances locally developed training may be necessary.

2.47 There could be locally developed training on enrolling customers and amending their details at the regional or service centre level. However, there is no central repository that lists the locally developed training. Human Services could not advise if there has been training in addition to the eLearning modules on the enrolment of customers or the amendment of customer information at the local level.

2.48 While eLearning can be a cost effective approach to training, it needs to be fit–for–purpose and consistent with policy and operational requirements. At present, the training available to customer service officers focuses on the essentials of enrolling customers and amending their details. The training does not explain more complex eligibility requirements and contains inconsistent instructions. Given the importance of threshold enrolment information and its amendment to the integrity of Medicare, Human Services should review the adequacy of these training modules.

Guidance on enrolling customers and amending their data

2.49 Human Services provides guidance on its intranet called 'eReference', which contains instructions on enrolling customers and amending their data. It provides greater detail in relation to specific eligibility requirements than the eLearning modules and links relevant guidance.

2.50 Within this structure, there is guidance recorded in different locations which is inconsistent. Consistent instructions would support customer service officers to effectively enrol customers and amend their details. This mitigates the risk of ineligible persons receiving benefits to which they are not entitled.

2.51 eReference includes sample images of some eligibility documentation but not all of the documents customers are required to provide to support their enrolment. Providing additional samples of the different categories of supporting documentation in the eReference guidance would be a cost-effective means to assist customer service officers verify eligibility documentation and identify the appropriate information to record. This can further contribute to the quality of the enrolment process.

2.52 Human Services advised it intends to consolidate reference and guidance materials as part of Service Delivery Reform.[58] It should review the consistency and content of guidance during this consolidation.

Recommendation No.1

2.53 To better support customer service officers who enrol Medicare customers and update their information, the ANAO recommends that Human Services review its eLearning training and eReference guidance for consistency and completeness.

Human Services' response:

2.54 *The department agrees with this recommendation.*

2.55 *The department has commenced a review of Medicare enrolment eReference guidance material. The department's eLearning training will also be reviewed to ensure consistency and completeness.*

58 Service Delivery Reform was announced by the Australian Government in December 2009. As part of the DHS integration, this five-year reform focuses on improving the effectiveness and efficiency of service delivery coordination and providing better access to social, health and welfare services.

3. Integrity of Unique Customer Reference Numbers

This chapter examines the integrity of the unique customer reference numbers recorded in the Consumer Directory, focussing on the incidence of duplicate reference numbers and enrolments.

Introduction

3.1 Unique customer reference numbers support the integrity of Medicare. These numbers are used to uniquely identify customers, their health data and their records. In turn, this assists to protect their privacy and the integrity of their clinical data.

3.2 Risks to the integrity of unique Medicare customer reference numbers arise where customers share these numbers or have more than one unique reference number. The ANAO tested the Medicare customer data for duplicate reference numbers and enrolments, which can result from compromised system controls and human error.

3.3 The ANAO requested an extract of Medicare customer records to test them for accuracy, completeness and reliability. For the extract, the ANAO requested specific data fields that are stored on all Medicare customer records[59], including the unique Medicare customer reference numbers. The records were extracted from the Medicare Data Warehouse[60] which contains a copy of the Medicare customer data stored in the Consumer Directory, which is updated daily.[61]

59 This included the records of customers who were living (approximately 24 million records), deceased (three million records) and whose enrolments were closed, such as visitors who no longer have an entitlement to Medicare (three million records). Each record contained the 'most current' data for each customer, for example, their current family name, resulting in the exclusion of historical data such as their maiden name.

60 The Medicare Data Warehouse produces internal and external reporting of Medicare performance and statistical data.

61 Human Services extracted the records over a period of two weeks commencing 3 September 2013. With some of the extracts being almost 30 million records in size, Human Services could not complete the extract in one day. Consequently, later extracts contained more records than earlier ones because they contained new records. The ANAO estimates the difference in the number of records between these extracts to be approximately 0.01 per cent.

Unique reference numbers

3.4 There are four unique reference numbers associated with each Medicare customer: Consumer ID; PIN; Medicare Reference Number; and IHI. These numbers are used to uniquely identify customers and their records, as well as to link customer data in the Consumer Directory and Medicare's various databases.[62]

3.5 Human Services intends that customers enrolled in Medicare should not be assigned identical reference numbers. Such a situation would compromise the integrity of Medicare customer data and present risks to customer privacy and clinical safety. The ANAO tested Medicare's customer records for duplicate reference numbers, as shown in Table 3.1.

Table 3.1: Results of ANAO's testing of Medicare unique customer reference numbers

Unique customer reference number	Purpose of the number	No. of unique reference numbers	No. of duplicates identified
Consumer ID: allocated to each customer record when it is created in the Consumer Directory.	Used to identify individual customer records.	29 438 433 Consumer IDs[1]	Nil
PIN: unique Medicare enrolment numbers.	Used to link customer records to their Medicare cards.	29 309 993 PINs	Nil
Medicare Reference Number: the combination of the customer's Medicare card number and their position on the card.	Used by healthcare providers to claim payments for Medicare services.	30 528 562 Medicare Reference Numbers[2]	One

62 Human Services is required under the *National Health Act 1953* to maintain customers' Medicare claims data in a separate database from customers' Pharmaceuticals Benefits Scheme data.

Unique customer reference number	Purpose of the number	No. of unique reference numbers	No. of duplicates identified
IHI: allocated to customers with an active Medicare enrolment in 2010.	Used as customer reference numbers for the Australian Government's 'eHealth' initiative.[3]	25 521 310 IHIs	Nil

Source: ANAO analysis.

Note 1: The Consumer Directory also includes data about customers' enrolments in the Australian Organ Donor Register. Customers who do not provide their consent to link their Australian Organ Donor Register enrolment to their Medicare enrolment will have two records and consequently, two Consumer IDs.

Note 2: Customers can have more than one Medicare Reference Number as they can be listed on more than one Medicare card. For example, a child with separated parents may be listed on both their mother's and father's cards.

Note 3: The Australian Government's 'eHealth' initiative is the electronic collection, management, storage and sharing of healthcare data.

3.6 As shown in Table 3.1, the ANAO identified one Medicare Reference Number which is shared by two customer records. Human Services investigated this duplicate Medicare Reference Number and found that it had been mistakenly issued by a customer service officer to two different family members sharing the same Medicare card in 1996, using the Medicare Enrolment File (the predecessor of the Consumer Directory). Human Services advised the ANAO that duplicate Medicare Reference Numbers cannot be issued using the Consumer Directory.

3.7 Up to nine people can be listed on a Medicare card so position numbers are between one and nine (see Figure 3.1 for a sample card). The ANAO identified 126 561 Medicare Reference Numbers with a position number of zero.

Figure 3.1: Sample Medicare card

Source: Department of Human Services, *Medicare* [Internet], available from <http://www.humanservices.gov.au/customer/dhs/medicare> [accessed March 2014].

3.8 Human Services advised that there are two causes of such records. The first is a process specified in the Medicare card business rules which allocates a position number of zero to a customer when they are added to and removed from a Medicare card on the same day.

3.9 The second cause of Medicare Reference Numbers having a position number of zero relates to the process used to allocate customers a Medicare card position number, when position numbers were first introduced in 1991. The first step in this process was to allocate customers with a position number of zero. When new cards were issued to customers, position numbers between one and nine were subsequently allocated. However, if customers were not issued a new card, their position number remained as zero.

3.10 The majority of the customers who had a position number of zero were associated with another card and had another valid Medicare Reference Number. However, the ANAO found that 14 of the customers who had a position number of zero were not associated with another card and had lodged claims using the invalid Medicare Reference Number. This indicates a weakness in Human Services' claiming system, which requires investigation by the department.

Duplicate customer records

3.11 Duplicate records are a threat to the integrity of a database as they fragment data. For Human Services, this risk relates to the accuracy, completeness and reliability of customer data which may be fragmented across more than one customer record. There is also a risk that duplicate customer enrolments can be used for fraudulent claiming or identity theft.

Findings from the ANAO's 2004–05 performance audit

3.12 Duplicate records, or duplicate customer enrolments, have been an ongoing data integrity issue in Medicare customer record databases. ANAO Audit Report No.24 2004–05 *Integrity of Medicare Enrolment Data* identified customers enrolled more than once in Medicare, which the department was aware of and was working to resolve.[63] While recognising the difficulty in verifying the duplicate records, the ANAO estimated the number of possible

63 ANAO Audit Report No.24 2004–05 *Integrity of Medicare Enrolment Data*, p. 40.

duplicate enrolments to be hundreds of individuals rather than thousands of individuals.

3.13 Recommendation No. 3 of the 2004–05 audit report was that the department:

- produce a report on possible duplicate enrolments, employing the data matching criteria envisaged for use with the Consumer Directory; and
- resolve as many duplicate Medicare enrolments as possible, before the Consumer Directory is fully implemented.[64]

3.14 At the time of the 2004–05 audit, the department was introducing the Consumer Directory to replace its existing customer record database—the Medicare Enrolment File. It agreed to this recommendation, responding that a new duplicate record reporting system had been designed based on the CDMS customer matching criteria.

3.15 Human Services advised the ANAO that this recommendation had been implemented but this could not be demonstrated. The department has a process in place for detecting and resolving duplicate enrolments (refer to paragraphs 3.21 to 3.22), which the ANAO examined.

Duplicate PIN Resolution project

3.16 Following the introduction of IHIs in mid–2010, Human Services undertook a data cleansing exercise to identify duplicate Medicare customer enrolments. This recognised the risk that if both enrolments were active and the customer requested a Personally Controlled Electronic Health Record, their clinical data would be incomplete as it would only reflect the data recorded on one record. This situation presented a clinical safety risk for the customer and a reputational risk for Human Services.

3.17 Human Services implemented a project in 2010–11 which identified and resolved 10 553 duplicate records.[65] Subsequently, in July 2011, Human Services established a Duplicate PIN working group to consider ways to prevent duplicate enrolments; correctly resolve duplicates in a timely manner;

64 ibid., p. 16.

65 This was equivalent to 5252 matches. A customer can be enrolled more than twice and have three or more records. Consequently, there were an uneven number of duplicate records.

identify and resolve intertwined records[66]; and provide accurate and timely data to the Human Services Executive about duplicate enrolments.

3.18 The working group submitted a 'Quick Wins' proposal relating to refining the customer enrolment search and introducing an additional warning message for the enrolment of customers over the age of 12 months as most customers born in Australia will have already been enrolled by this age.

3.19 The working group also prepared a report outlining its analysis and made 24 recommendations for short, medium and long term implementation.[67] Human Services advised the ANAO in November 2013 that it implemented 15 of the 24 recommendations and determined some recommendations were not able to be implemented due to resource constraints.

3.20 One of the recommendations was that a specialist team be established, on an ongoing basis, consisting of three full–time equivalent positions. Two of these positions were to be responsible for investigating possible duplicate enrolments, resolving them and providing feedback to customer service officers. The third position was to have responsibility for identifying the underlying causes of duplicate enrolments, making recommendations to Human Services management about improvements to prevent duplicate enrolments and identifying the training needs of customer service officers and improvements for guidance material.

3.21 In response, Human Services established a small team of staff to identify and resolve duplicate enrolments and provide feedback to customer service officers who have enrolled a customer more than once. In 2012–13, this team investigated an average of 95 possible duplicates each week and confirmed a total of 911 duplicate records for the financial year (approximately 76 per month).

3.22 The work of the team has strengthened Human Services' processes to identify duplicate enrolments. However, the department advised that the volume of work associated with identifying and resolving duplicate records limits the team's capacity to undertake broader work regarding these types of records, including identifying underlying causes and recommending actions to

66 Intertwined records are records which are shared by two customers (refer to paragraphs 3.33 to 3.40).

67 The report made 26 recommendations, however, two were similar and one could not be implemented as it was that IHIs should not be suppressed when resolving an intertwined record, and this is incorrect.

the Human Services Executive to address these causes. The department also advised that it has taken action to increase awareness among customer service officers regarding the impact of duplicate enrolments. An ongoing focus on identifying 'upstream' measures to prevent duplicate enrolments would deliver additional benefit to Human Services by reducing the 'downstream' workload associated with resolving duplicates and consequently, improving the efficiency of its operations.

ANAO testing for duplicate enrolments

3.23 The ANAO conducted a number of tests of Human Services' Medicare customer records to identify possible duplicate enrolments. Duplicate enrolments compromise both the integrity of the system of unique customer reference numbers[68], and the integrity of customer records.[69]

3.24 Duplicate enrolments can be difficult to detect as testing can result in 'false positives'. False positives are records which appear to be a duplicate enrolment, but which on closer inspection, relate to different customers. The ANAO conducted a series of tests aimed at progressively eliminating false positives by applying more stringent matching criteria.

3.25 The ANAO also tested for possible duplicate enrolments where the customer was recorded as deceased on one record and where there were claims on the second record. The ANAO could not determine whether these claims had been subsequent to the customer's recorded date of death. These matches demonstrate the risks associated with duplicate enrolments that one record could be used for fraudulent claiming or identity theft purposes.

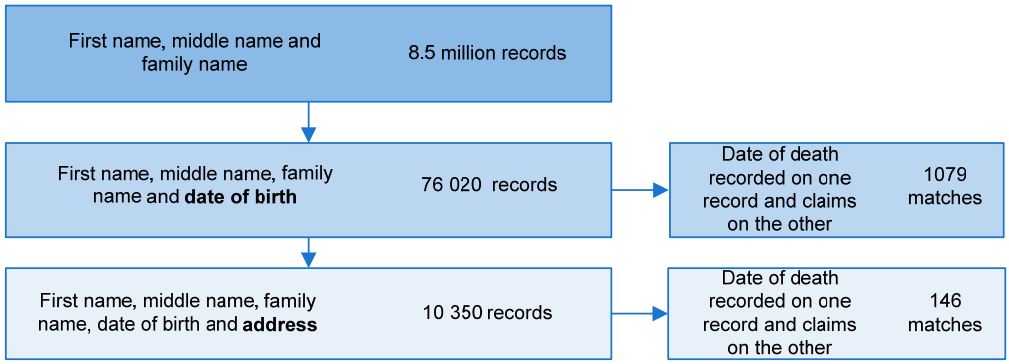
3.26 The ANAO's testing identified 8.5 million records which matched on first name, middle name and family name. Most of these possible duplicates will be false positives because many people share the same name.

3.27 As shown in Figure 3.2, by including date of birth to the name match test, the number of possible duplicates reduced to 76 020 records. When address was added to the matching criteria, the ANAO identified 10 350 possible duplicates.

68 As affected customers have more than one Consumer ID, PIN and IHI.

69 Customer health information may be fragmented across more than one record compromising its integrity and reliability.

Figure 3.2: Name matching criteria and number of matched records



Source: ANAO analysis.

3.28 The ANAO undertook further testing of Medicare customer records, focussing on records which matched on customers' initials and different dates of birth and gender, as outlined in Table 3.2. The results of these tests demonstrate the risk that if customer information is incorrectly or incompletely recorded, the effectiveness of the customer search undertaken by staff at the enrolment stage can be compromised—resulting in a duplicate enrolment.

Table 3.2: Results of ANAO's data integrity testing

Testing	ANAO findings
First and middle name initials, family name, date of birth and address.	The ANAO identified between approximately 28 000 and 43 600 possible duplicate records which matched on customers' first and middle initials, family name, dates of birth and addresses.[1] Almost 20 000 possible duplicate records matched on first name initial, family name, date of birth and address but had different middle initials recorded.[2]
First and middle names, family name and addresse with different birth days, months and years.	The ANAO's tests identified thousands of possible duplicate records which matched on customers' names and addresses but which had different dates of birth recorded.
First name, middle name, family name, date of birth and address but different genders.	The ANAO identified between 800 and almost 4000 possible duplicate records which matched on customers' names, date of birth and address but had different genders recorded on each record.

Source: ANAO analysis.

Note 1: In total, 47 821 records were identified in this test, however, 4238 of these records had an affirmative multiple birth indicator indicating they were a twin etc. Human Services advised that this indicator was introduced in 2006 and consequently, some of the 43 600 records may also be for twins etc.

Note 2: This includes where an initial was recorded on one record and not the other record.

3.29 For these tests, some of the matched records were for different customers, including matches which appeared to be twins or parents and children. However, some of these records appeared to be for the same customer, including records where the customers' names had been inconsistently recorded and customers' dates of birth or gender had been incorrectly recorded.

3.30 At least 18 194 records (or 8797 matches) had one active record and one inactive record, indicating that they were likely duplicate enrolments. In a database containing almost 30 million records, the number of possible duplicates identified by the ANAO is not significant. However, these records do represent a risk to the integrity of Medicare.

3.31 Duplicate customer records fragment data across two records presenting a potential clinical safety risk. Further, the possible duplicate enrolments where customers were recorded as deceased on one record and there were claims on the second record highlight the potential risks of fraudulent claiming and identity theft.

3.32 The possible duplicate records, identified by the ANAO, had incomplete, incorrect and inconsistently recorded customer data. Records with incorrect or incomplete data can lead to the creation of a duplicate enrolment. Enhancing its customer enrolment search criteria to recognise customer records with variations to a customer's name, date of birth and gender details, would improve Human Services' capacity to identify existing customer enrolments and consequently, prevent duplicate enrolments. Further, requiring customers' names to be recorded in full would assist to accurately identify existing customer enrolments.

Intertwined customer records

3.33 A further risk to the integrity of Medicare customer data arises from intertwined records. These are records shared by two different customers. This means that they share the same Consumer ID, PIN, and IHI, and their health data is stored on the same record.

3.34 Intertwined records are created when customer services officers incorrectly enable two customers to use the same PIN. This can occur for two existing customers but most commonly occurs during the customer enrolment process. For example, if the customer service officer selects another customer's record from the enrolment search results and updates it with the personal

details of the customer they are enrolling, both customers will share that record.

3.35 These records represent a clinical safety risk to customers as their recorded health data is combined with the health data of another customer. It also represents a privacy risk if one of the customers views their personal and/or health data, including claiming history, through a Medicare Online Services account, Personally Controlled Electronic Health Record, Medicare Express Plus mobile phone application account or by requesting a copy of their claims data from Human Services.

3.36 Intertwined records are difficult to identify and to date, have been brought to Human Services' attention by customer queries. For example, Human Services identified one intertwined record for two children after the parent of one of the children received an immunisation certificate for the other child and contacted Human Services. Human Services advised that it has recorded 34 intertwined records since 2011–12, when it commenced recording identified instances.

3.37 These records are difficult to resolve. To mitigate the potential privacy and clinical safety risks when resolving these records, a number of actions need to be undertaken. While assurance has been provided within Human Services that guidelines on resolving these types of records were developed and implemented, as yet no guidance or procedures have been put in place. This creates a risk that the necessary steps are not taken when resolving intertwined records.

3.38 The development and implementation of appropriate guidelines would provide assurance that intertwined records are being addressed in a consistent manner so as to mitigate the privacy and clinical safety risks associated with these records.

3.39 While it is necessary to resolve intertwined records, it is also desirable to prevent them. Intertwined records result from human error: either because they have been incorrectly resolved as duplicate enrolments or because one customer is enrolled on another customer's record. Human Services has a review process for resolving possible duplicate records aimed at preventing intertwined records. However, it has not implemented any specific measures aimed at preventing the creation of intertwined records when customers are first enrolled.

3.40 Human Services advised that it established an Intertwined Records Working Group in February 2014, during the course of the audit, with representation from relevant business areas. The group will look at the cause of intertwined records; ways of identifying these records; and standardised processes for resolution.

Conclusion

3.41 The integrity of Medicare customer data is underpinned by unique reference numbers intended to identify individual customers, and a unique customer record containing accurate and complete customer information.

3.42 The ANAO's testing showed that there is a high level of integrity with Medicare's unique customer reference numbers. Only one number, a Medicare Reference Number, was shared by two records. However, the ANAO identified thousands of possible duplicate records—some of which are likely to be duplicate enrolments. These customers have more than one Consumer ID, PIN and IHI. Further, their health information may be fragmented across different customer records, compromising its integrity and reliability. While the number of possible duplicate records identified by the ANAO is not significant when compared to the large number of customer records held in the Consumer Directory, these records nonetheless compromise the integrity of the department's Medicare customer data holdings.

3.43 Intertwined records are also a data integrity issue. Affected customers have the same Consumer ID, PIN, and IHI and these records give rise to privacy and clinical safety risks. While Human Services has taken some action to prevent the creation of these types of records, it could do more. The department should introduce guidelines to address intertwined records, which could form part of the work being undertaken by the department's Intertwined Records Working Group.

Recommendation No.2

3.44 To better manage duplicate and intertwined records and improve the integrity of its customer data, the ANAO recommends that Human Services:

- consider ways to better identify duplicate customer enrolments;
- investigate the underlying causes of duplicate enrolments with a view to informing approaches to their prevention; and
- develop and implement guidelines for resolving intertwined records.

Agency response:

3.45 *The department agrees with this recommendation.*

3.46 *The department commenced a programme of work to address intertwined records in early 2014. This work will build on existing automated reports that identify possible duplicate records, and includes:*

- *undertaking a comprehensive analysis of the Consumer Directory to identify and analyse the extent of intertwined records by June 2014;*
- *cleansing the Consumer Directory of any intertwined records identified by September 2014;*
- *reviewing customer service procedures for core functions which are identified as risk points for the creation of intertwined records by October 2014; and*
- *establishing an escalation framework to capture intertwined records at the time of creation to allow for prompt corrective action, by December 2014.*

4. Integrity of Customer Data

This chapter examines the integrity of Medicare customer data stored in the Consumer Directory, focussing on the input controls applied by Human Services to ensure information is recorded accurately.

Introduction

4.1 The collection of accurate, complete and reliable data supports the effective enrolment of eligible customers in Medicare and ensures their access to Medicare benefits is consistent with their entitlement. There are mandatory personal and eligibility customer data fields in the Consumer Directory, which customer service officers are required to complete when adding or amending information.

4.2 These fields can assist to determine a customer's eligibility for enrolment as well as their ongoing entitlement to Medicare benefits. The ANAO tested these fields for completeness, accuracy and reliability.

Personal customer data

4.3 For personal customer data fields, the ANAO tested the names, dates of birth and death, gender and address fields.

Names

4.4 There are three name fields: first name, middle name and family name. First name and family name are mandatory fields, unless the 'only name' indicator is selected for the customer. According to the Consumer Directory system specifications, for customers who have only one name, it should be recorded in the family name field and the 'only name' indicator should be selected. The ANAO tested all 29.3 million Medicare customer records[70] and found one customer who did not have a family name recorded, which contravenes the system specifications.[71] The ANAO identified 23 979 records which did not have a first name or middle name recorded. This is consistent with the process for recording one name.

70 That existed as at 16 September 2013.

71 This customer did have a first name recorded and no claims recorded on their record.

4.5 The ANAO also identified 86 records which had a first and/or middle name recorded and had text in the family name field which said 'no name' or 'only name'. This suggests some customer service officers may not understand the process for recording a name for customers with only one name. Human Services' guidance for registering a customer with one name does not instruct customer service officers to record that name in the family name field or to select the 'only name' indicator. Human Services could benefit from reviewing its guidance on recording one name.

4.6 Recording customers' first and middle names in full can assist in preventing duplicate enrolments as it allows the accurate identification of customers. The ANAO tested 29.3 million Medicare customer records for initials recorded in name fields and found:

- 2554 records had one character recorded in the first name field;
- 16 014 910 records with one character recorded in the middle name field. Eighteen of these records had a number recorded and two had a hyphen recorded; and
- 679 records had one character recorded in the family name field, of which one record had a zero recorded.[72]

4.7 Human Services does not have guidance instructing customer service officers to record customers' first and middle names in full or record customers' middle names, if they have one. Human Services would benefit from recording customers' full names to assist with preventing duplicate enrolments and improve the integrity of Medicare customer data.

4.8 The ANAO identified approximately 800 records with 'Baby' or a variation of 'Baby', for example 'Baby 1', recorded as the customer's first name. Human Services advised that 'Baby' can be a legitimate name. Nevertheless, those records which have 'Baby' recorded instead of 'Newborn' are inconsistent with Human Services' guidance, 'Enrolment of a child', which states that for newborn children who have not been named, customer service officers should record 'Newborn' in the first name field. To improve customer

72 According to the system specifications for the Consumer Directory, the first name, middle name and family name fields can have alpha and numeric characters recorded. They can also have an apostrophe and hyphen recorded but no other type of symbol should be recorded in these fields.

service officers' understanding of this requirement, this instruction should also be included in the guidance on enrolling a newborn child.[73]

Date of birth

4.9 Date of birth is a mandatory field in the Consumer Directory. The ANAO tested the Medicare customer records for dates of birth and found that every customer had a date of birth recorded and all dates of birth were recorded in the correct format (DDMMYYYY).

4.10 The ANAO also tested the date of birth field for logical relationships with other recorded dates. The testing identified 1539 customers who had an enrolment date prior to their date of birth. According to the system specifications for the Consumer Directory, there are controls for the date of birth field, including that it must be numeric, it must be a valid calendar date and it cannot be in the future. Consistent with the system specifications, the ANAO did not identify any customer records with a date of birth in the future. Human Services could also consider introducing a control to prevent dates of entitlement being recorded before dates of birth.

4.11 The ANAO identified 25 customers with a date of birth prior to 1870.[74] Twenty of these records do not have a date of death recorded. These customers would be approximately 143 years old. While 24 of these records did not have a claims history, one of these records had a last claim date in 2013. Human Services' investigation of this record showed that the affected customer's date of birth had been incorrectly recorded and the department advised the ANAO that it has subsequently corrected the record.

4.12 Effective data cleansing can identify and rectify erroneous data. In ANAO Audit Report No.24 2004–05 *Integrity of Medicare Enrolment Data*, the ANAO made a number of recommendations in relation to the migration of customer data from the Medicare Enrolment File to the Consumer Directory. Included was a recommendation regarding the 'Medicare Enrolment Data

73 This guidance is: 'Add a person to an existing card (including a Newborn)'; 'Register a Newborn or Person to an Existing Card'; 'Newborn enrolment'; 'Newborn child enrolment enquiries'; and 'Newborn child enrolments'. Human Services advised that it intends to consolidate reference and guidance material including the guidance material for newborns.

74 Only two of these records had an active enrolment; that is, they had no end date recorded for eligibility or Medicare enrolment and did not have an expired Medicare card.

Field Assessment Report: Recommendations for Data Cleansing' (August 2002) (the Data Cleansing Report).[75]

4.13 The Data Cleansing Report made 14 recommendations in relation to data cleansing activities to be undertaken before the migration of data as well as providing guidance on the process for the data migration.

4.14 In its 2004–05 report, the ANAO observed that Human Services had not implemented all of the 14 recommendations from the Data Cleansing Report and recommended that Human Services:

- fully implement the data cleansing recommendations contained in its review, 'Medicare Enrolment Data Field Assessment Report: Recommendations for Data Cleansing'; and
- conduct a contemporary data field assessment to identify any records generated between 2002 and 2004, that require cleansing.[76]

4.15 Human Services advised the ANAO that it had implemented the recommendation included in the 2004–05 audit report. The ANAO's analysis of customers' date of birth data found 1539 records with enrolment dates prior to the customers' dates of birth. In its 2004–05 audit report, the ANAO identified 2093 records of this nature. While not definitive as there may be other causes for the reduction in number of these records, the ANAO's testing suggests that that Human Services has corrected a number of these records. This, however, does not demonstrate effective implementation of the recommendation. Human Services can continue to improve the accuracy and integrity of Medicare customer data by implementing controls to prevent illogical relationships between dates and reviewing records to identify inactive records and those with unusual activity.

Date of death

4.16 The ANAO undertook a number of logic tests on the date of death fields. According to the Australian Bureau of Statistics, in 2012 the average life

75 In preparation for the migration of customer data to the Consumer Directory, Human Services analysed the data in the Medicare Enrolment File and identified data quality issues including that the data: did not meet current or future business rules; had been corrupted with spurious values; and contained illogical relationships between some dates, for example some customers' enrolment start dates were before their birth dates. These results were outlined in the Data Cleansing Report.

76 ANAO Audit Report No.24 2004–05 *Integrity of Medicare Enrolment Data,* p. 16, Recommendation No. 1.

expectancy for a male and a female at birth was 79.9 years and 84.3 years, respectively.[77] The ANAO identified 936 245 customers over the age of 85 years old, including 1295 customers over the age of 100 years old, who had claimed in the six months prior to the testing and who did not have a date of death recorded. Of the 936 245 records, 40 541 did not have a claim recorded in the 12 months prior to testing and did not have a date of death recorded.[78]

4.17 Some of the customer records without a recent claim may be for customers who are deceased. If that is the case, these records could be at risk of being used for fraudulent claiming activities or false identity purposes. Human Services introduced its automated FODD file matching[79] in response to a recommendation made in the ANAO's 2004–05 performance audit report. However, it may be necessary to supplement this process by testing records for inactivity on a risk basis, to identify records which require deactivation.[80]

4.18 The ANAO also identified 12 835 records with recorded claims after the customer's date of death. Of these records, 75 per cent had claims within one to ten days of the customer's date of death and another 18 per cent had claims within ten to 100 days. Claims can be lodged up to two years after a customer's date of death by the customer's agent, for example, their partner or a person with a power of attorney, for the treatment of the customer prior to their death. A claimant can apply to the Minister to seek a longer period to lodge a claim.

4.19 The remaining seven per cent of these 12 835 records (835 records) had claims 100 days or more after the customer's death, including 446 records with claims lodged two or more years after the customer's date of death. Some of these records had the same date of birth and death recorded and consequently, had significant lengths of time between the customer's recorded date of death and last claim—the lengthiest being 102.5 years. Human Services reviewed the five records with the lengthiest periods between customers' dates of death and last claims and found that the dates of death had been erroneously recorded,

77 Australian Bureau of Statistics, *1.1 DEATHS, Selected summary statistics — 2002, 2011 and 2012* [Internet], ABS, available from <http://www.abs.gov.au/ausstats/abs@.nsf/mf/3302.0> [accessed November 2013].

78 Of these 40 541 records, 17 053 did not have a claim recorded in the 12 to 24 months prior to testing; 10 165 did not a have a claim in the 24 to 36 months prior to testing; 7082 did not have a claim in the 36 to 48 months prior to testing; and, 6241 did not have a claim in over 48 months prior to testing.

79 This process automatically updates customer records in the Consumer Directory with dates of death provided by the state and territory registries of births, deaths and marriages.

80 ANAO Audit Report No.24 2004–05 *Integrity of Medicare Enrolment Data,* p. 17, Recommendation No. 5.

but since the ANAO's data extract (taken in September 2013), three of the five records had been corrected through FODD data matching. Human Services advised that it is reviewing its guidance for recording customers' dates of death to provide greater consistency.

Gender and address

4.20 The ANAO tested the mandatory gender field of Medicare customer records and found all customer records have a gender recorded. The system specifications provide for only two values in the gender field: 'M' for male and 'F' for female. All customer records complied with this specification.[81]

4.21 Address fields, except the country field, are mandatory fields. The ANAO identified records that had incomplete address fields, including:

- 7147 records without a street number or street name recorded;
- 78 records without a value entered in the state field; and
- six records without an entry in the postcode field.

4.22 Human Services advised that not all addresses include a street number or name, for example addresses in some remote Indigenous communities. Nevertheless, those records without a state or postcode recorded are inconsistent with the system specifications.

4.23 The ANAO's analysis of Medicare customer records found 634 858 customers who are flagged as having returned mail from their recorded addresses; of whom, 335 588 had returned Medicare cards.[82] Of these 634 858 customers, 475 133 had made a claim in the six months prior to September 2013 indicating they were active customers without an up–to–date address; of whom, 268 776 had returned Medicare cards.

4.24 An up–to–date address is mandatory data when enrolling in Medicare. Returned mail is an indication that Medicare customer personal information is inaccurate or not up–to–date. Human Services advised that there is no process

81 The ANAO identified seven records which had 'U' (unknown) recorded in the gender field. Human Services' investigation of these records found that this discrepancy was due to the timing of the data extracts for the ANAO's testing and these records contained a correct data value in the Consumer Directory.

82 More than one customer can have the same address, for example families will share a common address. There are 634 858 customers linked with the 423 200 unique addresses flagged as having returned mail.

in place to follow–up and update addresses of Medicare customers who have returned mail.

4.25 There is a risk of inappropriate use of Medicare cards when they are mailed to invalid customer addresses. To reduce that risk and improve the overall efficiency of re–issuing Medicare cards, Human Services could consider the benefits of a more active approach to following up returned mail. This could include a process where customer addresses with returned mail are checked using other available contact details for customers, including phone numbers and email contact details. Further, Human Services could consider other government entities' processes to keep address records up–to–date.[83] Such a process would need to balance the costs of its introduction with the costs and risks associated with invalid addresses.

Accuracy and completeness of personal customer data

4.26 The ANAO identified a very small number of records which were inconsistent with the Consumer Directory system specifications, for example, one record which did not have a family name recorded and records which had incomplete addresses. Some of these records may be the result of Human Services' approach to migrating the customer data from the Medicare Enrolment File to the Consumer Directory.

4.27 In the Medicare Enrolment File, when consumers had more than one Medicare card, their data was recorded more than once. Human Services identified that this led to disparities between the data recorded for each card, for example, different genders or dates of birth recorded for the same customer. In the Consumer Directory, customer data is recorded once. To facilitate the migration of customer data from the Medicare Enrolment File to the Consumer Directory, Human Services developed an approach, known as the representative member segment, to identify the most correct customer data and to consolidate it into one record.

4.28 In the 2004–05 audit report, the ANAO identified risks with this approach; in particular, that incorrect data recorded about the customer may be migrated to the Consumer Directory, such as an incorrectly recorded gender

83 For example, Australia Post has a service which allows individuals to notify organisations of a new address when they move permanently. This service requires an organisation to have an agreement with Australia Post for this notification to occur. The Australian Electoral Commission has such an agreement with Australia Post.

or date of birth. Further, the representative member segment approach did not include any logic checking of dates to provide assurance that the correct dates were being migrated. For example, that the customer's birth date was before their Medicare enrolment date.

4.29 The 2004–05 audit addressed this issue by recommending that Human Services conduct a review of the effectiveness of the 'representative member segment' approach to consolidating Medicare enrolment data, by selecting a representative sample of such records and manually assessing the accuracy and validity of the consolidated records.[84]

4.30 Human Services advised the ANAO that it had implemented this recommendation. However, in the current audit, the ANAO observed that the representative member segment rules applied by Human Services to migrate the data to the Consumer Directory were not different from those analysed by the ANAO during the previous audit, indicating that Human Services had not varied its planned approach. The ANAO's findings did not support Human Services' advice that the ANAO's previous recommendation had been implemented effectively.

4.31 Human Services advised that it does not test recorded Medicare customer data for completeness, accuracy or reliability. In addition to the records identified which were inconsistent with the system specifications and Human Services processes, the ANAO's testing found records which were inactive or had unusual activity. For example, the ANAO identified 40 541 records of customers over the age of 85 years without a recent claim, including 20 records with a date of birth recorded prior to 1870. It also identified a record with a date of birth prior to 1870 with a recent claim.

4.32 Data integrity testing can help Human Services identify and close records, where appropriate. Testing can take a number of forms, such as a regular program, a periodic program or a program of spot tests. An appropriate process would assist Human Services mitigate the risks of records being used by ineligible persons to claim Medicare benefits or fraudulently used for claiming or identity purposes.

84 ANAO Audit Report No.24 2004–05 *Integrity of Medicare Enrolment Data,* p. 43, Recommendation No. 4.

Recommendation No.3

4.33 To further improve the completeness, accuracy and reliability of Medicare customer data, the ANAO recommends that Human Services undertake targeted, risk-based data integrity testing of Medicare customer records.

Agency response:

4.34 *The department agrees with this recommendation.*

4.35 *The department currently has a comprehensive programme of monitoring customer claiming activities using a variety of mechanisms. This includes a data mining system that monitors and analyses customer claiming to identify unusual claims activity and a programme of payment accuracy review. The department will further enhance and strengthen this programme by commencing targeted testing of Medicare customer data by 1 July 2014.*

Accuracy of customer eligibility documentation

4.36 Prior to the introduction of the Consumer Directory, eligibility documentation was not recorded in the Medicare Enrolment File. Now, the Medicare Entitlement Business Rules require customer service officers to record at least one acceptable eligibility document.

4.37 There are 20 records for customers who were enrolled without eligibility documentation recorded after it was compulsory for customer services officers to use the Consumer Directory.[85] These records contravene the Medicare Entitlement Business Rules which require an eligibility document to be recorded for a customer enrolment and indicate the Consumer Directory system controls need to be enhanced.

4.38 The ANAO identified 4 359 129 records associated with 5 543 817 eligibility documents recorded. When recording customers' eligibility documentation, customer service officers are required to select the type of document being recorded from a drop–down list and then record either the document number or date, depending on the document type. For example,

85 This was on 9 September 2006. The ANAO's testing identified 58 records without eligibility documentation recorded. However, Human Services' investigation of these records confirmed that 38 of them had eligibility documentation recorded in the Consumer Directory. It was determined through joint investigation that due to the timing of these customers' enrolments, their records in the ANAO's data extract did not have eligibility documentation recorded.

Human Services guidance states that the document number should be recorded for birth certificates and extracts, passports and travel documents.[86] For other types of documents, the date should be recorded, for example, citizenship papers or naturalisation certificates.

4.39 The fields for recording the document number and the document date are mandatory free text fields for eligibility documents. The ANAO's testing did not identify any records with an eligibility document of 'passport', 'birth certificate' or 'birth extract' which had a blank reference number field indicating that the Consumer Directory controls are effective in this area.

4.40 There are, however, data quality issues with some of the records that have an eligibility document recorded. In particular, the ANAO found records that contravened the Medicare Entitlement Business Rules, including free text entries that:

- emulated the eligibility document, for example, 2123 records with 'passport' as the eligibility document, which then have the word 'passport' recorded in the reference number field;
- described the eligibility documents, for example, 4012 records with 'proof of birth' recorded in the reference number field;
- did not align with the text entry, for example, text recorded for the eligibility document 'passport' included 'lease', 'school letter', 'stat dec' and 'student'; or
- were a single number, letter or symbol, for example, there were 675 records with 'passport' recorded as the eligibility document with this type of corresponding text.

4.41 For some eligibility document types, it is likely to be unclear to customer service officers what data they are required to record. There are 23 entries which can be selected from the drop–down list of eligibility documents and the guidance available only provides instructions on recording 12 documents. Human Services should consider reviewing this guidance. There is also scope for Human Services to reinforce existing requirements for recording eligibility documents, to improve the quality of data recorded.

86 The Medicare Entitlement Business Rules state that reference numbers should also be recorded for identity documents and adoption papers.

Completeness of customer eligibility data

4.42 The ANAO examined Medicare customer records to confirm that the eligibility documentation and entitlement period recorded for customers was in accordance with their eligibility type.

Permanent resident visa holders

4.43 Permanent resident visa holders are recorded as 'Migrants' in the Consumer Directory. To enrol in Medicare, they are required to provide a current passport, and valid visa or an original visa grant letter. The ANAO tested the eligibility documentation recorded for permanent resident visa holders.

4.44 The ANAO identified 1.5 million records of permanent resident visa holders which had one or more eligibility documents recorded; of which, at least one document was a passport, visa or visa grant letter, as required for enrolment. The ANAO also identified 34 129 records which had one document recorded, however, was not one of the three documents required by permanent resident visa holders to enrol in Medicare. Consequently, the 34 129 records do not reflect whether these customers have provided the necessary documentation to support their enrolment.

Permanent resident visa applicants

4.45 To enrol in Medicare, permanent resident visa applicants ('Conditional migrants') are required to provide:

- a current passport or travel document;
- a valid visa or original visa grant letter; and
- evidence of relationship with a spouse, parent or child who is an Australian citizen or permanent visa holder, where necessary.[87]

4.46 The ANAO identified 157 809 of 336 558 records of permanent resident visa applicants, with at least one eligibility document recorded. Of these records, 155 620 had one or more of the required eligibility documents and 2189 records did not have any of these documents recorded. It is not possible

87 Holders of visa subclasses 309 (Partner–Provisional) and 310 (Interdependency–Provisional) are only required to provide their passport and visa. Applicants of parent visas are not entitled to Medicare.

to determine from these 2189 records whether the customers provided the appropriate eligibility documentation to support their enrolment.

4.47 While their permanent resident visa application is being considered, these customers are enrolled for 12 month periods for up to three years after which time they can be enrolled for two consecutive six month periods.[88] The ANAO identified 315 897 'Conditional migrant' records, of which 15 703 had a Medicare card expiring more than 12 months after the date of ANAO testing.

4.48 The ANAO also identified 1129 'Conditional migrant' records which did not have an end date recorded on their record. These customers may be accessing Medicare benefits without an entitlement.

Visitors from Reciprocal Health Care Agreement countries

4.49 Visitors from ten countries can access Medicare benefits through Reciprocal Health Care Agreement arrangements.[89] The ANAO tested the Medicare customer records to confirm that visitors, registered for Medicare, were from these ten countries. Out of 286 355 customer records for visitors, the ANAO identified two customer records where the customers were not from one of these ten countries.

4.50 Visitors are entitled to Medicare benefits for a limited period of time—usually the period of their visa. The ANAO tested customer records with a visitor entitlement type for an end date and identified 2743 records with no end date recorded. Some of these customers may be accessing Medicare benefits without an entitlement.

4.51 Visitors from Italy and Malta are only entitled to Medicare benefits for six months following their arrival in Australia. Of the 2743 records, 101 were visitors from Italy and 16 were for visitors from Malta. The ANAO identified 1331 records for visitors from Italy and Malta with entitlement periods which were greater than six months, and there were claims for Medicare benefits on 311 of these records after the six month entitlement period. These customers may also be accessing Medicare benefits without an entitlement.

---

88 Human Services advised the ANAO that permanent resident visa applicants can remain eligible beyond this period if they have lodged an appeal in relation to a decision to reject their application for a permanent resident visa. The ANAO identified 10 815 records for customers who had been enrolled in Medicare for more than four years, of which 1005 customers had been enrolled for more than six years.

89 These countries are: Belgium, Finland, Netherlands, Ireland, Italy, Malta, Norway, Sweden, United Kingdom and Slovenia.

4.52 Visitors from New Zealand and Ireland are not entitled to enrol in Medicare. However, they can access services as a public patient in a public hospital for medically necessary treatment and purchase prescription medicines which are subsidised under the Pharmaceutical Benefit Scheme at the general rate.

4.53 'RHCA New Zealand' is an entitlement type in the Consumer Directory as prior to 1 September 1999, when a new agreement was introduced, visitors from New Zealand could enrol in Medicare. However, the ANAO identified 325 visitors from New Zealand who were enrolled after this date.

4.54 Of the 61 614 records with an entitlement of 'RHCA New Zealand', the ANAO identified 1142 records which did not have an end date recorded. Of the records without an end date, 52 had claims post 1 September 1999; 31 had claims in 2013, ten had claims in 2012; and 11 had claims between 2008 and 2011. These customers are not entitled to claim Medicare benefits. Further, if these claims are for out–of–hospital treatment, they are not covered by the agreement. Testing of claims data was outside the scope of this audit.

4.55 Human Services had several opportunities to implement controls to prevent customers being enrolled using the entitlement type, 'RHCA New Zealand', including when it became an ineligible entitlement type and when migrating the customer data from the Medicare Enrolment File to the Consumer Directory. Due to Human Services' lack of action in this area, customers are lodging claims under an entitlement type which has been invalid for more than ten years.

Other limited entitlement types

4.56 As outlined in Table 4.1, there are other entitlement types which have limited or no access to Medicare benefits in addition to visitors and permanent resident visa applicants, including:

- Expired entitlement types: these were legitimate entitlement types which have been discontinued. The discontinuation date for these entitlement types varies from 31 December 1993 to 4 February 2002.
- Limited entitlement types: these are valid entitlement types for a limited period of time. The claims made by the customers with these entitlement types may be within their entitlement period, however, without a recorded end date this cannot be determined.

- No entitlement types: there are two entitlement types which were established to register customers but not enrol them. There is no entitlement to Medicare benefits associated with these entitlement types.
- Unknown entitlement type: when records were migrated to the Consumer Directory, those customers associated with a Ministerial Order were assigned the entitlement type of 'Ministerial Order (Migrated from Medicare Enrolment File)' as the Medicare Enrolment File did not record specific Ministerial Order types. It is not known whether these customers have a valid entitlement to Medicare benefits.

Table 4.1: Records with limited access entitlement types with no end date recorded

Entitlement type	Total no. of records	No. of records with no end date recorded	No. of records with a claim made in 2013	No. of records with a claim date after entitlement period
Expired entitlement types	35 488	394	77	93
Limited entitlement types	32 665	57	16	Unknown[1]
No entitlement	13 882	13 789	8	10
Unknown (Ministerial order (Migrated from Medicare Enrolment File))	506	37	18	Unknown[1]

Source: ANAO analysis.

Note 1: The associated claims with these records may be within the customers' entitlement periods, however, as no end dates are recorded, this is unknown.

4.57 Some of these entitlement types were determined to be ineligible for Medicare benefits a number of years earlier, however, as some of these records do not have end dates recorded, these customers have been able to continue accessing Medicare benefits.

4.58 When customer data was migrated from the Medicare Enrolment File to the Consumer Directory, data integrity issues were identified. These issues were reported to relevant program areas for resolution. However, the ANAO's 2004–05 performance audit found that there was evidence these issues had not been addressed.

4.59 At that time, the ANAO acknowledged that not all data quality issues could have been resolved prior to the migration. However, it identified areas

which could have been improved, including correcting consumer entitlement types and entitlement periods. The ANAO noted that the migration of customer data had provided the opportunity for Human Services to identify and address data quality issues, but this opportunity had not been realised. To support the migration of accurate customer data to the Consumer Directory, the ANAO recommended that Human Services:

- reconsider enforcing all CDMS business rules during the data migration; and
- consider the risks of commencing the new system with incorrect data, against the associated costs and benefits of enforcing all business rules before the changeover from the Medicare Enrolment File to the Consumer Directory.[90]

4.60 Human Services advised the ANAO that this recommendation had been implemented, however, the records identified in Table 4.1 indicate that the department did not implement the ANAO's recommendation. While these records were determined to be ineligible entitlement types prior to the migration of customer data to the Consumer Directory, Human Services did not take the opportunity to correct these records and they were subsequently migrated without addressing known data quality issues.

Conclusion

4.61 The ANAO's analysis of Medicare customer records has identified integrity issues with customer data. In particular, the ANAO identified instances where:

- data is inconsistently, inaccurately and incompletely recorded; and
- mandatory data fields are incomplete.

4.62 Of greatest concern are the active records for customers with no entitlement to Medicare benefits. For example, those customers whose entitlement has ended or who were never entitled to Medicare but who are currently claiming benefits. These records indicate that Human Services requires more effective system controls.

90 ANAO Audit Report No.24 2004–05 *Integrity of Medicare Enrolment Data*, p. 16, Recommendation No. 2.

4.63 The ANAO also identified records without sufficient information recorded about eligibility documentation to support customers' Medicare enrolments. Consequently, it cannot be determined whether these customers are eligible for Medicare. There would be benefit in Human Services emphasising the need for customer service officers to record eligibility documentation consistent with requirements.

4.64 The ANAO's testing indicated that Human Services did not implement the recommendations in the ANAO's 2004–05 performance audit aimed at improving the integrity of customer data prior to its migration to the Consumer Directory. Consequently, the issues identified ten years ago have persisted and continue to compromise the integrity of Medicare customer data. To the extent that agreed audit recommendations are not implemented in a timely manner, Human Services is foregoing opportunities to enhance its performance.[91] Implementation is facilitated by internal monitoring and reporting on progress, and an effective process for documenting the closure of recommendations.

4.65 In a database of almost 30 million records, the number of records affected by data integrity issues is not significant. Nevertheless, they indicate that there are system control weaknesses which represent a risk to the integrity of Medicare. The consequences of such issues can include people who are not entitled accessing Medicare benefits, which in turn has an impact on Australian Government expenditure.

91 ANAO Audit Report No.25 2012–13 *Defence's Implementation of Audit Recommendations*, p. 13 and 16 and ANAO Audit Report No.53 2012–13 *Agencies' Implementation of Performance Audit Recommendations*, p. 16.

Recommendation No.4

4.66 To ensure that only those customers eligible to receive Medicare benefits can access them, the ANAO recommends that Human Services review existing entitlement types and implement controls where relevant, to:

- prevent instances of customers being enrolled under invalid entitlement types and accessing Medicare benefits without an entitlement; and
- ensure mandatory data fields are completed, and that data entries are consistent with business and system rules.

Agency response:

4.67 *The department agrees with this recommendation.*

4.68 *The department has a range of checks and controls to prevent customers being enrolled under invalid entitlement types. These include system controls to verify entitlement types. Our review activity and strengthening of controls will be supported even further by the other recommendations in this report.*

5. Privacy of Customer Data

This chapter discusses Human Services' management of the privacy of Medicare customer data.

Introduction

5.1 Protecting the privacy of Medicare customers' personal information is a longstanding requirement for Human Services and is set out in legislation. To meet legislative requirements for the management of Medicare customer data, manage the risk to Human Services' reputation and provide assurance to Medicare customers, the department has put in place a range of policies and procedures.

5.2 To determine whether the department has met its privacy obligations in managing Medicare customer information, this chapter examines Human Services':

- privacy policies and procedures;
- compliance with legislative and policy requirements; and
- privacy training and awareness activities.

Privacy policies and procedures

Operational Privacy Policy

5.3 Human Services' 'Operational Privacy Policy' was endorsed by the Secretary on 15 January 2013 and sets out the privacy requirements for all staff.[92] It is a key element of Human Services' framework to meet its legislative responsibilities for Medicare customer privacy.

5.4 The 'Operational Privacy Policy' covers relevant requirements, sets out staff obligations and is accessible to Human Services staff through the intranet on a page that provides information and links to supporting material about

92 Staff includes ongoing or non–ongoing employees, contractors and consultants.

privacy.[93] Human Services has also introduced privacy policies that apply to Service Delivery Reform (SDR).[94]

Project–based Privacy Impact Assessments

5.5 Under the Human Services 'Operational Privacy Policy', new projects or proposals must undergo a Privacy Impact Assessment.[95] Although Privacy Impact Assessments are not required under the *Privacy Act 1988* they are used as a better practice assessment tool which outline the privacy implications of a project; help to minimise privacy risk and impacts; and allow Human Services to assess whether it is meeting its legal obligations.[96]

5.6 Human Services inconsistently applied its Privacy Impact Assessment requirement to three recent projects which impact on the privacy of Medicare customer data:

- 'Tell Us Once': provided a systematic assessment of the possible privacy impacts under the Privacy Act but it did not analyse the impact of the legislative secrecy provisions that apply to Medicare (refer to paragraphs 5.11 to 5.15) and did not indicate why these provisions did not apply or were not considered;
- Medicare Express Plus mobile phone application: did not have a Privacy Impact Assessment completed prior to its release[97]; and
- Document Verification Service[98]: had a Privacy Impact Assessment which considered the relevant privacy and secrecy provisions.

---

93 The departmental intranet page provides contact details, resources, eReference products, general data, references and links.

94 These policies include the Service Delivery Reform Privacy Framework, which was developed in consultation with the OAIC, and the Service Delivery Reform Privacy Consent Policy. The Service Delivery Reform Privacy Consent Policy includes a business process to ensure that a customer's consent is informed and that the customer understands the terms of the use and sharing of personal data.

95 The Department Secretary or Deputy Secretary can waive the requirement for a Privacy Impact Assessment.

96 Office of the Australian Information Commissioner, *Privacy Impact Assessment Guide Reviewed May 2010,* OAIC, available from <http://www.oaic.gov.au/privacy/privacy–resources/privacy–guides/privacy–impact–assessment–guide> [accessed 19 November 2013].

97 Human Services advised that a Privacy Impact Assessment was being undertaken which would review the current production of the Medicare Express Plus mobile phone application.

98 This service is being implemented at the request of the Council of Australian Governments (COAG). Driver's licenses, passports, citizenship certificates, visas, Medicare cards, as well as birth, marriage and change of name certificates are among the identity documents that can be verified. This system reduces the risk of a stolen identity being used and allows for real time checks of whether documents, such as Medicare cards as proof-of-identity documents, are accurate and up-to-date.

5.7 The Human Services Service Delivery Reform Privacy Framework requires the design of projects to address privacy and secrecy considerations. Human Services has not complied with this requirement due to the absence of a Privacy Impact Assessment for the Medicare Express Plus mobile phone application.

5.8 Further, the 'Tell Us Once' Privacy Impact Assessment did not demonstrate that all relevant privacy and secrecy considerations had been addressed. Human Services advised the ANAO that although an assessment of secrecy provisions was not included in the 'Tell Us Once' Privacy Impact Assessment, the department had sought and received legal advice regarding the provisions.[99] Despite this advice being received prior to the finalisation of the Privacy Impact Assessment, it was not acknowledged in the Assessment and it was therefore unclear whether the relevant provisions had been considered.

5.9 Human Services is applying better practice guidance from the Office of the Australian Information Commissioner (OAIC) by requiring Privacy Impact Assessments for new projects.[100] However, it is not consistently preparing Privacy Impact Assessments for new projects and, when prepared, the Privacy Impact Assessments may not cover all relevant privacy and secrecy legislative requirements. Human Services should consistently prepare Privacy Impact Assessments to fully realise the benefits of this approach.

Compliance with legislative and policy requirements

5.10 The privacy and secrecy provisions that apply to Medicare customer data are set out in the *National Health Act 1953*, the *Health Insurance Act 1973* and the Privacy Act.[101]

The *National Health Act 1953* and the *Health Insurance Act 1973*

5.11 The secrecy provisions of the *National Health Act 1953* and the *Health Insurance Act 1973* apply to all staff performing duties, or exercising powers

99 Human Services advised that this advice was not included in the Privacy Impact Assessment to maintain professional privilege.

100 A Human Services steering committee also endorses Privacy Impact Assessments associated with Service Delivery Reform.

101 This audit did not examine the secrecy and confidentiality provisions that apply to Medicare under section 15 of the *Healthcare Identifiers Act 2010* or section 59 of the *Personally Controlled Electronic Health Records Act 2012*.

under these Acts or under Medicare.[102] These provisions are additional to, and have precedence over, the provisions of the Privacy Act.[103] They restrict the communication of information and specify when and to whom the department can lawfully release information.[104]

5.12 Human Services responds to its legislative secrecy requirements primarily through preventive measures including:

- making staff aware of relevant consent and disclosure provisions and the associated delegation and authorisation instruments required to appropriately exercise powers under the National Health and Health Insurance Acts;
- providing data about the secrecy provisions on its intranet, including an overview of the secrecy provisions on the departmental intranet and advising staff to seek advice from the Human Services privacy section when required; and
- referencing legislative requirements for secrecy including those contained in the 'Operational Privacy Policy' (refer to paragraph 5.4).

5.13 Human Services also maintains a register of delegations and authorisations including those relating to Medicare which is supported by a Secretary's Management Direction which restricts the employees who can exercise delegations.

5.14 Measures for identifying privacy incidents include providing guidance for the reporting of privacy incidents which outline the relevant secrecy provisions that apply to Medicare customer data.

5.15 Through the above measures, Human Services provides information and support to staff to assist them to understand their legislative secrecy responsibilities under the *National Health Act 1953* and the *Health Insurance Act 1973*.

---

102 The relevant secrecy provisions are section 130 of the *Health Insurance Act 1973* and section 135A of *the National Health Act 1953*.

103 The secrecy provisions continue to apply to staff after they leave the department. A contractor having access to Medicare customer data, would also be covered by the secrecy provisions.

104 These provisions allow for communicating protected information to other government agencies and in the public interest. This means that the Chief Executive Medicare can communicate 'protected information' to specified government agencies in certain circumstances. For example, disclosures may be made to the Department of Veterans' Affairs and the Department of Immigration and Border Protection under section 130(7) of the *Health Insurance Act 1973.*

Privacy Guidelines for Medicare Benefits and Pharmaceutical Benefits Programs

5.16 In addition to the secrecy provisions, section 135AA of the *National Health Act 1953* requires the Privacy Commissioner to issue guidelines that relate to the Medicare Benefits Program and the Pharmaceutical Benefits Program.[105] Human Services must comply with these *Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs (*the guidelines*).*[106]

5.17 The guidelines introduce standards additional to the requirements of the Information Privacy Principles (IPPs) under the Privacy Act. They regulate the way that agencies link and store claims data obtained under the Medicare Benefits Program and the Pharmaceutical Benefits Program.[107]

5.18 While these guidelines principally relate to claims data, Guideline 2.2 specifically mentions the Medicare enrolment and entitlement databases, which hold Medicare customer data, and requires that these databases be separate. The guidelines state:

> Databases of claims data obtained under the Medicare Benefits Program and the Pharmaceutical Benefits Program (that is, the 'Medicare Benefits claims database' and the 'Pharmaceutical Benefits claims database') must be kept separate from Medicare Australia's enrolment and entitlement databases.[108]

5.19 Human Services advised that it meets Guideline 2.2 through system architecture and design. That is, by maintaining the eligibility and enrolment data of consumers and providers separately; processing claims in its mainframe, the Customer Information Control System; and, maintaining Pharmaceutical Benefits Scheme claiming data on another system.

5.20 Guideline 2.5 establishes a reporting regime which requires Human Services to submit a Technical Standards Report (TSR) to the Privacy Commissioner specifying compliance with the criteria in Guideline 2.4. These

105 The Privacy Commissioner is part of the OAIC, which is responsible for the privacy functions that are conferred by the *Privacy Act 1988* and other laws.

106 Office of the Australian Information Commissioner, *Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs* [Internet], OAIC, available from: <http://www.oaic.gov.au/privacy/applying–privacy–law/legally–binding–privacy–guidelines–and–rules/privacy–guidelines–for–the–medicare–benefits–and–pharmaceutical–benefits–programs–issued–march–2008–effective–from–1–july–2008> [accessed 12 November 2013].

107 Such linkages may reveal detailed data on the health status and history of the majority of Australians, beyond what is necessary for the administration of the respective programs.

108 Office of the Australian Information Commissioner, op.cit., p. 4.

criteria set out the matters that the TSR must address which relate to the Medicare Benefits claims database and the Pharmaceutical Benefits claims database, including that adequate data security arrangements are in place. Human Services is also required to lodge a variation report to advise the Privacy Commissioner if it varies the technical standards under Guideline 2.6.

5.21 The 2004–05 performance audit found that Human Services was not able to produce a TSR of the type required by the Guidelines.[109] The audit recommended that Human Services redevelop and lodge a TSR that complied with the guidelines (Recommendation No. 6). In agreeing to the recommendation, Human Services also indicated that it would amend the TSR with future changes.

5.22 Human Services submitted a final version of a TSR on 23 October 2009, four years after the ANAO audit report was tabled and some nine months after the date specified by the Privacy Commissioner's Guidelines. The guidelines, which were re–issued on 6 March 2008, and took effect on 1 July 2008[110], required Human Services to lodge a TSR within six months of the guidelines coming into effect; that is, by 1 January 2009.

5.23 The department's current TSR, which has not been updated since October 2009, refers to organisational details, policies and references which are out–of–date and inaccurate. In light of inaccuracies in the TSR observed by the ANAO, there is scope for Human Services to:

- reassess its compliance with the privacy guidelines and ensure there is an accurate and up–to–date description of the technical standards lodged with the OAIC; and
- develop and implement a review process for the TSR that monitors and provides variation reports to the OAIC in a more timely manner.

The *Privacy Act 1988* and Information Privacy Principles

5.24 The Privacy Act includes 11 IPPs. These principles are intended to provide individuals with protection against the mishandling of their personal

109 ANAO Audit Report No.24 2004–05 *Integrity of Medicare Enrolment Data*, p. 68.

110 The ANAO Audit Report No.24 2004–05 *Integrity of Medicare Enrolment Data* assessed compliance with the 22 January 1996 version of the Guidelines. This audit assesses Human Services compliance with the Guidelines issued on 6 March 2008 and which took effect on 1 July 2008.

data.[111] They apply to Human Services whenever it collects, stores, uses and discloses any personal data about individuals as part of Medicare. The Privacy Act defines personal data as:

> data or an opinion (including data or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the data or opinion.[112]

5.25 The IPPs set out minimum standards for Australian, ACT and Norfolk Island government agencies. The Privacy Commissioner issued guidelines for the application of the principles, which are not legally binding.[113] In relation to Medicare customer data, the processes, guidance and policies that Human Services has in place are generally compliant with the IPPs as outlined in Table 5.1.

111 The 11 IPPs in section 14 of the Privacy Act were in effect during the conduct of the audit. They are to be replaced by 13 Australian Privacy Principles that come into effect in March 2014. The ANAO did not test Human Services' policy and procedures against the new Australian Privacy Principles but noted that Human Services has made some preparations for their introduction as part of privacy law reform activities associated with the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* which was passed with amendments on 29 November 2012.

112 This is the definition from section 6 of the *Privacy Act 1988* which has been adopted in the Human Services 'Operational Privacy Policy'.

113 Office of the Australian Information Commissioner, *Guidelines to Information Privacy Principles* [Internet] OAIC, available from: <http://www.oaic.gov.au/privacy/privacy–act/information–privacy–principles> [accessed 17 October 2013].

Table 5.1: Human Services' processes, guidance and policies' compliance with IPPs

IPP Number(s)	Description of IPP	Compliant
1	Requires that Human Services only collect personal information for a lawful purpose, which is directly related and necessary to its functions.[114]	✓
2	Requires that when Human Services asks for personal information it must explain why it is collecting the information, relevant legislation and how this information will be shared.	✓*
3	Requires Human Services, when it asks for personal information, to ensure that it is relevant, up–to–date and complete. The department is also obliged to minimise the degree of intrusion when collecting personal information.	✓
4	Requires Human Services, as a record keeper of personal information, to ensure that this data is stored and kept secure from loss, unauthorised access, use, modification, disclosure and other misuse.	✓*
5	Requires Human Services to publish details of its records that contain personal information[115], reflecting an expectation that entities not secretly keep personal information about individuals.	✓
6	Allows individuals to access their records.	✓
7–8	Requires Human Services to take all reasonable steps to ensure a record is accurate, relevant, up–to–date and not misleading.	✓
9–11	Relates to the use of personal information for relevant purposes, limits on use of personal information and limits on disclosure.	✓

Source: ANAO analysis.

Note*: Compliant with areas for improvement.

5.26 Table 5.1 shows that there are two areas for improvement in relation to Human Services' compliance with the IPPs:

- consistency of disclosure provisions in the privacy notes provided in the Medicare Express Plus mobile phone application (IPP2); and
- security arrangements including physical, data and personnel security as well as security governance (IPP4).

114 Medicare's functions are set out in s. 6 of the *Human Services (Medicare) Act 1973*.

115 There is a similar requirement in section nine of the *Freedom of Information Act 1982* regarding the obligation to publish details of department manuals and other policy and procedural documentation used in the decision–making process.

Disclosure provisions on privacy notes

5.27 The Medicare Express Plus mobile phone application has two privacy statements.[116] One is on the Human Services website and the other is in the terms and conditions that must be accepted to use the mobile phone application for the first time. Both the privacy notices for the Medicare Express Plus mobile phone application are generally compliant with the minimum requirements of IPP2 as they indicate that personal information is collected for a Medicare or Human Services purpose; that this information may be required by law; and may be disclosed to other parties where it is authorised or required by law or by consent.

5.28 However, the terms and conditions for the mobile application specifically mention that certain information may be disclosed, such as email and mailing addresses, to Apple in accordance with the terms of Apple's iOS Developer Program License Agreement.[117] This potential disclosure provision is not included in the information on the Human Services website.

5.29 For consistency and further transparency, Human Services could align the disclosure provisions for the information privacy notes provided in the terms and conditions for the Medicare Express Plus mobile phone application with those provided on the Human Services website.

Security of personal information

5.30 In terms of physical security, Human Services has in place Physical Security Guidelines which respond to the mandatory requirements of the *Protective Security Policy Framework* and the implementation of the *Australian Government Physical Security Management Core Policy.*

5.31 As required by the *Protective Security Policy Framework*, Human Services undertook a self–assessment of its compliance against the 33 mandatory areas, which identified non–compliance in four areas:

- physical security—protection of information and ICT systems;
- security governance—training and education, departmental planning and risk management;

116 There is also a copy of the full privacy policy that can be obtained at Human Services Service Centres.

117 The software developed for the Medicare Express Plus mobile phone application is currently only available through Apple on the iTunes App Store which is subject to Apple's Developer Program License Agreement. The license agreement must be agreed to prior to developing software for Apple's iOS (a mobile operating system).

- information security—management of information and ICT systems; and
- personnel security—application of security vetting and designated security assessed positions.

5.32 Human Services has advised it is taking steps to address these areas of non–compliance, including:

- undertaking audits of compliance with physical security requirements and annual reviews of implementation of ICT infrastructure security arrangements;
- promoting security awareness and training, and identifying and responding to additional training needs; and
- reviewing the Departmental Security Plan to ensure that *Protective Security Policy Framework* requirements are met.

Privacy training and awareness activities

5.33 Privacy training and awareness activities are a component of Human Services' induction training which all new starters are required to complete within two weeks of joining the department. Where possible, staff are also expected to attend a facilitated face–to–face training session.[118] Human Services monitors staff attendance by requiring them to submit a completion record[119] for their induction training and training records are maintained by the Learning and Development Branch.

5.34 The two mandatory eLearning modules are: 'An introduction to privacy, secrecy and confidentiality in Human Services'; and 'Legislation and Human Services'.[120] The modules reflect Human Services' legislative and policy obligations including those for secrecy and confidentiality and the IPPs under the Privacy Act. An interactive web–based format steps through relevant scenarios of privacy issues along with advice and data on staff responsibilities and the implications of non–compliance. The modules include knowledge checks and links to supporting and further data are also provided.

118 Staff who are returning after an absence of 12 months or longer are required to complete the mandatory eLearning modules.

119 This record is signed by the staff member's manager and sent to the relevant National Learning Network (NLN) representative.

120 The eLearning privacy package forms part of the induction and annual privacy refresher package.

Conclusion

5.35 Overall, Human Services has a comprehensive framework for managing Medicare customer privacy. Specifically, Human Services has processes, guidance and policies in place to support compliance with the:

- relevant legislative provisions under the *National Health Act 1953* and the *Health Insurance Act 1973* for secrecy and confidentiality;
- obligations of the IPPs under the *Privacy Act 1988*; and
- the *Privacy Guidelines for Medicare Benefits and Pharmaceutical Benefits Programs*.

5.36 Human Services has identified areas of non-compliance in relation to the mandatory requirements of the *Protective Security Policy Framework* which it is taking action to address. Other shortcomings with Human Services' management of the privacy of Medicare customer data could be addressed by:

- implementing a review and update process for the Technical Standard Report and lodging variation reports with the OAIC; and
- providing consistent disclosure provisions for the Medicare Express Plus mobile phone application.

6. Security of Customer Data

This chapter examines Human Services' security arrangements for Medicare customer data.

Introduction

6.1 The Australian Signals Directorate[121] issues the Australian Government's Information Security Manual (ISM). This is the standard for security of Australian Government and some state and territory agencies' ICT systems. The ISM includes three documents: *Executive Companion*, *Principles Document* and *Controls*.

6.2 The *Controls* manual applies to a range of Australian Government and state and territory agencies, including Human Services. The purpose of the manual is to assist these agencies to apply a risk–based approach to protecting their data and ICT systems.

6.3 In relation to Medicare customer data, Human Services' compliance with the ISM in the following areas was examined:

- Security documentation;
- System certification and accreditation;
- Risk management;
- Active security monitoring;
- User access; and
- Security awareness.

Security documentation

6.4 Appropriate documentation can support the accurate and consistent application of policies and procedures. It also increases accountability and provides a standard to measure against.[122] The ISM outlines the mandatory documents agencies are required to prepare in relation to ICT systems.

121 In May 2013, the Defence Signals Directorate was renamed the Australian Signals Directorate.

122 Australian Signals Directorate, *Information Security Manual: Controls*, Australian Signals Directorate, Canberra, 2013, p. 24.

6.5 The ANAO examined Human Services' suite of documentation for Medicare. Table 6.1 outlines Human Services' compliance with preparing documents mandated by the ISM.

Table 6.1: Human Services' compliance with mandatory security documentation

Document	Purpose	Compliant
Information Security Policy	Statement of high level security policies.	✓
Security Risk Management Plan(s)	Best practice approach to identifying and reducing potential security risks. There can be one plan to cover multiple systems but every system needs to be covered by one.	×
System Security Plan(s)	Describes the implementation and operation of a system's controls. Every system is required to be covered by a plan, however, common details of multiple systems can be consolidated into one plan.	×
Standard Operating Procedures(s)	Step–by–step guide to undertaking security related tasks. Common procedures for multiple systems can be consolidated into one set of procedures. Each system needs to be covered by a set of procedures.	×
Incident Response Plan	Plan for responding to cyber security incidents.	✓

Source: ANAO analysis of Human Services information.

6.6 At the time of the ANAO's analysis, there was variation in the extent to which Human Services had developed the mandatory security documentation for the ICT systems used to record, process and store Medicare customer data: the Consumer Directory, CDMS, MyGov, Medicare Express Plus mobile phone application and Medicare Online Services. Some documentation had been completed; some remained in draft form; and some documents had not been prepared.

6.7 Preparing these documents will provide assurance that Human Services has the appropriate documentation in place to manage the security of customer data.

Business Continuity and Disaster Recovery plans

6.8 Business continuity plans can assist agencies to ensure critical system functions continue to operate when the system is in a degraded state.[123]

123 ibid., p. 36.

Disaster Recovery Plans assist agencies to reduce the time between a disaster occurring and critical functions being restored. The ISM recommends that agencies have both business continuity and disaster recovery plans.[124]

6.9 Human Services has a policy and framework for business continuity. It is currently developing business continuity plans under the 'Business Continuity Framework' for each Human Services division. As part of this process, each division has undertaken a business impact analysis to identify critical functions.

6.10 Human Services has a policy and strategy for disaster recovery. It also has a draft Disaster Recovery Plan for its data centres, however, this draft plan does not reflect all of the critical functions identified in the business impact analyses. Human Services would benefit from finalising a disaster recovery plan, which reflects the critical functions identified.

System certification and accreditation

6.11 Accreditation is the process whereby the residual security risks associated with a system and its data are recognised and accepted. Accreditation is undertaken prior to operating a system and involves conducting an audit to review the system architecture, including security documentation, and assessing the implementation and effectiveness of system controls. Audits result in a report that outlines areas of compliance and non–compliance and suggest actions for improvement.

6.12 Following the audit, an assessment of the residual security risk relating to the operation of the system is required. This assessment is included in a certification report which is provided to the accreditation authority, who is generally the agency head or their delegate.

6.13 The ISM requires agencies to ensure their Standard Operating Environment[125], network infrastructure and gateways[126] are accredited before they are used to process, store or communicate sensitive or classified

124 ibid., p. 36.

125 Standard Operating Environments are the operating system and associated software that is deployed on multiple devices, including servers, workstations, laptops and mobile devices.

126 Gateways securely manage data between connected networks from different security domains.

information. Agencies are also required to ensure that all systems are accredited before they are connected via a gateway.[127]

6.14 Human Services has 'Certification and Accreditation Policy and Procedures', which outlines the processes for certifying and accrediting Human Services systems. According to Human Services' policy, the certification process assesses five aspects of system development and operation resulting in a certification report. This report is then considered as part of the accreditation process.

6.15 Human Services provided the ANAO with a certificate of conditional provisional accreditation for its gateway which was valid until February 2014. However, it was unable to provide evidence of certification for the systems which record, process and store Medicare customer data: the CDMS, Consumer Directory, MyGov, Medicare Online Services and the Medicare Express Plus mobile phone application. It also could not provide evidence of accreditation of its Standard Operating Environment.

6.16 Certification and accreditation of systems and their supporting ICT infrastructure is both a requirement of the ISM and Human Services' own policy. These processes provide assurance that security risks are being managed to an acceptable level. Human Services would benefit from completing the certification and accreditation requirements outlined in the ISM to demonstrate that the associated risks are being managed to an acceptable level.

Recommendation No.5

6.17 To ensure compliance with the mandatory requirements of the Information Security Manual, the ANAO recommends that Human Services:

- undertake a review of existing documentation and finalise all mandated security documents; and
- complete the mandated certification and accreditation processes for the systems that record, process and store Medicare customer data and the ICT infrastructure that supports them.

127 Australian Signals Directorate, op cit., p. 39.

Agency response:

6.18 *The department agrees with this recommendation.*

6.19 *A review of existing documentation has been completed with all mandatory security documents finalised. The mandatory certification and accreditation processes consist of several components and the requirement for certification and accreditation will be completed by 30 June 2014.*

Risk management

6.20 The ISM encourages agencies to take a risk–based approach to data security.[128] Table 6.2 outlines agencies' responsibilities in relation to risk management and Human Services' compliance with these responsibilities.

Table 6.2: Human Services' compliance with risk management

Requirement	Compliant
Identify and analyse security risks to their data and systems	✓
Treat risks that are deemed to be unacceptable and mitigate residual risks by introducing alternative security measures	×
Formally accept risks deemed to be acceptable and monitor them on an ongoing basis	✓
Incorporate the controls outlined in the ISM into their risk management processes	–[1]
Identify specific system risks that require the implementation of controls additional to those specified in the ISM	✓
Document identified risks, the evaluation of those risks and the mitigation strategies introduced to manage them in the Security Risk Management Plan	×

Source: ANAO analysis and Australian Signals Directorate, *Information Security Manual: Controls*, Australian Signals Directorate, Canberra, 2013.

Note 1: While controls outlined in the ISM have been identified by Human Services as treatments for identified risks, some of these controls are not in place (refer to paragraph 6.24).

6.21 To manage risks to ICT systems and data, Human Services' Chief Information Officer (CIO) Group, which maintains the Consumer Directory, CDMS and other systems such as Medicare Online Services and Express Plus Medicare mobile phone application, developed its own *CIO Group Risk Management Plan*.

128 ibid., p. 5.

6.22 The plan identifies 17 risks associated with the group's 17 business goals. As part of Human Services broader risk management framework, the CIO Group is required to report on these risks monthly to the Governance branch which, in turn, reports to the Risk, Business Continuity and Security Committee. Two of these 17 risks are directly related to the integrity of Medicare customer data: 'Failure to ensure continuity of ICT services and minimise the business impact of a major disruption' (Risk six) and 'Failure to maintain integrity and confidentiality of data' (Risk 12). These risks are rated as 'high' and 'medium' after treatment, respectively.

6.23 The ICT Group has also established a Risk Review Board which meets regularly to review the CIO Group's risks; provide a link between the departmental and group's risks; monitor the implementation of strategies and actions in response to audit findings; and support the management of risk and continuity of business delivery. The focus of this group is consistent with the requirements outlined in the ISM (refer to Table 6.2). The regular attention of this group; particularly in relation to the effectiveness of controls and treatments will provide ongoing assurance that risks are being managed effectively.

6.24 Human Services' risk management in relation to Medicare customer data is mostly compliant with the requirements of the ISM. However, it could address the shortcomings in its risk management approach, including:

- some of the existing controls and treatments[129] for the two relevant risks identified in the *CIO Group Risk Management Plan* are not in place and consequently, these risks may not be adequately treated; and
- Security Risk Management Plans have not been finalised for all systems that record, process and store Medicare customer data (refer to paragraphs 6.4 to 6.7).

Active security monitoring

6.25 Monitoring systems and data allows agencies to identify and address security risks. Assessing vulnerabilities prior to the introduction of a system and ongoing monitoring of ICT systems, allows agencies to analyse risks and implement treatments to manage them. Human Services has processes in place

129 Some of the proposed treatments for these risks are not expected to be implemented until June 2014.

to assess security risks prior to systems being introduced. It also conducts regular monitoring of security threats.

Prior to system introduction

6.26 Human Services has processes to detect vulnerabilities prior to the introduction of a new system or system enhancement, including penetration testing and code review.

Penetration testing

6.27 Penetration testing involves testing systems and software for security vulnerabilities, which are ranked in terms of seriousness. Human Services advised that it conducts penetration testing for all new external facing systems[130], or where significant changes are made to an existing system. Identified 'extreme', 'high', and 'medium' risks must have agreed mitigation strategies, prior to systems implementation.

6.28 When vulnerabilities are identified, they are assigned to a Senior Executive Officer with Human Services for resolution. They are also reviewed by the ICT Security Section when it undertakes a system compliance review.[131] Human Services advised that vulnerabilities which are rated as medium or higher must be remediated by or as part of the next system release.

6.29 Medicare Online Services was tested in 2008, when it was introduced, and was found to have 'moderate' business risk exposure on a five point scale between 'insignificant' and 'extreme', which could be exploited for false identity purposes. Human Services addressed this vulnerability in 2010—two years after it was identified.[132]

6.30 Prior to their introduction, the Medicare Express Plus mobile phone application and MyGov were also subject to penetration testing, however, a different risk ranking scale was applied than that used in the Medicare Online Services penetration testing (refer to Note 1 of Table 6.3). The results of these tests are outlined in Table 6.3.

130 Human Services advised that an external facing system is one that is accessible via the internet.

131 These are undertaken at least biannually.

132 This vulnerability was addressed as it was creating an increase in customer enquiries.

Table 6.3: Penetration testing results

System	No. of vulnerabilities identified
Medicare Express Plus mobile phone application	One medium Two informational[1]
MyGov	Four medium Four low severity Four informational[1]

Source: ANAO analysis of Human Services internal documents.

Note 1: These vulnerabilities were ranked using the Common Vulnerability Scoring System. At a minimum, the scoring system takes into account: how the vulnerability is exploited; the complexity of attack required to exploit the vulnerability; the number of times the attacker must authenticate to a target to exploit the vulnerability; and the impact on confidentiality, integrity and availability.

6.31 The 'medium' vulnerability identified for the Medicare Express Plus mobile phone application was the same type of vulnerability identified in the Medicare Online Services penetration testing (refer to paragraph 6.29). Human Services would benefit from using the results of penetration testing to inform future system development in order to prevent known vulnerabilities prior to a system release.

6.32 For the four 'medium' vulnerabilities identified in the MyGov penetration testing report, the impact of one was unknown. However, for the remaining three vulnerabilities where the impact was known, there were associated risks to the privacy and security of customer data and the potential for fraudulent online claiming.

6.33 As a result of this audit, Human Services advised that it:

- has addressed two of the 'medium' vulnerabilities identified for MyGov; and
- intends to address the remaining two 'medium' MyGov vulnerabilities and the Medicare Express Plus mobile phone application 'medium' vulnerability after further analysis to be completed by June 2014.

6.34 Human Services' approach to resolve these vulnerabilities is inconsistent with the department's policy that all vulnerabilities rated as 'medium' or higher must be rectified in the next release cycle. Given the recognised risks associated with these vulnerabilities, the ANAO suggests that they be addressed.

6.35 More broadly, Human Services' policy to address 'medium' or higher rated vulnerabilities is not being implemented consistently and there are deficiencies with the existing review process aimed at monitoring the

rectification of these vulnerabilities. The ANAO suggests that Human Services consider reviewing its current monitoring process with a view to providing more effective oversight of the rectification of vulnerabilities rated as 'medium' or higher.

Security code review

6.36 Security code review is an audit of an application's source code[133] and is intended to examine whether appropriate controls are in place and that they are working as intended. As part of conducting a code review, a number of tests are undertaken to identify vulnerabilities. Human Services advised that code reviews were introduced in 2011 and are undertaken for approximately 90 per cent of new systems development.

6.37 Table 6.4 outlines the results of the code reviews undertaken prior to the introduction of MyGov and the Medicare Express Plus mobile phone application, and shows that no major vulnerabilities were identified. A code review was not undertaken for Medicare Online Services as this was introduced before the code review process was adopted by Human Services.

Table 6.4: Code review results

System	Vulnerabilities identified
Medicare Express Plus mobile phone application	No major vulnerabilities identified but the report did highlight the vulnerability identified in the penetration testing where there was an error message generated from a log-on request (Table 6.3).
MyGov	Code is quite sound with five minor findings.

Source: ANAO analysis of Human Services information.

Threat landscape reports

6.38 Human Services monitors security risks on an ongoing basis by producing an IT Security Threat Landscape report which is presented to the Risk, Business Continuity and Security Committee. These monthly reports outline a number of security threats, including incidents, internet threats, cyber security and access revocation. Additional items are added to these reports when Human Services determines they require ongoing monitoring.

133 Source code are high–level instructions for an application which are then written as object code used to instruct an application.

6.39 Centrelink self–service accounts, specifically locked accounts due to unauthorised access, are included in the IT Security Threat Landscape reports, but monitoring of Medicare accounts is not included. There is risk associated with Medicare online claiming as there is the opportunity for a person to use a customer's account or their own, to fraudulently claim Medicare benefits.

6.40 Human Services should consider monitoring unsuccessful access attempts and unusual claiming activity associated with Medicare Online Services and the Medicare Express Plus mobile phone application in its Threat Landscape Report given the associated risk.

User access

6.41 To maintain the privacy and security of customer data, departments should have appropriate controls in place for users to access data and systems.[134] These include comprehensive processes to monitor access and clearly defined roles and responsibilities to effectively manage unauthorised access and privacy incidents[135] if they occur. These management and control processes should be supported by appropriate staff guidance and awareness that aims to prevent unauthorised access and privacy incidents.

6.42 The two main repositories for Medicare customer data are the Consumer Directory and the Medicare Data Warehouse. To securely manage and protect the privacy of Medicare customer data within a database environment, agencies require effective controls to:

- provide and monitor access; and
- manage unauthorised access[136] and privacy incidents.

Providing and monitoring access

6.43 Human Services has processes for granting new users access to the Consumer Directory and Medicare Data Warehouse. Access privileges are managed by registering and authorising users. The process of granting user access aligns with the requirement of IPP4 for secure and legitimate access and Human Services' 'Operational Privacy Policy' and 'Access Control Policy—

134 Australian Signals Directorate, op cit., p. 190.

135 Privacy incidents can be defined as incidents raised by staff, customers, the OAIC or the Commonwealth Ombudsman.

136 Unauthorised access is the misuse of protected data held by Human Services. It occurs when a staff member inappropriately uses protected data that they have access to as part of their duties.

Medicare Program' whereby access to Medicare customer data is provided based on a demonstrated business need.

Medicare Data Warehouse

6.44 Human Services has advised the ANAO that the Medicare Data Warehouse is expected to be decommissioned by the third quarter of 2014, and Medicare customer data is being transferred to a single Human Services Enterprise Data Warehouse platform.[137] The Medicare Data Warehouse can be accessed in two main ways: DB2[138] (database) tables and reports published on the SAS Data Delivery Portal.[139]

6.45 While the process of granting access to the Medicare Data Warehouse is consistent with legislative and policy requirements (refer to paragraph 6.43), the user access form for the *Medicare Data Warehouse SAS Data Delivery Portal* is out–of–date. Human Services would benefit from keeping the list of data owners, from whom approval is required, up–to–date so that approval is obtained from the correct data owners. This approach would also contribute to a more efficient approval process.

6.46 Human Services can significantly improve its management and monitoring of access to the Medicare Data Warehouse. Access controls for exiting users are not in place and Human Services does not have a process for removing users from the Medicare Data Warehouse. The list of current Medicare Data Warehouse users includes users who were last active from 2007 through to 2013. The ANAO suggests that Human Services develop and implement a process to manage exiting users of the Medicare Data Warehouse and that it maintain an up–to–date list of users.

6.47 Human Services does not regularly monitor access to the Medicare Data Warehouse and does not report on use and access to the Medicare Data Warehouse. To provide assurance that Medicare customer data is not being inappropriately accessed, the ANAO suggests that Human Services commence monitoring and reporting access to the Medicare Data Warehouse and the Enterprise Data Warehouse, once the Medicare customer data is transferred.

---

137 Human Services advised the ANAO that the data associated with each of the service delivery brands will be maintained separately within the new platform.

138 DB2 is a family of database server products developed by IBM.

139 SAS Data Delivery Portal is a web application interface to the Medicare Data Warehouse that provides access to performance and statistical reports.

Consumer Directory

6.48 In terms of managing exiting users from the CDMS, all staff have a unique identifier attached to their access profile which matches their job description. When staff leave the department they no longer have an active user profile and can no longer access the CDMS. Reports are run daily to identify staff who have left the department the previous day, to confirm that their access has been disabled. When a staff member changes position, there is also a requirement for manager[140] or director level approval before access is approved.

6.49 A list of current users of the Consumer Directory showed that all users had accessed the directory within the preceding 11 months which indicated that access was actively managed. When staff transfer internally they are granted access in accordance with their new role and their previous access is removed.

6.50 Access to the Consumer Directory via the CDMS is actively monitored. This includes the use of data matching tools to identify unauthorised access to customer records. The main detection tool for Medicare is the Data Access Review Tool. This tool was developed to automatically detect staff members who may have inappropriately accessed the records of customers associated with them and is conducted on a fortnightly basis. Human Services also routinely logs access to systems[141], monitors access to high profile individuals' records and regularly receives allegations via tip–offs and referrals from internal and external sources. These are given first priority for investigation.

6.51 As part of the *Internal Fraud Control and Unauthorised Access Detection Program*[142], Human Services also has targeted detection projects which respond to emerging risks. These complement business–as–usual monitoring activities such as the Data Access Review Tool. The combination of monitoring and investigative activities contributes to protecting the privacy and security of Medicare customer data and systems.

140 Executive Level 1 or higher approval is required for access to the CDMS.

141 Human Services monitors users with incompatible access privileges across Human Services systems including the CDMS. This is done on a monthly basis and reported quarterly.

142 The *Internal Fraud and Unauthorised Access Detection Program* was designed to detect incidents which may indicate the occurrence of internal fraud and/or unauthorised access of data. These incidents are then assessed to determine whether further review or investigation action is required.

6.52 Despite Human Services' efforts, unauthorised access[143] continues to be the most frequent behaviour referred for code of conduct investigations. In 2012–13, there were 75 cases of unauthorised access finalised which related to Medicare. Human Services advised that of these 75 cases, 32 were referred for further action including six cases which were substantiated.

Developments in managing unauthorised access and privacy incidents

6.53 A number of recent developments in Human Services have affected the management of unauthorised access and privacy incidents in Human Services:

- A whole of department process to manage unauthorised access—which sets out key decision points; allocates responsibilities; and identifies associated referral and reporting processes.[144]
- Pressure testing—spot checks and formal audits to identify potential threats and risks to provide assurance that access to personal protected data is legitimate.
- Code of conduct procedures and sanctions—includes a referral process and sanctions for code of conduct breaches.[145] Quarterly reports on code of conduct activities are provided to the Secretary.
- Privacy incident reporting—in addition to established procedures for reporting privacy incidents, including reporting to the OAIC[146], Human Services has introduced an annual privacy incident report to the Executive Committee with subsequent reporting being provided on a quarterly basis.
- Information access policy statement—which assists staff to understand their obligations with respect to access, use or disclosure of information which the department holds.

143 This relates to staff accessing customer records without a legitimate business purpose, for example, the records of family members, ex–partners, neighbours or work colleagues.

144 The three branches are: Internal Fraud Control and Investigations, Workplace Relations and Ombudsman Privacy and Freedom of Information.

145 Sanctions include counselling, termination of employment and prosecution for staff depending on the nature and severity of unauthorised access or privacy breaches.

146 When Human Services identifies an incident that may affect one or more customers in a significant way, it may voluntarily notify the OAIC of the breach.

6.54 Taken together, these developments and their associated activities contribute to the framework for managing unauthorised access and privacy incidents for Medicare customer data.

Security awareness

6.55 The ISM notes that continual data security awareness cultivates a security culture. It requires agencies to provide ongoing security awareness and training to staff about data security policies.[147]

6.56 Human Services provides a general security awareness eLearning module that can be accessed by staff on its website. In addition, it provides four security induction eLearning modules, three of which are mandatory.[148]

6.57 Human Services also provides some security information on its intranet including:

- information security and classifications; and
- better practice password guidance.

6.58 In assessing its compliance against the *Protective Security Policy Framework*[149], Human Services found it was non–compliant with this requirement because while it could report the number of staff and contractors who had completed security awareness training, it could not identify those staff and contractors who had not. In response to this finding, Human Services is undertaking a number of corrective actions including:

- promoting the security eLearning module and other personnel security information;
- reviewing security training to identify whether additional training is required; and
- providing security training to identified elements of Human Services staff, including Senior Executive and staff who hold particular security clearances.

147 Australian Signals Directorate, op cit., p. 72.

148 The three mandatory modules are: Module one—'Physical security'; Module two—'The Australian Government Security Classification System and Protectively Marking and Handling Data'; and Module 4—'Security in a Customer Face to Face Environment'. Module 3—'Personnel Security/Security Clearances' is optional.

149 The *Protective Security Policy Framework* is issued by the Attorney–General's Department. It requires that agencies undertake an annual self–assessment of 33 mandatory components.

Conclusion

6.59 Human Services undertakes a range of information security initiatives, including pre–deployment vulnerability testing of ICT systems, security monitoring, user access management and risk management activities. There are, however, opportunities to improve the implementation of some of these initiatives so that Human Services is compliant with the ISM requirements.

6.60 There are opportunities for Human Services to improve its compliance with the ISM including:

- ensuring that the controls and treatments identified to mitigate identified risks are in place;
- adopting a more risk-based approach to active security monitoring activities;
- monitoring and reporting on access to the Medicare Data Warehouse; and
- implementing the actions identified to assist it to meet its security awareness and training responsibilities.

6.61 In particular, Human Services is not compliant with the mandatory security documentation requirement of the ISM as it has not prepared all of the relevant documents for the systems which record, process and store Medicare customer information. Further, Human Services is not compliant with the mandatory system certification and accreditation requirements outlined in the ISM, which should be completed.

Ian McPhee
Auditor-General

Canberra ACT
24 April 2014

Appendices

Appendix 1: Agency Response

Australian Government
Department of Human Services

Kathryn Campbell CSC
Secretary

Ref: EC14/86

Dr Tom Ioannou
Group Executive Director
Performance Audit Services Group
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Dr Ioannou

Thank you for the opportunity to comment formally on the proposed 'section 19' report arising from the Australian National Audit Office (ANAO) performance audit on the *Integrity of Medicare Customer Data*, dated 7 March 2014.

The Department of Human Services (the department) agrees with the ANAO's recommendations. The department places an extremely high level focus on the security of our systems and the protection of data and the report's commentary will assist the department to improve our standards even further.

Attachment A to this letter details our overall response to the proposed report and to each of the ANAO's recommendations.

If you would like to discuss the department's response, please do not hesitate to contact Jenny Benjamin, National Manager Medicare and Veterans Branch on (02) 6143 7294.

Yours sincerely

Kathryn Campbell
9 April 2014

PO Box 3959, Manuka ACT 2603 • Telephone (02) 6223 4411 • Facsimile (02) 6223 4489
Internet www.humanservices.gov.au

Attachment A

Response to the section 19 report on the performance audit on the Integrity of Medicare Customer Data

Recommendation No.1
To better support customer service officers who enrol Medicare customers and update their information, the ANAO recommends that Human Services review its eLearning training and eReference guidance for consistency and completeness.

DHS response:
The department agrees with this recommendation.

The department has commenced a review of Medicare enrolment eReference guidance material. The department's eLearning training will also be reviewed to ensure consistency and completeness.

Recommendation No.2
To better manage duplicate and intertwined records and improve the integrity of its customer data, the ANAO recommends that Human Services:

- consider ways to better identify duplicate customer enrolments;
- investigate the underlying causes of duplicate enrolments with a view to informing approaches to their prevention; and
- develop and implement guidelines for resolving intertwined records.

DHS response:
The department agrees with this recommendation.

The department commenced a programme of work to address intertwined records in early 2014. This work will build on existing automated reports that identify possible duplicate records, and includes:

- undertaking a comprehensive analysis of the Consumer Directory to identify and analyse the extent of intertwined records by June 2014;
- cleansing the Consumer Directory of any intertwined records identified by September 2014;
- reviewing customer service procedures for core functions which are identified as risk points for the creation of intertwined records by October 2014; and
- establishing an escalation framework to capture intertwined records at the time of creation to allow for prompt corrective action, by December 2014.

Recommendation No.3
To further improve the completeness, accuracy and reliability of Medicare customer data, the ANAO recommends that Human Services undertake targeted, risk-based data integrity testing of Medicare customer records.

DHS response:
The department agrees with this recommendation.

The department currently has a comprehensive programme of monitoring customer claiming activities using a variety of mechanisms. This includes a data mining system that monitors and analyses customer claiming to identify unusual claims activity and a programme of payment accuracy review. The department will further enhance and strengthen this programme by commencing targeted testing of Medicare customer data by 1 July 2014.

Recommendation No.4
To ensure that only those customers eligible to receive Medicare benefits can access them, the ANAO recommends that Human Services review existing entitlement types and implement controls where relevant, to:

- prevent instances of customers being enrolled under invalid entitlement types and accessing Medicare benefits without an entitlement; and
- ensure mandatory data fields are completed, and that data entries are consistent with business and system rules.

DHS response:
The department agrees with this recommendation.

The department has a range of checks and controls to prevent customers being enrolled under invalid entitlement types. These include system controls to verify entitlement types. Our review activity and strengthening of controls will be supported even further by the other recommendations in this report.

Recommendation No.5
To ensure compliance with the mandatory requirements of the Information Security Manual, the ANAO recommends that Human Services:

- undertake a review of existing documentation and finalise all mandated security documents; and
- complete the mandated certification and accreditation processes for the systems that record, process and store Medicare customer data and the ICT infrastructure that supports them.

DHS response:
The department agrees with this recommendation.

A review of existing documentation has been completed with all mandatory security documents finalised. The mandatory certification and accreditation processes consist of several components and the requirement for certification and accreditation will be completed by 30 June 2014.

3

Summary of comments for the report

The Department of Human Services welcomes this report and agrees with the five ANAO audit report recommendations. The department recognises that the audit highlights several opportunities to further strengthen and enhance the management and integrity of the Medicare customer data and is strongly committed to ensuring the ongoing completeness, accuracy and reliability of customer records.

The department also notes acknowledgement by the ANAO of its well-developed Privacy and Quality Assurance Frameworks, and the high degree of integrity in the unique customer reference numbers within the Consumer Directory.

Index

Series Titles

ANAO Audit Report No.1 2013–14
Design and Implementation of the Liveable Cities Program
Department of Infrastructure and Transport

ANAO Audit Report No.2 2013–14
Administration of the Agreements for the Management, Operation and Funding of the Mersey Community Hospital
Department of Health and Ageing
Department of Health and Human Services, Tasmania
Tasmanian Health Organisation – North West

ANAO Audit Report No.3 2013–14
AIR 8000 Phase 2 — C-27J Spartan Battlefield Airlift Aircraft
Department of Defence

ANAO Audit Report No.4 2013–14
Confidentiality in Government Contracts: Senate Order for Departmental and Agency Contracts (Calendar Year 2012 Compliance)
Across Agencies

ANAO Audit Report No.5 2013–14
Administration of the Taxation of Personal Services Income
Australian Taxation Office

ANAO Audit Report No.6 2013–14
Capability Development Reform
Department of Defence

ANAO Audit Report No.7 2013–14
Agency Management of Arrangements to Meet Australia's International Obligations
Across Agencies

ANAO Audit Report No.8 2013–14
The Australian Government Reconstruction Inspectorate's Conduct of Value for Money Reviews of Flood Reconstruction Projects in Queensland
Department of Infrastructure and Regional Development

ANAO Audit Report No.9 2013–14
Determination and Collection of Financial Industry Levies
Australian Prudential Regulation Authority
Department of the Treasury

ANAO Audit Report No.10 2013–14
Torres Strait Regional Authority — Service Delivery
Torres Strait Regional Authority

ANAO Audit Report No.11 2013–14
Delivery of the Filling the Research Gap under the Carbon Farming Futures Program
Department of Agriculture

ANAO Report No.12 2013–14
2012–13 Major Projects Report
Defence Materiel Organisation

ANAO Audit Report No.13 2013–14
Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2013
Across Agencies

ANAO Audit Report No.14 2013-14
Explosive Ordnance and Weapons Security Incident Reporting
Department of Defence

ANAO Audit Report No.15 2013–14
The Indigenous Land Corporation's Administration of the Land Acquisition Program
Indigenous Land Corporation

ANAO Audit Report No.16 2013–14
Administration of the Smart Grid, Smart City Program
Department of the Environment
Department of Industry

ANAO Audit Report No.17 2013–14
Administration of the Strengthening Basin Communities Program
Department of the Environment

ANAO Audit Report No.18 2013–14
Administration of the Improving Water Information Program
Bureau of Meteorology

ANAO Audit Report No.19 2013–14
Management of Complaints and Other Feedback
Australian Taxation Office

ANAO Audit Report No.20 2013–14
Management of the Central Movement Alert List: Follow-on Audit
Department of Immigration and Border Protection

ANAO Report No.21 2013–14
Pilot Project to Audit Key Performance Indicators

ANAO Report No.22 2013–14
Air Warfare Destroyer Program
Department of Defence
Defence Materiel Organisation

ANAO Report No.23 2013–14
Policing at Australian International Airports
Australian Federal Police

ANAO Report No.24 2013–14
Emergency Defence Assistance to the Civil Community
Department of Defence

ANAO Report No.25 2013–14
Management of the Building Better Regional Cities Program
Department of Social Services
Department of the Environment

ANAO Report No.26 2013–14
Medicare Compliance Audits
Department of Human Services

ANAO Report No.27 2013–14
Integrity of Medicare Customer Data
Department of Human Services

Better Practice Guides

The following Better Practice Guides are available on the ANAO website:

Implementing Better Practice Grants Administration	Dec. 2013
Human Resource Management Information Systems: Risks and controls	June 2013
Preparation of Financial Statements by Public Sector Entities	June 2013
Public Sector Internal Audit: An investment in assurance and business improvement	Sept. 2012
Public Sector Environmental Management: Reducing the environmental impacts of public sector operations	Apr. 2012
Developing and Managing Contracts: Getting the right outcome, achieving value for money	Feb. 2012
Public Sector Audit Committees: Independent assurance and advice for chief executives and boards	Aug. 2011
Fraud Control in Australian Government Entities	Mar. 2011
Strategic and Operational Management of Assets by Public Sector Entities: Delivering agreed outcomes through an efficient and optimal asset base	Sept. 2010
Planning and Approving Projects – an Executive Perspective: Setting the foundation for results	June 2010
Innovation in the Public Sector: Enabling better performance, driving new directions	Dec. 2009
SAP ECC 6.0: Security and control	June 2009
Business Continuity Management: Building resilience in public sector entities	June 2009
Developing and Managing Internal Budgets	June 2008
Agency Management of Parliamentary Workflow	May 2008
Fairness and Transparency in Purchasing Decisions: Probity in Australian Government procurement	Aug. 2007
Administering Regulation	Mar. 2007
Implementation of Programme and Policy Initiatives: Making implementation matter	Oct. 2006