The Auditor-General
Auditor-General Report No.5 2026–27
Performance Audit

Artificial Intelligence and Medicare Benefits Integrity

Department of Health, Disability and Ageing

Australian National Audit Office

ISSN 1036–7632 (Print)
ISSN 2203–0352 (Online)
ISBN 978-1-76192-057-8 (Print)
ISBN 978-1-76192-058-5 (Online)

Chief Operating Officer
Corporate Management Group
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Or via email:
communication@anao.gov.au.

Australian National Audit Office

Canberra ACT

21 September 2026

Dear President
Dear Mr Speaker

In accordance with the authority contained in the *Auditor-General Act 1997*, I have undertaken an independent performance audit in the Department of Health, Disability and Ageing. The report is titled *Artificial Intelligence and Medicare Benefits Integrity.* 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

Dr Caralee McLiesh PSM
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 their 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:
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Phone: (02) 6203 7300
Email: ag1@anao.gov.au

Auditor-General reports and information about the ANAO are available on our website:
http://www.anao.gov.au

Audit team

Dr Vivian Turner
Benjamin Foreman
Benjamin Siddans
Qing Xue
Nathan Daley
Christine Chalmers

Contents

Audit snapshot

Auditor-General Report No.5 2026–27

Artificial Intelligence and Medicare Benefits Integrity

Why did we do this audit?

- In 2024–25, Medicare Benefits Schedule (MBS) benefits and Pharmaceutical Benefits Scheme expenditure totalled over $52 billion. A 2023 review estimated the cost of MBS health provider non-compliance to be $1.5 to $3 billion.
- The audit was conducted to provide assurance to the Parliament as to whether the Department of Health, Disability and Ageing (DHDA) is effectively managing artificial intelligence (AI) use in supporting health provider compliance.

Key facts

- DHDA has identified that AI is already in use in healthcare settings; for example, in disease screening; residential aged care; use of scribes; supporting clinical decisions; surgical tools; and medical records.
- DHDA used an AI-enabled model to detect potential MBS health provider fraud and non-compliance from July 2024 to December 2025.

What did we find?

- DHDA's arrangements to manage AI use at an enterprise level are largely effective. Arrangements for managing AI use to support health provider compliance are partly effective.
- DHDA has assessed risks and established governance arrangements for its own AI use, but assurance could be stronger. DHDA is starting to consider the risks of AI use by health providers, including in MBS claiming, but has not yet systematically assessed and managed these risks. Given the pace of AI adoption, DHDA could be more proactive.
- DHDA makes little use of AI for managing health provider compliance. An MBS fraud and non-compliance detection system pre-dated whole-of-government AI requirements but was not implemented fully in line with better practice. DHDA has not assessed whether AI could strengthen compliance activity, which is limited relative to the estimated cost of non-compliance.

What did we recommend?

- There were three recommendations to DHDA related to managing risks of AI in healthcare settings; improving AI use case governance; and strengthening assurance over AI use, including cyber security risks.
- DHDA agreed to all three recommendations.

3,779

Identified cases of MBS fraud and non-compliance in 2024–25.

8

Potential fraud or non-compliance cases identified using, in part, the AI model.

$5.2 million

Estimated value of potential fraud or non-compliance identified using, in part, the AI model.

Summary and recommendations

Background

1. The Medicare Benefits Schedule (MBS), Pharmaceutical Benefits Scheme (PBS) and Child Dental Benefits Schedule (CDBS) are Australian Government healthcare programs providing subsidies for healthcare services and medicines. Health providers and pharmacists make claims to the Australian Government for services and products provided under the MBS, PBS and CDBS. In 2024–25, MBS and CDBS benefits and PBS expenditure totalled over $52 billion.

2. The Department of Health, Disability and Ageing's (DHDA) purpose is to 'support the Government to lead and shape Australia's health, disability and aged care systems through evidence-based policy, well-targeted programs and best practice regulation.'[1] DHDA manages the MBS, PBS and CDBS with Services Australia. Through portfolio budget statements Program 2.6 (Health Benefit Compliance), DHDA aims to '[s]upport the integrity of health benefit claims through prevention, early identification and treatment of incorrect claiming, inappropriate practice and fraud.'[2] The Benefits Integrity Division within DHDA is responsible for managing health provider compliance.

3. In August 2023 DHDA began developing a MBS fraud and non-compliance detection system to identify potential MBS fraud and serious non-compliance by analysing provider claiming data. The MBS fraud and non-compliance detection system is comprised of six models covering different claiming behaviours or characteristics. One of the six models was considered by DHDA to be an artificial intelligence (AI)-enabled model, with the remaining five models using standard statistical modelling. The AI-enabled model was in use from July 2024 to December 2025.

4. AI has the potential to impact multiple facets of healthcare and is already in use in healthcare settings; for example, in disease screening; residential aged care; use of scribes[3]; supporting clinical decisions; surgical tools; and medical records.

5. The Australian Government has stated that AI has the potential to enhance Australia's wellbeing, quality of life and economic growth.[4] In its *Data and Digital Government Strategy* published in December 2023, the government committed to adopting AI to 'improve user experience, support evidence-based decisions and gain efficiencies in agency operations' and to equip entities to safely engage with emerging technologies, including AI.[5]

---

1 Department of Health, Disability and Ageing, *Corporate Plan 2025–26*, DHDA, Canberra, 2025, p. 6, available from https://www.health.gov.au/resources/publications/corporate-plan-2025-26 [accessed 12 May 2026].

2 Department of Health, Disability and Ageing, *Department of Health, Disability and Ageing 2024–25 Annual Report*, DHDA, Canberra, November 2025, pp. 100–103, available from https://www.health.gov.au/resources/publications/department-of-health-disability-and-ageing-2024-25-annual-report [accessed 12 May 2026]

3 Digital scribes or AI scribes are tools which capture conversations between patients and healthcare practitioners. These tools generate clinical notes, summaries and documents which may be added to patient records. Scribes can use a range of technologies including AI.

4 Department of Industry, Science and Resources, *Safe and responsible AI in Australia Consultation — Australian Government's interim response*, DISR, Canberra 2024, p. 4, available from https://consult.industry.gov.au/supporting-responsible-ai [accessed 12 May 2026].

5 Australian Government, *Data and Digital Government Strategy*, Australian Government, Canberra, December 2023, pp. 16 and 20, available from https://www.dataanddigital.gov.au/strategy [accessed 12 May 2026].

The *2025 Implementation Plan* for the *Data and Digital Government Strategy* describes AI as a 2026 government priority.[6] Australian Government requirements and guidance for AI governance and management within the Australian Public Service (APS) are evolving. The *Policy for the responsible use of AI in government* took effect on 1 September 2024 and the *AI Plan for the Australian Public Service* was released in November 2025.[7]

Rationale for undertaking the audit

6. Artificial intelligence is an emerging technology that is increasingly used by the APS and in healthcare settings. AI offers the promise of better services, enhanced productivity and efficiency, but has the potential for increased risk and unintended consequences. Between July 2024 and December 2025, DHDA used an AI-enabled model to detect potential health provider fraud and non-compliance in the MBS.

7. In 2024–25, MBS and CDBS benefits and PBS expenditure totalled over $52 billion. A March 2023 *Independent Review of Medicare Integrity and Compliance* estimated that the value of health provider non-compliance could be in the range of $1.5 to $3 billion.[8]

8. This audit continues the ANAO's work in examining the governance of emerging technologies and is the ANAO's second audit[9] examining the administration of specific AI systems against the *Technical standard for government's use of artificial intelligence*.[10] It provides independent assurance to the Parliament as to whether DHDA is effectively managing AI risks associated with health provider compliance, including risks to programs DHDA manages.

Audit objective and criteria

9. The objective of this audit was to assess the effectiveness of DHDA's management of AI use in supporting health provider compliance. To form a conclusion against the objective, the ANAO examined the following criteria:

- Did DHDA have appropriate governance arrangements supporting its adoption of AI?
- Did DHDA have fit-for-purpose assurance arrangements over the adoption of AI by health providers?
- Did DHDA have fit-for-purpose arrangements for the design, development and deployment of AI models for managing health provider non-compliance?
- Was DHDA effectively monitoring and reporting the impact of its use of AI?

6 Australia Government, *2025 Implementation Plan*, Australian Government, November 2025, available from https://www.dataanddigital.gov.au/implementation-plan/2025 [accessed 12 May 2026].

7 Appendix 4 of Auditor-General Report No.43 2025–26 *Artificial Intelligence Use in IP Australia* details the policy's mandatory requirements, available from https://www.anao.gov.au/work/performance-audit/artificial-intelligence-use-ip-australia [accessed 5 August 2026].

8 Dr Pradeep Philip, *Independent review of Medicare integrity and compliance*, Deloitte Access Economics, March 2023, p. 4, available from https://www.health.gov.au/resources/publications/independent-review-of-medicare-integrity-and-compliance-final-report [accessed 12 May 2026].

9 The first audit was Auditor-General Report No.43 2025–26 *Artificial Intelligence Use in IP Australia.*

10 Digital Transformation Agency, *Australian Government AI technical standard*, DTA, Canberra, August 2025, available from https://www.digital.gov.au/policy/ai/AI-technical-standard [accessed 12 May 2026].

Conclusion

10. DHDA's arrangements to manage AI use at an enterprise level are largely effective. Arrangements for managing AI use to support health provider compliance are partly effective. DHDA is establishing governance arrangements that are largely fit for purpose to support AI adoption across the department, in line with whole-of-government requirements. Assurance arrangements are developing and could be strengthened to provide greater visibility over whether AI is being used in line with legal, policy and departmental requirements.

11. DHDA has begun considering risks from AI use in healthcare settings, including in health provider benefits claiming, but has not systematically identified, assessed and treated these risks. Given the pace of change, accelerating this work would better position DHDA to manage risks to benefits integrity, cyber security and other departmental objectives.

12. DHDA makes limited use of AI to manage health provider compliance, and its compliance activity is small relative to the estimated cost of MBS health provider non-compliance. DHDA has not assessed the costs and benefits of using AI to strengthen its compliance activity.

13. The primary AI use case examined in this audit — the MBS fraud and non-compliance detection system — pre-dated DHDA's current AI governance arrangements and was not developed, deployed or fully assured in line with current AI use case requirements and better practice. If the MBS fraud and non-compliance detection system uses an AI-enabled model in the future, these gaps will need to be addressed under Digital Transformation Agency requirements. Evaluation and performance monitoring of the system has been limited, with eight potential fraud or non-compliance matters referred for preliminary analysis.

Supporting findings

Governance arrangements for artificial intelligence

14. DHDA has appropriate governance arrangements at an enterprise level to support the adoption of AI within the department. Risks have been identified and assessed in many areas of the department; policies and frameworks have been developed; key governance committees have oversight of risks; roles and responsibilities for managing AI risks and implementation have been established; guidance materials exist; and most staff have undertaken training. AI-specific governance arrangements have evolved in response to growing use of AI in the department and the introduction of whole-of-government requirements. While DHDA did not develop AI-specific governance arrangements prior to the implementation of whole-of-government policies, it is progressing the implementation of governance arrangements to align to policy minimum requirements. Specific consideration of risk in relation to the role of AI in managing health provider compliance has been limited. (See paragraphs 2.5 to 2.25)

Artificial intelligence use by health providers

15. DHDA has partly fit-for-purpose risk management and assurance arrangements over the adoption of AI by health providers. AI-enabled software is increasingly available to health providers, including tools that support MBS billing. At a high level, DHDA and other Australian Government entities have identified risks associated with AI use in healthcare settings, including in health provider billing. These AI risks include: potential for bias; erroneous outputs; patient

data exposure; low practitioner AI literacy; insufficient performance monitoring; and patient consent issues. Services Australia has expressed concern to DHDA about providers using AI to test MBS eligibility for multiple items and suggest billing options. DHDA has not yet systematically identified, assessed and established treatments for AI risks. Governance committees have considered some of the risks and further analysis is underway. (See paragraphs 3.4 to 3.19)

Design, development, deployment and assurance of artificial intelligence in the department

16. Arrangements for the design, development and deployment of AI models are maturing.

- DHDA has established processes for use case registration, consideration of ethical risks, information security and privacy assessment that are largely or fully aligned with whole-of-government AI governance requirements. As of April 2026 most registered AI use cases related to Microsoft Copilot.
- DHDA's AI use case assessment process is continuing to develop to meet whole-of-government requirements, some of which are not mandatory until later in 2026 and 2027. DHDA is maturing AI policies and procedures to ensure that legal and cyber security risks are considered and treated, and that the *Technical standard for government's use of artificial intelligence* is applied to use cases.
- DHDA's development and deployment of an AI-enabled MBS fraud and serious non-compliance detection system, which pre-dated new whole-of-government requirements for AI use cases, partly aligned with better practice for AI development and deployment. There was no considered assessment prior to development and deployment of ethical risks, legal risks, data suitability, sensitivity, privacy or cyber security. During development and deployment, there were deficiencies in system validation, approval and monitoring. Process improvements are planned and underway.
- Assurance planning and processes are also developing. Departmental incident management policies have been partly updated to reflect new risks. DHDA has identified some unrestricted and unapproved use of AI, including through an AI stocktake completed in June 2026. There is a draft AI Assurance Framework. As of June 2026 there is incomplete assurance that AI use is being managed within expectations and in accordance with legal and policy frameworks. (See paragraphs 4.5 to 4.26)

Monitoring, evaluating and reporting the impact of artificial intelligence

17. Monitoring, evaluation and reporting on the cost and impact of AI use in the department has been largely limited to a Microsoft Copilot rollout. DHDA considers the evaluation of business area AI use cases to be the responsibility of individual use case owners.

18. Whole-of-government and DHDA AI policies do not require the development of cost-benefit analyses for AI use cases. There has been no analysis of the costs of developing the MBS fraud detection system, including the costs of developing the AI-enabled model within it. There has been some analysis of the system's benefits in terms of new potential fraud matters identified (and potential net recoveries), which does not specifically examine the tangible and intangible benefits of AI use.

19. Eight potential non-compliance or fraud matters were created and referred for preliminary analysis using, in part, the AI-enabled model in the MBS fraud detection system. While ad hoc preliminary performance analysis showed the AI-enabled model was efficacious, it was not used after December 2025, when it was determined that resourcing required for manual assessment of fraud and non-compliance 'signals' could not keep up with the volume of potential matters generated. There was no corresponding assessment of the benefits and costs of this decision. There has been some reporting to governance committees about the performance of the MBS fraud detection system, which has not specifically examined the role of AI in the system. DHDA's compliance activity remains limited relative to the estimated cost of MBS provider non-compliance. (See paragraphs 5.3 to 5.19)

Recommendations

Recommendation no. 1
Paragraph 3.20

The Department of Health, Disability and Ageing work with other government entities and sector stakeholders to identify and assess: the risks associated with the use of artificial intelligence in healthcare settings, including from health providers using artificial intelligence in Medicare Benefits Schedule claiming; whether current regulatory and other controls are effective in mitigating risks; and possible treatments for artificial intelligence risks outside of tolerance.

Department of Health, Disability and Ageing response: *Agreed*

Recommendation no. 2
Paragraph 4.10

The Department of Health, Disability and Ageing strengthen compliance with whole-of-government policy by:

(a) incorporating the consideration of legal risks in revised use case assessment processes;

(b) ensuring that all artificial intelligence systems in use in the department have appropriate authorisation and that security risks are identified, documented, managed and accepted before systems and applications are authorised for use; and

(c) implementing controls to ensure that approval processes for use cases are followed.

Department of Health, Disability and Ageing response: *Agreed*

Recommendation no. 3
Paragraph 4.21

The Department of Health, Disability and Ageing strengthen assurance by:

(a) ensuring its cyber security policies reflect the unique risks posed by artificial intelligence and are updated in a considered way; and

(b) ensuring closure documentation for internal and external reviews and audits is clear, comprehensive and relevant to ensure that decision-makers have full visibility of the basis for closure.

Department of Health, Disability and Ageing response: *Agreed*

Summary of entity response

20. The proposed audit report was provided to DHDA. DHDA's summary response is provided below and the full response is at Appendix 1.

Department of Health, Disability and Ageing

The Department of Health, Disability and Ageing welcomes the audit and acknowledges the ANAO's examination of the governance and use of artificial intelligence, including in the context of Medicare benefits integrity.

The department recognises that artificial intelligence presents both opportunities and emerging risks across the health system and government. As artificial intelligence adoption has increased, the department has strengthened its governance, risk management, assurance and oversight arrangements and will continue to mature these in line with evolving whole-of-government requirements and sector practices. The department agrees with the recommendations and is already undertaking work in several of the areas identified by the ANAO.

Artificial intelligence-related risks arise across policy, regulatory, operational and service delivery contexts. Health providers may use artificial intelligence in ways that are consistent with Medicare requirements. However, artificial intelligence-enabled processes may influence provider behaviour and create new risks. In relation to Medicare benefits integrity, the department's focus remains on preventing and responding to incorrect, inappropriate and fraudulent claiming, regardless of how claims are prepared or submitted. The department will continue to work with Services Australia and other stakeholders through existing Medicare integrity arrangements to identify, assess and respond to emerging program risks and to ensure existing controls remain effective and proportionate.

The department remains committed to supporting the safe, responsible and effective use of artificial intelligence across Australia's health system.

Key messages from this audit for all Australian Government entities

21. Below is a summary of key messages, including instances of good practice, which have been identified in this audit and may be relevant for the operations of other Australian Government entities.

Governance and risk management

- Experimentation with new technologies can uncover opportunities for improvement in regulatory effectiveness and efficiency. Benefits measurement is important in determining which opportunities merit further exploration or investment. Tangible and intangible benefits can be compared to costs to help determine if the investment represents value for money. This requires planning; analysis; documentation; and reporting back to decision-makers.
- The AI lifecycle includes conception, development, testing, deployment, use and retirement. AI assurance mechanisms need to take account of all lifecycle stages.
- Government policy requires entities to update existing policies to incorporate the new risks posed by AI. Meaningful updates will attempt to anticipate and respond to how AI could uniquely disrupt business continuity.
- In addition to establishing fit-for-purpose governance arrangements for an entity's AI use cases, entities should be alert to how AI is affecting, enabling or disrupting key external stakeholders including service recipients, third-party providers, and intermediaries. In the context of rapid societal change, entities' risk assessment and treatment need to keep pace.
- AI is increasingly embedded within software programs and accessible through web browsers, creating risks to entity data and increasing the potential for inappropriate or unintended use. Entities need visibility over AI use, clear policies, effective training and communication, and assurance activities that monitor AI use and test whether controls are operating effectively. Leaders play an important role in setting expectations and promoting a culture of responsible AI use, so that staff understand their obligations and are equipped to identify and manage risks associated with AI-enabled tools.

Audit findings

1. Background

Introduction

1.1 Artificial intelligence (AI) is increasingly becoming part of everyday lives, including in the work of the Australian Public Service (APS). AI has the potential to impact multiple facets of healthcare and is already in use in healthcare settings; for example, in disease screening; residential aged care; use of scribes[11]; supporting clinical decisions; surgical tools; and medical records.

1.2 The Australian Government has adopted the Organisation for Economic Co-operation and Development definition of an AI system.

> An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions, that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.[12]

1.3 The government has stated that AI has the potential to enhance Australia's wellbeing, quality of life and economic growth.[13] In its *Data and Digital Government Strategy*, published in December 2023, the government committed to adopting AI to 'improve user experience, support evidence-based decisions and gain efficiencies in agency operations' and to equip entities to safely engage with emerging technologies, including AI.[14] The *2025 Implementation Plan* for the *Data and Digital Government Strategy* describes AI as a 2026 government priority.[15] The *AI Plan for the Australian Public Sector* sets out the path to accelerating the adoption of AI across the public sector through leveraging the technology to allow officials to unlock productivity gains.[16,17]

1.4 AI encompasses four specialised domains (see Figure 1.1).[18]

- Generative AI is focused on creating new content such as text, images, video, code or data using patterns from data already learnt. An example of generative AI is a large language model. Widely used large language models include ChatGPT, Google Gemini and Microsoft 365 Copilot.

11 Digital scribes or AI scribes are tools which capture conversations between patients and healthcare practitioners. These tools generate clinical notes, summaries and documents which may be added to patient records. Scribes can use a range of technologies including AI.

12 Organisation for Economic Co-operation and Development, *Recommendation of the Council on Artificial Intelligence* [Internet], OECD, amended 3 May 2024, available from https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 [accessed 12 May 2025].

13 DISR, *Safe and responsible AI in Australia Consultation — Australian Government's interim response*, p. 4.

14 Australian Government, *Data and Digital Government Strategy*, pp. 16 and 20.

15 Australia Government, *2025 Implementation Plan*.

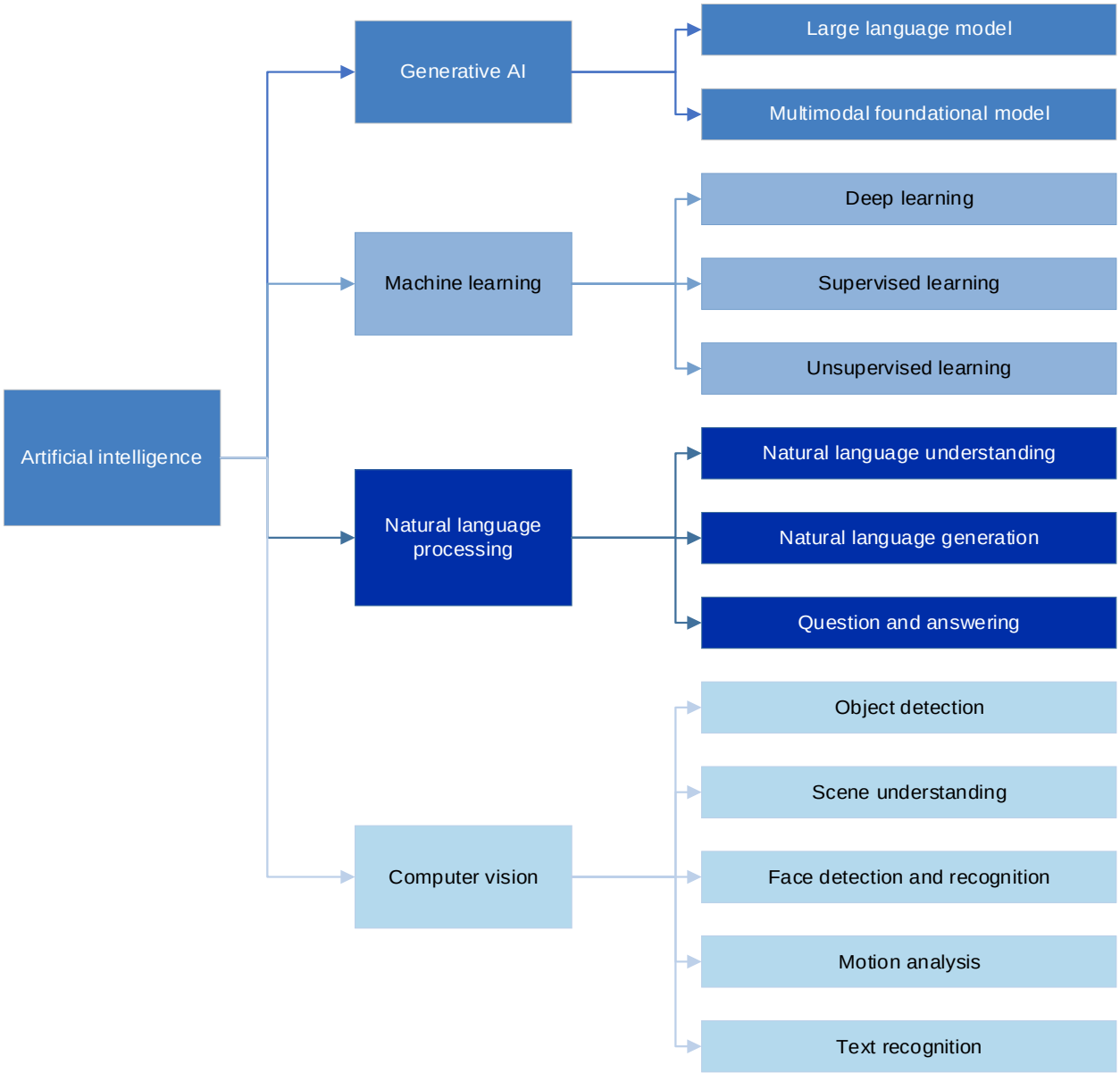
16 Digital Transformation Agency, *AI Plan for the Australia Public Service 2025*, DTA, November 2025, available from https://www.digital.gov.au/policy/ai/australian-public-service-ai-plan-2025 [accessed 12 May 2026].

17 Appendix 3 of Auditor-General Report No.43 2025–26 *Artificial Intelligence Use in IP Australia* provides a timeline of key Australian Government and Parliamentary AI initiatives.

18 Digital NSW, *A common understanding: simplified AI definitions from leading standards* [Internet], available from https://www.digital.nsw.gov.au/policy/artificial-intelligence/a-common-understanding-simplified-ai-definitions-from-leading [accessed 12 May 2026].

- Machine learning involves algorithms learning patterns from data that improve over time without the need for explicit programming, for the purposes of making predictions or decisions. An example of machine learning is an algorithm that predicts the movies a user of a streaming service might like based on movies they have already watched.
- Natural language processing enables a computer to process and generate human language. An example is translation features on a computer or chatbots.
- Computer vision enables a computer to process and interpret visual information such as images or camera feeds. Applications include facial recognition and self-driving cars.

Figure 1.1: Specialised artificial intelligence domains



Source: Adapted by the ANAO from Digital NSW, *A common understanding: simplified AI definitions from leading standards* [Internet], available from https://www.digital.nsw.gov.au/policy/artificial-intelligence/a-common-understanding-simplified-ai-definitions-from-leading [accessed 12 May 2025].

1.5 AI systems differ in their technical characteristics, intended purposes and deployment contexts, resulting in varying levels and types of risk. Australian Government guidance and assurance frameworks recognise that generative AI, automated decision-making[19] and safety critical applications such as clinical or regulatory decision support, present distinct risks, including differences in transparency, predictability, potential for misuse and consequences of failure. Entities using different types of AI need to identify, assess and treat the specific risks and potential impacts of the AI they implement, rather than applying uniform requirements across all AI uses. Box 1 outlines the differences between an AI model, tool, system and use case.

Box 1: Key terms used in this audit

AI model — a mathematical or logical representation used within an AI system to generate outputs such as predictions, content or decisions from input data.

AI tool — a software application or service that provides users access to AI system capabilities to perform tasks or support decision-making. An AI tool typically operates in a standalone fashion and is focused on a specific task.

AI system — a machine-based system that, for explicit or implicit objectives, infers from the inputs it receives how to generate outputs such as predictions, content, recommendations, or decisions. An AI system typically consists of one or more AI models, AI tools, and other supporting applications that allow the system to carry out more complex tasks.

AI use case — a specific application of an AI tool or system(s) to achieve certain objectives or perform certain tasks. An AI tool or system may be used for more than one use case.

Artificial intelligence in the Australian Government sector

1.6 Australian Government requirements and guidance for AI governance and management in the APS are evolving. The *Policy for the responsible use of AI in government* took effect on 1 September 2024 and the *AI Plan for the Australian Public Service* was released in November 2025.[20]

Policy for the responsible use of AI in government

1.7 The government released the *Policy for the responsible use of AI in government* to 'position the Australian Government as an exemplar under its broader safe and responsible AI agenda' and

19 The Senate Select Committee on Adopting AI (see paragraph 1.11) defined automated decision making as: 'the application of automated systems in any part of a decision-making process. [Automated decision making] includes using automated systems to: make the final decision; make an interim assessment or decision leading up to the final decision; recommend a decision to a human decision-maker; guide a human decision-maker through relevant facts, legislation or policy; and automate aspects of the fact-finding process which may influence an interim decision or the final decision'.
Automated decision making may or may not employ AI.
Select Committee on Adopting Artificial Intelligence (AI), Parliament of Australia, *Select Committee on Adopting Artificial Intelligence (AI),* (2024), para. 1.31, available from https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Adopting_Artificial_Intelligence_AI [accessed 12 May 2025].

20 Appendix 4 of Auditor-General Report No.43 2025–26 *Artificial Intelligence Use in IP Australia* details the policy's mandatory requirements.

'to create a coordinated approach to government's use of AI'.[21] The policy required entities to[22] designate 'accountable officials' by 30 November 2024[23] and publish AI transparency statements by 28 February 2025.[24]

1.8 Version 2.0 of the policy was released on 15 December 2025.[25] Version 2.0 defines an AI use case as: 'a specific application of an AI system or systems to achieve certain objectives or perform certain tasks.' The policy specified that an AI use case is considered 'in-scope' of the policy where any of the following apply.

- The use, misuse or failure of AI could lead to more than insignificant harm to individuals, communities, organisations, the environment or the collective rights of cultural groups including First Nations peoples.
- The use of AI will materially influence administrative decisions that affect individuals, communities, organisations, the environment or the collective rights of cultural groups including First Nations peoples.
- It is possible the public will directly interact with, or be significantly impacted by, the AI or its outputs without human review.
- The AI is designed to use personal or sensitive data or security classified information.
- It is deemed an elevated risk AI use case as directed by the [Digital Transformation Agency].[26]

1.9 Version 2.0 of the policy required entities to develop a strategic approach to AI adoption within six months of the policy coming into effect (that is, by 15 June 2026) and implement training and governance arrangements for AI use cases within 12 months of the policy coming into effect (that is, by 15 December 2026).

AI Plan for the Australian Public Service

1.10 The *AI Plan for the Australian Public Service* outlines a series of objectives for government, including to improve AI literacy, drive AI adoption through a coordinated approach and lead by

21 Digital Transformation Agency, *Policy for the responsible use of AI in Government*, version 1.1, DTA, Canberra, September 2024, pp. 4–5, available from https://www.digital.gov.au/ai/policy/download [accessed 12 May 2026].

22 The policy is mandatory for non-corporate Commonwealth entities, except for entities in the Defence portfolio and the national intelligence community. Corporate Commonwealth entities are encouraged to apply the policy.

23 Accountable officials must: be accountable for implementation of the policy within their entities; notify the Digital Transformation Agency where the entity has identified a new high-risk use case; be a contact point for whole-of-government AI coordination; engage in whole-of-government AI forums and processes; and keep up to date with changing requirements.

24 This statement must provide the public with relevant information about the entity's use of AI including information on: compliance with the policy; measures to monitor the effectiveness of deployed AI systems; and efforts to protect the public against negative impacts.

25 Digital Transformation Agency, *Policy for the responsible use of AI in government*, version 2.0, DTA, Canberra, December 2025, available from https://www.digital.gov.au/ai/ai-in-government-policy [accessed 12 May 2026].

26 ibid., p. 22.

example. The plan requires that entities appoint Chief AI Officers by July 2026 to promote adoption of AI and encourage collaboration across the public service.[27]

Previous reviews and audits relating to the governance of artificial intelligence

1.11 The Senate Select Committee on Adopting AI tabled its report in November 2024, which made 13 recommendations including that the Australian Government: introduce new legislation to regulate high risk uses of AI; increase support for sovereign AI capability in Australia; extend and apply the existing work health and safety legislative framework to the workplace risks posed by AI adoption; and introduce a right for individuals to request information on how substantially automated decisions with legal or other significant effects are made.[28] The Australian Government's April 2026 response stated that it would: support sustainable AI infrastructure; support the growth of Australia's AI ecosystem and the widespread responsible adoption of AI; prevent and mitigate AI harm; build a workforce ready for a future enabled by AI; support the creative sector during the AI age; ensure the transparent use of automated decision-making by the government to improve public services; and expand digital literacy to safeguard elections in Australia.[29]

1.12 The Joint Committee of Public Accounts and Audit (JCPAA) conducted an inquiry into the use and governance of AI systems by public sector entities, and tabled its report in February 2025.[30] The report made four recommendations relating to collecting data on the use and understanding of AI in the APS; convening a whole-of-government working group; establishing a Joint Committee on Artificial Intelligence and Emerging Technologies; and Digital Transformation Agency guidance. The Chair of the JCPAA noted the need for effective and coordinated governance frameworks for AI systems within the APS. The government had not responded to the report as of August 2026.

1.13 Auditor-General Report No.22 2024–25 *Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2024* stated that during 2023–24:

> 64 per cent of entities that used AI had also established internal policies governing the use of AI (2022–23: 44 per cent). Twenty-seven per cent of entities had established internal policies regarding assurance over AI use.[31]

---

27 Digital Transformation Agency, *AI Plan for the Australia Public Service 2025*, p. 19; and Department of Finance, *Establishing Chief AI Officers for the APS* [Internet], Finance, Canberra, December 2025, available from https://www.finance.gov.au/about-us/news/2025/establishing-chief-ai-officers-aps [accessed 12 May 2026].
The Department of Finance guidance states that the Chief AI Officer is 'expected to be existing senior leaders in their agency, separate to the Accountable Official where possible.'

28 Select Committee on Adopting Artificial Intelligence (AI), *Select Committee on Adopting Artificial Intelligence (AI)*.

29 Department of Industry, Science and Resources, *Australian Government response to the Senate Select Committee on Adopting Artificial Intelligence (AI) report: Final Report and Interim Report*, DISR, Canberra, April 2026, available from https://www.aph.gov.au/Parliamentary_Business/Tabled_Documents/15891 [accessed 12 May 2026].

30 Joint Committee of Public Accounts and Audit, *Inquiry into the use and governance of artificial intelligence systems by public sector entities- 'Proceed with Caution',* (2025), Parliament of Australia, Canberra, available from https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/PublicsectoruseofAI/Report [accessed 12 May 2025].

31 Auditor-General Report No.22 2024–25 *Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2024*, ANAO, Canberra, 2025, para. 10, available from https://www.anao.gov.au/work/financial-statement-audit/audits-of-the-financial-statements-of-australian-government-entities-the-period-ended-30-june-2024 [accessed 12 May 2026].

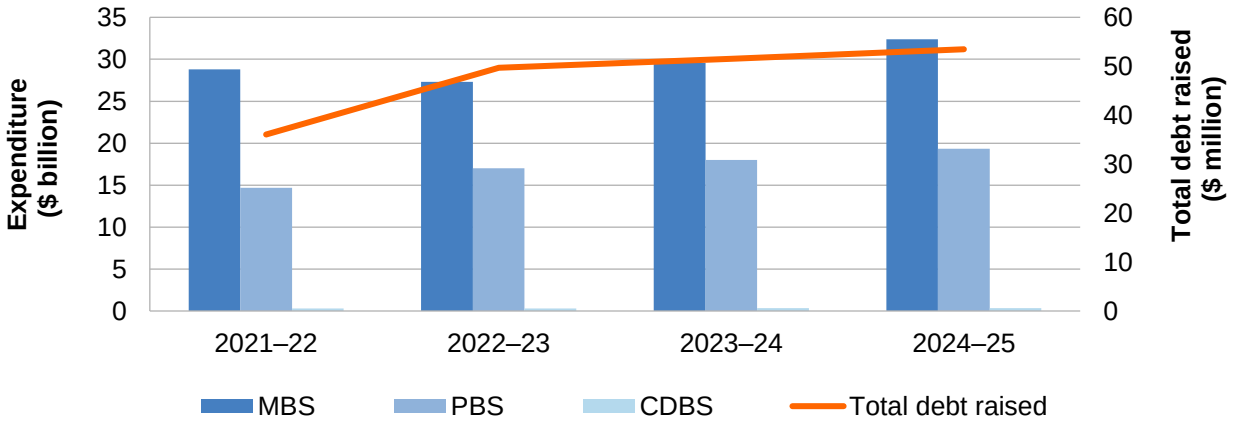
1.14 Auditor-General Report No.26 2024–25 *Governance of Artificial Intelligence at the Australian Taxation Office* assessed the Australian Taxation Office's (ATO) governance of AI at the enterprise level.[32] The audit found the ATO had partly effective arrangements to support the adoption of AI. Auditor-General Report No.43 2025–26 *Artificial Intelligence Use in IP Australia* assessed IP Australia's use of AI in the patent rights process.[33] The audit found that IP Australia had largely effective arrangements with opportunities to further refine and mature governance processes and the monitoring of outcomes from AI.

Management of health provider fraud and non-compliance

1.15 The Department of Health, Disability and Ageing (DHDA) is a non-corporate Commonwealth entity with 7,130 ongoing employees in 2024–25.[34] DHDA's purpose is to 'support the Government to lead and shape Australia's health, disability and aged care systems through evidence-based policy, well targeted programs and best practice regulation.'[35]

1.16 The Medicare Benefits Schedule (MBS), Pharmaceutical Benefits Scheme (PBS) and Child Dental Benefits Schedule (CDBS) are Australian Government healthcare programs providing subsidies for healthcare services and medicines. The MBS lists subsidised services, which include consultations with health practitioners, mental health services, surgical services, diagnostic imaging, eye tests and pathology tests. The PBS lowers the cost of some prescription medicines. The CDBS subsidises basic dental services for eligible children. Depending on the circumstance, a patient, health provider or pharmacist can submit a claim to be paid for services and products provided under the MBS, PBS and CDBS. In 2024–25, MBS and CDBS benefits paid and PBS expenditure totalled over $52 billion (Figure 1.2).

Figure 1.2: MBS and CDBS benefits, PBS expenditure and total debt raised against confirmed cases of MBS, PBS and CDBS fraud or non-compliance



Note: The *Commonwealth Fraud and Corruption Control Framework* defines non-compliance as '[a]ny failure to meet obligations under applicable laws, regulations, agreements, contracts or other requirements. This includes intentional, reckless, negligent, and unintentional acts' and fraud as '[d]ishonestly obtaining (including

32 Auditor-General Report No.26 2024–25 *Governance of Artificial Intelligence at the Australian Taxation Office,* ANAO, Canberra, 2025, available from https://www.anao.gov.au/work/performance-audit/governance-of-artificial-intelligence-the-australian-taxation-office [accessed 12 May 2026].

33 Auditor-General Report No.43 2025–26 *Artificial Intelligence Use in IP Australia*, ANAO, Canberra, 2026.

34 DHDA, *Department of Health, Disability and Ageing 2024–25 Annual Report*, p. 304.

35 DHDA, *Corporate Plan 2025–26*, p. 6.

attempting to obtain) a gain or benefit, or causing a loss or risk of loss, by deception or other means.' DHDA applies these definitions in its *Health Provider Compliance Strategy 2025–26*. See Attorney-General's Department, *Commonwealth Fraud and Corruption Control Framework*, AGD, Canberra, 2024, p. 41, available from https://www.counterfraud.gov.au/library/framework-2024 [accessed 12 May 2026] and Department of Health, Disability and Ageing, *Health Provider Compliance Strategy 2025–26*, DHDA, Canberra, 2025, p. 3, available from https://www.health.gov.au/resources/publications/health-provider-compliance-strategy-2025-30 [accessed 12 May 2026].

Source: ANAO analysis of DHDA advice and data from the following sources: MBS data from Department of Health, Disability and Ageing, *Medicare annual statistics — State and territory (2009–10 to 2024–25)*, DHDA, Canberra, 2025, available from https://www.health.gov.au/resources/publications/medicare-annual-statistics-state-and-territory-2009-10-to-2024-25 [accessed 12 May 2026]; PBS data from Department of Health, Disability and Ageing, *PBS Expenditure and Prescriptions*, DHDA, Canberra, 2025, available from https://www.pbs.gov.au/info/statistics/expenditure-prescriptions/pbs-expenditure-and-prescriptions [accessed 12 May 2026]; and CDBS data from Department of Health, Disability and Ageing, *Dental Benefits Schedule quarterly statistics by state and territory (December quarter 2025–26)*, DHDA, Canberra, 2026, available from https://www.health.gov.au/resources/publications/dental-benefits-schedule-quarterly-statistics-by-state-and-territory-december-quarter-2025-26 [accessed 12 May 2026].

1.17 DHDA and Services Australia manage the MBS, PBS and CDBS.

- DHDA has overall policy responsibility for the MBS, PBS and CDBS. DHDA's responsibilities also include ensuring compliant health provider claiming for Australian Government healthcare program payments. Through portfolio budget statements Program 2.6 (Health Benefit Compliance), DHDA aims to support the integrity of health benefit claims through prevention, early identification and treatment of incorrect claiming, inappropriate practice and fraud.[36] The Benefits Integrity Division within DHDA is responsible for managing health provider compliance.
- Services Australia is responsible for registration of and payments to MBS providers and the administration of provider records. Services Australia provides data to DHDA to support DHDA's health provider compliance activities. Services Australia is responsible for patient compliance with the requirements of the MBS and CDBS.

1.18 DHDA and Services Australia have a compliance protocol (last updated September 2024) detailing the responsibilities of each entity for compliance activities and the sharing of information and intelligence to detect, prevent, investigate and address non-compliance and prosecute fraud. The compliance protocol states that: DHDA has responsibility for health provider compliance; Services Australia provides resources for compliance activities, if required; and that the entities jointly manage identified risks and requirements.

1.19 Auditor-General Report No.17 2020−21 *Managing Health Provider Compliance* examined DHDA's compliance program for the MBS, PBS, and Practice Incentives Program.[37,38] The audit found DHDA's health provider compliance approach was partly effective and made two recommendations: cost health provider compliance activities and improve health benefit compliance performance reporting.

1.20 In November 2022 the *Independent Review of Medicare Integrity and Compliance* (the Philip Review) was established to examine the integrity of the MBS and its compliance mechanisms, and

36 DHDA, *Department of Health, Disability and Ageing 2024–25 Annual Report*, pp. 100–103.

37 Auditor-General Report No.17 2020−21 *Managing Health Provider Compliance,* ANAO, Canberra, 2020, available from https://www.anao.gov.au/work/performance-audit/managing-health-provider-compliance [accessed 12 May 2026].

38 The Practice Incentives Program is aimed at supporting health professionals and practices to deliver quality care, enhance capacity and improve access and health outcomes for patients.

provide an evidence-based estimate of the value of non-compliance and fraud in the MBS.[39] The March 2023 final report made 23 recommendations covering four areas: governance and structure; operational processes; modernising technology; and strengthening legislation. Recommendations included those related to data assets, analysis and linkages; risk-based business rules; and health provider practice management software used for provider claims.[40] The Philip Review estimated that the value of health provider non-compliance could be in the range of $1.5 to $3 billion.[41] DHDA advised the ANAO that in 2024–25, it raised approximately $53.5 million in debt for approximately 7,500 confirmed cases of MBS, PBS and CDBS fraud or non-compliance (Figure 1.2).[42]

1.21 In the 2023–24 federal Budget, $29.8 million was provided over four years for the measure *Strengthening Medicare — improving Medicare integrity*. The majority of the funding was to establish a taskforce to respond to the Philip Review recommendations and introduce analytical tools and methods to identify fraud and serious non-compliance. In the 2026–27 federal Budget, $146.8 million over four years was allocated to: establish enhanced, expanded and ongoing MBS integrity capabilities in DHDA and Services Australia; improve non-compliance and fraud detection, disruption and prevention efforts; and continue responding to the Philip Review recommendations. DHDA advised the ANAO in March 2026 that mechanisms to assess progress on the implementation of the Philip Review recommendations include: an October 2024 'health check'; engagement of Boston Consulting Group[43] from March to July 2025 to develop an improved business model for the Benefits Integrity Division; a June 2025 internal audit[44]; and planning for an evaluation.

1.22 Auditor-General Report No.7 2024−25 *Fraud Control Arrangements in the Department of Health and Aged Care* found DHDA had partly effective fraud control arrangements, with a lack of up-to-date fraud risk assessments at the enterprise level, fraud risk assessments for programs and testing of fraud control effectiveness.[45] The report made five recommendations related to risk assessment, internal audit processes, controls testing, fraud investigator qualifications, and quantification and recording of external fraud loss estimates.

Artificial intelligence and health provider claiming

1.23 An MBS 'claiming channel' is an Australian Government digital pathway or system to allow providers to submit and receive claims. Several MBS claiming channels are integrated with health provider practice management software and have built in validations applied to claims prior to submission to Services Australia to enable full assessment. Services Australia's provider claiming IT system uses business rules to assess MBS, PBS and CDBS claims. The Philip Review recommended

39 Dr Pradeep Philip, *Independent review of Medicare integrity and compliance*.

40 Including closer integration of practice management software with claims assessment rules to avoid unintentional non-compliance with the rules.

41 Dr Pradeep Philip, *Independent review of Medicare integrity and compliance*, p. 4.

42 DHDA states in its 2024–25 Annual Report that 'Education, behaviour changes and upfront preventative system controls are vital to avoid non-compliance' and that 'Additional compliance benefits include behavioural savings of $345.82 million', calculated using an 'agreed methodology'.
DHDA, *Department of Health, Disability and Ageing 2024–25 Annual Report*, pp. 100–101.

43 AusTender contract notice CN4133000-A1 valued at $2,183,500.

44 The audit found there was evidence to support closure of Auditor-General recommendations and progress to address the Philip Review recommendations. Gaps remained in relation to design, delivery and reporting.

45 Auditor-General Report No.7 2024−25 *Fraud Control Arrangements in the Department of Health and Aged Care,* ANAO, Canberra, 2024, available from https://www.anao.gov.au/work/performance-audit/fraud-control-arrangements-the-department-health-and-aged-care-2024 [accessed 12 May 2026].

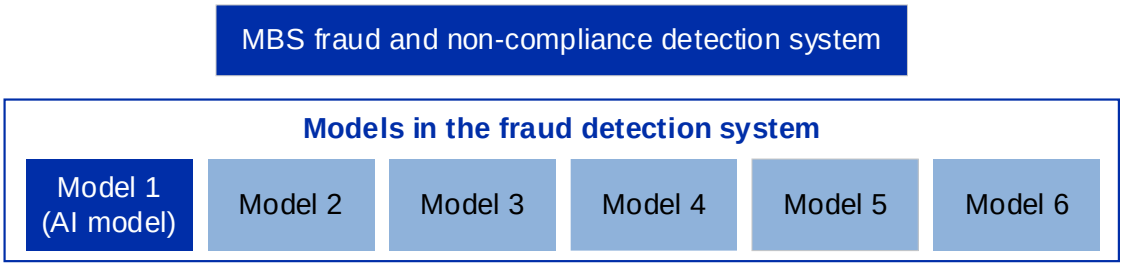
'[i]mplement[ing] enhancements to the end-to-end claiming journey to strengthen the first line of defence position and enable continuous monitoring of all MBS claim transactions.'[46]

1.24 Services Australia's October 2025 AI transparency statement states 'We do not use AI to process claims' and Services Australia advised the ANAO in January 2026 that it was not using AI to manage or monitor provider compliance for the MBS, PBS or CDBS.[47] DHDA advised the ANAO in November 2025 that it was using AI (machine learning models) for the identification of potential health provider non-compliance.[48]

1.25 As part of its broader compliance management approach, in August 2023 DHDA began developing a MBS fraud and non-compliance detection system to detect potential MBS fraud and serious non-compliance through the analysis of provider claiming data. The MBS fraud and non-compliance detection system is comprised of six models covering different claiming behaviours or characteristics (Figure 1.3).

1.26 A November 2024 risk assessment of the MBS fraud and non-compliance detection system (see Table 4.1) stated that models within the MBS fraud and non-compliance detection system can use supervised and unsupervised machine learning models.[49] One of the six models was an AI model, with the remaining five models using standard statistical modelling. The AI-enabled model was in use from July 2024 to December 2025, when the AI technology behind the model was replaced with standard statistical modelling for the same claiming behaviour (see Chapter 5).

Figure 1.3: Use of AI for detecting potential health provider fraud and non-compliance



Note: Model 1 was changed from an AI-enabled model to a standard statistical model in December 2025 but retained the ability to identify the same claiming behaviour/characteristic.

Source: ANAO analysis of DHDA documentation.

1.27 DHDA officials review data from the MBS fraud and non-compliance detection system to identify signals of potential fraud or serious non-compliance. If signals are detected, DHDA officials may conduct a manual preliminary analysis. If concerns about possible fraud or serious

46 Dr Pradeep Philip, *Independent review of Medicare integrity and compliance*, Recommendation 2, p. 10.

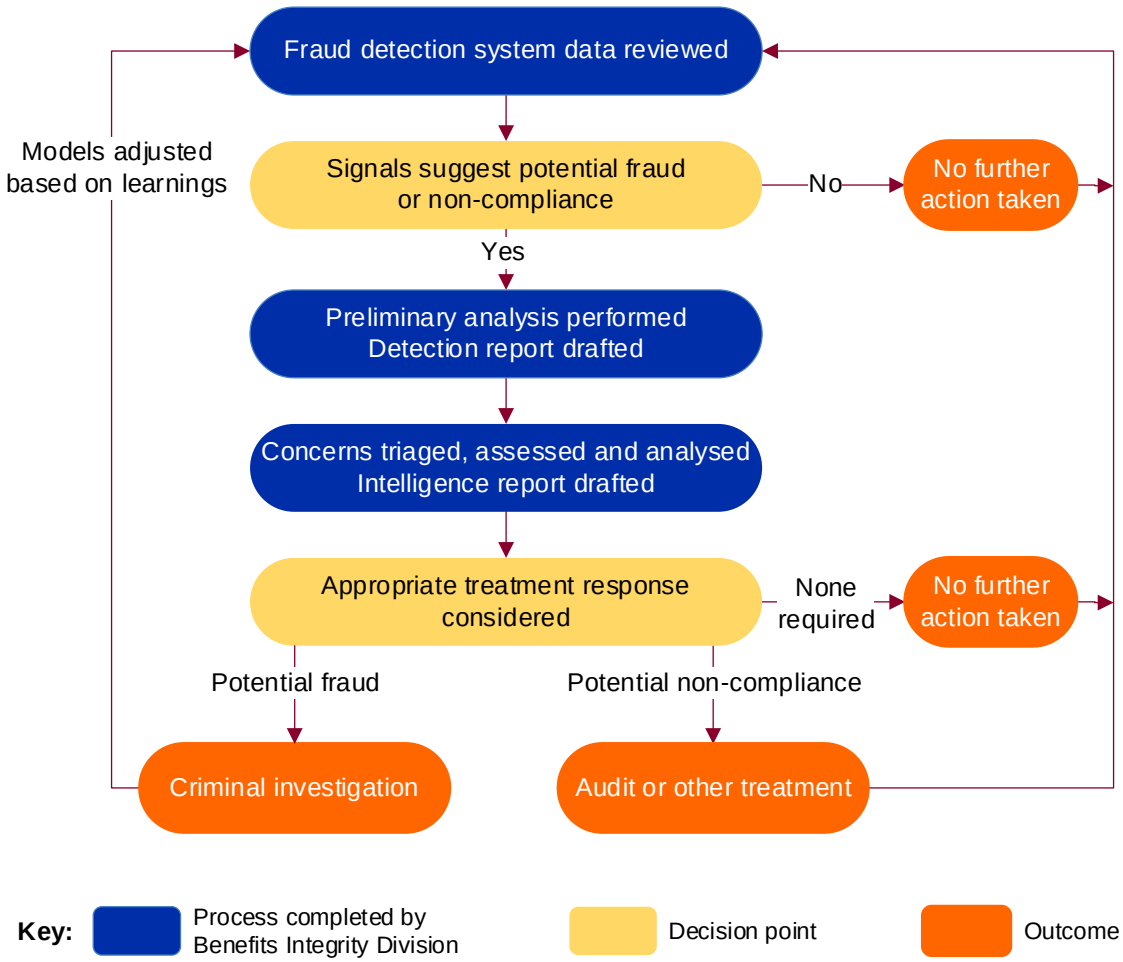
47 Services Australia, *Automation and Artificial Intelligence Transparency Statement* [Internet], Canberra, October 2025, available from https://www.servicesaustralia.gov.au/automation-and-artificial-intelligence-transparency-statement [accessed 12 May 2026].

48 DHDA staff have access to Microsoft 365 Copilot, an AI tool that is integrated with Microsoft Office applications. DHDA has developed six 'low-risk, productivity-enhancing' use cases for Copilot: document summarisation and analysis; content creation and editing; meeting and task management; data insights and visualisation; information extraction and background research; and image generation. DHDA advised the ANAO in January 2026 that the Benefits Integrity Division only uses Copilot for these purposes.

49 Supervised learning involves training an algorithm using labelled data where each input has a corresponding output. Unsupervised learning involves the analysis of unlabelled data to discover hidden patterns, structures or relationships without human guidance.

non-compliance are held following the preliminary analysis, the matter is required to be referred for further analysis and investigation by DHDA officials to determine treatment options (Figure 1.4).

Figure 1.4: Processing of potential fraud or non-compliance signals detected using the MBS fraud and non-compliance detection system



Source: Adapted by ANAO from DHDA documentation.

1.28 The Benefits Integrity Division, which is responsible for managing health provider compliance, is comprised of five branches with differing roles in the end-to-end compliance process. The division had an average staffing level of 358 in April 2026 and an operating budget of $42.77 million for 2025–26.

Rationale for undertaking the audit

1.29 Artificial intelligence is an emerging technology that is increasingly used by the APS and in healthcare settings. AI offers the promise of better services, enhanced productivity and efficiency, but has the potential for increased risk and unintended consequences. Between July 2024 and December 2025, DHDA used an AI-enabled model to detect potential health provider fraud and non-compliance in the MBS.

1.30 In 2024–25, MBS and CDBS benefits and PBS expenditure totalled over $52 billion. A March 2023 *Independent Review of Medicare Integrity and Compliance* estimated that the value of health provider non-compliance could be in the range of $1.5 to $3 billion.[50]

1.31 This audit continues the ANAO's work in examining the governance of emerging technologies and is the ANAO's second audit[51] examining the administration of specific AI systems against the *Technical standard for government's use of artificial intelligence*.[52] It provides independent assurance to the Parliament as to whether DHDA is effectively managing AI risks associated with health provider compliance, including risks to programs DHDA manages.

Audit approach

Audit objective, criteria and scope

1.32 The objective of this audit was to assess the effectiveness of DHDA's management of AI use in supporting health provider compliance. To form a conclusion against the objective, the ANAO examined the following criteria:

- Did DHDA have appropriate governance arrangements supporting its adoption of AI?
- Did DHDA have fit for purpose arrangements for the design, development and deployment of AI models for managing health provider non-compliance?
- Was DHDA effectively monitoring and reporting the impact of its use of AI?
- Did DHDA have fit for purpose assurance arrangements over the adoption of AI by health providers?

1.33 Although Services Australia has a role in managing the MBS, Services Australia advised the ANAO that it does not use AI to manage or monitor health provider non-compliance and was not included in the audit.

Audit methodology

1.34 The audit methodology involved:

- analysis of DHDA and Services Australia documentation;
- review of two public contributions to the audit from peak bodies; and
- meetings and walkthroughs with DHDA officials.

1.35 Australian Government entities largely give the ANAO electronic access to records by consent, in a form useful for audit purposes. For the purposes of this audit, DHDA advised the ANAO that it would not voluntarily provide certain information requested by the ANAO due to concerns about its obligations under the *Privacy Act 1988*, secrecy provisions in DHDA portfolio legislation, confidentiality provisions in contracts and the *Public Interest Disclosure Act 2023*. To provide comfort to the Secretary regarding DHDA's obligations under portfolio legislation, on 28 November 2025 the Auditor-General issued the Secretary of DHDA with a notice to provide

50 Dr Pradeep Philip, *Independent review of Medicare integrity and compliance*, p. 4.

51 The first audit was Auditor-General Report No.43 2025–26 *Artificial Intelligence Use in IP Australia.*

52 DTA, *Australian Government AI technical standard*.

information and produce documents pursuant to section 32 of the *Auditor-General Act 1997*. Under this notice, DHDA agreed to provide the requested information and documents.

1.36 The audit was conducted in accordance with ANAO Auditing Standards at a cost to the ANAO of approximately $337,000.

1.37 The team members for this audit were Dr Vivian Turner, Benjamin Foreman, Benjamin Siddans, Qing Xue, Nathan Daley and Christine Chalmers.

2. Governance arrangements for artificial intelligence

Areas examined

This chapter examines whether the Department of Health, Disability and Ageing (DHDA) has appropriate governance arrangements supporting the adoption of artificial intelligence (AI) in the management of health provider compliance.

Conclusion

DHDA has appropriate governance arrangements at an enterprise level to support the adoption of AI within the department. Risks have been identified and assessed in many areas of the department; policies and frameworks have been developed; key governance committees have oversight of risks; roles and responsibilities for managing AI risks and implementation have been established; guidance materials exist; and most staff have undertaken training. AI-specific governance arrangements have evolved in response to growing use of AI in the department and the introduction of whole-of-government requirements. While DHDA did not develop AI-specific governance arrangements prior to the implementation of whole-of-government policies, it is progressing the implementation of governance arrangements to align to policy minimum requirements. Specific consideration of risk in relation to the role of AI in managing health provider compliance has been limited.

2.1 AI governance is an evolving area, with a common theme that there is no one size-fits-all governance model. The *National framework for the assurance of artificial intelligence* states that '[g]overnance structures should be proportionate and adaptable to encourage innovation while maintaining ethical standards and protecting public interests'.[53] The *Policy for the responsible use of AI in government* is intended to 'complement and strengthen … existing frameworks in use by the [Australian Public Service].'[54]

2.2 Section 16 of the *Public Governance, Performance and Accountability Act 2013* states that 'the accountable authority of a Commonwealth entity must establish and maintain an appropriate system of risk oversight, management and internal control for the entity.' The purpose of the Commonwealth Risk Management Policy is to 'embed risk management into the culture and work practices of entities to improve decision making in order to maximise opportunities and better manage uncertainty'.[55]

2.3 In November 2022 ChatGPT, a large language model chatbot assistant, was publicly released leading to mainstream popularity of AI. Early versions of Microsoft 365 Copilot, also a large language model chatbot assistant, were introduced in February 2023. DHDA rolled out Microsoft 365 Copilot

53 Australian Government et al., *National framework for the assurance of artificial intelligence in government*, Australian Government, Canberra, June 2024, p. 7, see 'Governance', available from https://www.finance.gov.au/government/public-data/data-and-digital-ministers-meeting/national-framework-assurance-artificial-intelligence-government [accessed 12 May 2026].

54 DTA, *Policy for the Responsible use of AI in government*, version 2.0, p. 4.

55 Department of Finance, *Commonwealth Risk Management Policy*, Finance, Canberra, November 2022, available from https://www.finance.gov.au/government/comcover/risk-services/management/commonwealth-risk-management-policy [accessed 12 May 2026].

to staff between August and November 2025 (see paragraph 2.25). In August 2023 DHDA began developing a MBS fraud and non-compliance detection system to detect potential MBS fraud and serious non-compliance through the analysis of provider claiming data. An AI-enabled model was in use in the system from July 2024 to December 2025 (see paragraph 1.26).

2.4 This chapter assesses whether DHDA has fit-for-purpose: enterprise level arrangements to identify and manage risks related to the department's use of AI; and strategic and policy frameworks, governance and training to support AI adoption within the department. Chapter 3 assesses whether DHDA has arrangements to manage risks related to the use of AI by health providers.

Some groups and divisions have identified risks and treatments associated with AI use by DHDA staff and stakeholders and there is active oversight by the Audit and Risk Committee. There has been no specific identification of AI risks by the Benefits Integrity Division.

2.5 DHDA's Risk Management Framework outlines four levels of risk management (enterprise; group; division; and operational) and the responsible person at each level.

Enterprise risks

2.6 DHDA has six enterprise risks: delivery (including programs/projects, policy and regulatory); stakeholders; information technology, cyber security, data and digital services; people; financial; and legal compliance. No enterprise risk description directly refers to AI. DHDA's Risk Management Framework requires: annual review; updates to DHDA's Executive Committee and Audit and Risk Committee; and quarterly review of emerging risks.

2.7 The Executive Committee discussed AI as an emerging area of risk at four of 89 meetings between January 2023 and April 2026 (in July 2024, April 2025, March 2026 and April 2026). In the same period, the Audit and Risk Committee received updates from the Chief Digital Information Officer on AI use across the government and within DHDA, and associated emerging risks, in March 2024, June 2024, June 2025 and September 2025. The Audit and Risk Committee also received: quarterly updates on DHDA Group AI risks (see paragraph 2.9); a February 2025 Readiness for Artificial Intelligence Use internal audit; an Enterprise Fraud and Corruption Risk Assessment, which discussed emerging risks in the fraud and corruption landscape related to the use of AI by 'fraudsters' against DHDA (see paragraph 3.5); and other information on activities related to AI adoption within DHDA.[56]

2.8 The February 2025 internal audit was linked to the 'information technology, cyber security, data and digital services' enterprise risk. The audit recommended considering risks and controls associated with the wider adoption of AI. The Enterprise Fraud and Corruption Risk Assessment suggested investing in advanced AI technologies and infrastructure to better prepare the department.

56 DHDA's Audit and Risk Committee has five members selected for their expertise in public financial management.

Group risks

2.9 DHDA was comprised of seven groups.[57] DHDA's Risk Management Framework states that, at the group level, risk is managed through regular reporting to the Audit and Risk Committee. As of April 2026 three of the groups had identified AI risks.

- The Corporate Operations Group first identified an AI risk in July 2023, which it presented to the Audit and Risk Committee in September 2023. AI was described as having the potential to impact the department positively (efficiency, quality assurance, resource management) and negatively (data security, privacy, bias in decision-making, workforce structure). The risk was reported at eight of 10 subsequent Audit and Risk Committee meetings, with regular updates made to the risk description. In April 2026 the risk was described as:

  Enabling user adoption of emerging technologies such as [AI] may result in unknown security and legal risks due to the complexity and rapidly changing nature of the ICT landscape, insufficient of *[sic]* in-house expertise, and staff inability to identify and manage risks.

- The Health Products Regulation Group first presented an AI risk to the Audit and Risk Committee in September 2025: '[r]apid expansion of … AI-powered activity … contributing to increased pressure on the government to respond in a timely way and ensure the safety of Australians.'
- The Primary Care, Community and First Nations Group[58] first presented an AI opportunity to the Audit and Risk Committee in December 2025: '[t]o increase use of AI technologies to expediate administrative workloads.'
- As of April 2026 the Health Resourcing Group (which includes the Benefits Integrity Division), Ageing and Aged Care Group, Systems Strategy Group[59] and Disability and Carers Group had not identified any AI risks or opportunities in group reporting.

2.10 Treatments identified at the group level for AI risks included additional project resourcing; staff communication, training and education; stakeholder communications; technology certifications and user guidance; establishment of clear roles and responsibilities across groups; establishment of oversight committees; and enhancing and promoting existing data governance forums and processes. Management actions for the Corporate Operations Group AI risk were updated in April 2026 to include new AI governance processes.

Divisional and operational risks

2.11 DHDA's Risk Management Framework requires each division to complete annual business and risk plans. DHDA had 39 2025–26 business and risk plans covering all divisions. Of the 39 plans: five identified a risk related to AI; seven had a priority related to AI; 16 had an opportunity related to AI; and eight listed challenges related to AI. The Benefits Integrity Division listed two opportunities related to AI[60] but no risks, priorities or challenges. The Medicare Benefits and

57 The Health Resourcing Group was disbanded in August 2026, with relevant functions moved to other groups.

58 Prior to March 2026, the Primary Care, Community and First Nations Group was known as the Primary and Community Care Group.

59 Prior to a March 2026, the Systems Strategy Group was known as the Strategy and First Nations Group.

60 The opportunities related to automating and targeting post-payment activities to areas and cases with high risk and uplifting data and technology capabilities to enable contemporary compliance approaches.

Digital Health Division's priority was to 'Lead policy advice on the use of AI in Health care, including consideration of genomics, to support productivity' (see paragraph 3.4). It listed an opportunity and challenge related to the use of AI by health providers, but no AI risks. The Integrity and Assurance Division, which included the Fraud and Integrity Branch until it was moved into the Benefits Integrity Division in February 2026, detailed leveraging AI and digital tools as a priority and opportunity, but did not list any risks.

2.12 Benefits Integrity Division risk reporting at the program and project level does not identify AI risks or treatments.

DHDA is developing governance arrangements for AI that are aligned with whole-of-government requirements.

Artificial intelligence strategy

2.13 Version 2.0 of the *Policy for the responsible use of AI in government* states that government agencies must develop a strategic position on AI adoption within six months of the policy taking effect (that is, by 15 June 2026) and requires agencies to embed responsible AI practices within 12 months of the policy taking effect (that is, by 15 December 2026).[61]

2.14 DHDA's October 2025 AI Strategy and Roadmap outlines: an AI definition; drivers; vision, mission and outcomes; objectives; stakeholder groups and 'personas' (including healthcare providers); implementation priorities; and approach. The implementation priorities (staff AI capability; consultation and collaboration; transparency and trust; responsible AI governance; innovation and value management; and AI technology) map to enterprise risks. The strategy references *AI Ethics Principles.*[62] Staff are required to consider the safe, responsible and ethical use of AI for AI use cases (see Table 4.1).

Artificial intelligence policy

2.15 DHDA drafted an AI policy in January 2026 that aligns with the Department of Industry, Science and Resources' October 2025 *AI policy guide and template*.[63] The draft policy outlines roles and responsibilities; links to other documentation within DHDA; sets policy review frequency; sets out expected behaviours for designing, developing, procuring, deploying or interacting with AI systems; and lists risks and mitigations. The February 2025 internal audit recommended considering the definition and scope of AI and links to existing DHDA objectives, strategies and implementation plans when developing DHDA's policy position on the adoption of AI. DHDA advised the ANAO in May 2026 that the AI policy aligns to this recommendation and was scheduled to be approved by

61 DTA, *Policy for the responsible use of AI in Government*, version 2.0, p. 12.
Version 1.1 (effective September 2024 to 14 December 2025) did not require agencies to develop a strategic position.

62 There are eight *Australian AI Ethics Principles*: human, societal and environmental wellbeing; human-centred values; fairness; privacy protection and security; reliability and safety; transparency and explainability; contestability; and accountability.
Department of Industry, Science and Resources, *Australia's AI Ethics Principles*, DISR, Canberra, December 2025, available from https://www.industry.gov.au/publications/australias-ai-ethics-principles [accessed 12 May 2026].

63 National Artificial Intelligence Centre, *AI policy guide and template*, National AI Centre, Canberra, October 2025, available from https://www.ai.gov.au/staying-safe-and-responsible/essential-ai-practices/create-ai-policy [accessed 12 May 2026].

the Digital Committee in June 2026. As of August 2026 the AI policy had not been finalised and the recommendation had not been closed.

2.16 In January 2026 DHDA drafted an AI grants and procurement policy, the purpose of which was to 'articulate DHDA's expectations for the safe, responsible and ethical use of AI when grantees and suppliers interact with the department.' In June 2026 the draft policy was changed to voluntary 'guidance' and was scheduled to be presented to the Digital Committee in August 2026 for publication on the DHDA website. In response to a February 2025 internal audit recommendation, DHDA completed an AI stocktake in June 2026 (see Table 4.1) that included grantees and suppliers.

Artificial intelligence transparency statement

2.17 Version 1.1 of the *Policy for the responsible use of AI in government* required agencies to make publicly available a transparency statement within six months of the policy taking effect (that is, by 1 March 2025) and review and update the statement annually or sooner.[64] DHDA published an AI transparency statement on its website in May 2025, which it updated in February 2026.[65] DHDA's transparency statement aligns with Digital Transformation Agency (DTA) content requirements. The statements include that DHDA uses AI in policy and legal, scientific, compliance and fraud detection, corporate and enabling, and service delivery domains and that AI will improve service delivery, policy outcomes, efficiency and productivity. The updated statement in February 2026 provided more detailed information on DHDA's AI usage and governance.

2.18 The Benefits Integrity Division does not clearly document AI use. DHDA advised the ANAO in November 2025 that there were 12 machine learning models used in health provider compliance processes. In December 2025 DHDA provided the ANAO with a list of four tools that use AI. In January 2026 there was one AI-enabled model used to monitor health provider non-compliance. In February 2026 DHDA advised the ANAO that the AI-enabled model had been changed to a non-AI logistic regression model[66] in December 2025 (see Chapter 5).

Artificial intelligence governance structure

2.19 DHDA has governance committees that have considered AI risks (see Appendix 3). Between January 2023 and April 2026, the Executive Committee, Digital Committee, AI subcommittee to the Digital Committee, Strategic Business Committee, Medicare Integrity Reform Program Board and Medicare Integrity Reform Steering Group discussed AI risks and the legal and ethical use of AI at some meetings.

2.20 Version 1.1 of the *Policy for the responsible use of AI in government* required entities to designate accountable officials for implementing the policy within 90 days of the policy taking effect (that is, by 1 December 2024). Version 2.0 of the policy required entities to designate an

64 DTA, *Policy for the responsible use of AI in Government*, version 1.1, p. 13;
Digital Transformation Agency, *Standard for AI transparency statements*, DTA, Canberra, 2025, available from https://www.digital.gov.au/ai/ai-in-government-policy/standard-ai-transparency-statements [accessed 12 May 2026].

65 Department of Health, Disability and Ageing, *Artificial intelligence (AI) transparency statement*, DHDA, Canberra, 16 February 2026, available from https://www.health.gov.au/about-us/corporate-reporting/our-commitments/ai-transparency-statement [accessed 12 May 2026].

66 A logistic regression model is a statistical method used to estimate the probability of a binary outcome (such as 'yes' or 'no') based on one or more predictor variables.

accountable official and follow the *Standard for accountability* when doing so.[67] The *Standard for accountability* recommends choosing accountable officials that 'suit the agency context and structure', which could be one or more individuals or roles. The accountable official should have the 'authority and influence to effectively drive the policy's implementation in their agency.' The *AI Plan for the Australian Public Service* required entities to appoint chief AI officers by July 2026 to promote adoption of AI and encourage collaboration across the public service.[68]

- AI accountable official — DHDA initially appointed the Chief Digital Information Officer (CDIO) and Deputy Chair of the Digital Committee as DHDA's 'AI accountable official' and, in accordance with the *Standard for accountability,* advised the DTA of its nomination in November 2024. Guidance from the Department of Finance states that the chief AI officer is 'expected to be existing senior leaders in their agency, separate to the Accountable Official where possible.'[69] In March 2026 the AI subcommittee endorsed the transfer of the AI accountable official role to the First Assistant Secretary of the Information Technology Division.[70]
- Chief AI officer — In June 2026 DHDA appointed the Deputy Secretary for Systems Strategy as DHDA's Chief AI Officer.

2.21 The February 2025 Readiness for Artificial Intelligence Use internal audit recommended considering roles and responsibilities and their intersection with existing processes and working groups, and decision-making authority for the use of AI. DHDA drafted an AI Assurance Framework in October 2025 (see paragraph 4.25), which outlines AI governance roles and responsibilities. These appeared on the DHDA intranet (Figure 2.1). The DTA's *Artificial intelligence impact assessment tool* provides guidance for entities on key personnel responsibilities, including assessors, approvers and experts, for AI impact assessments.[71] DHDA has established the required roles in line with this guidance: an assessing officer (use case Assessing Officer); approving officer (use case Accountable Officer) and expert contributor (Centre of Excellence).

67 Digital Transformation Agency, *Standard for accountability*, DTA, Canberra, December 2025, available from https://www.digital.gov.au/ai/ai-in-government-policy/accountability [accessed 12 May 2026].

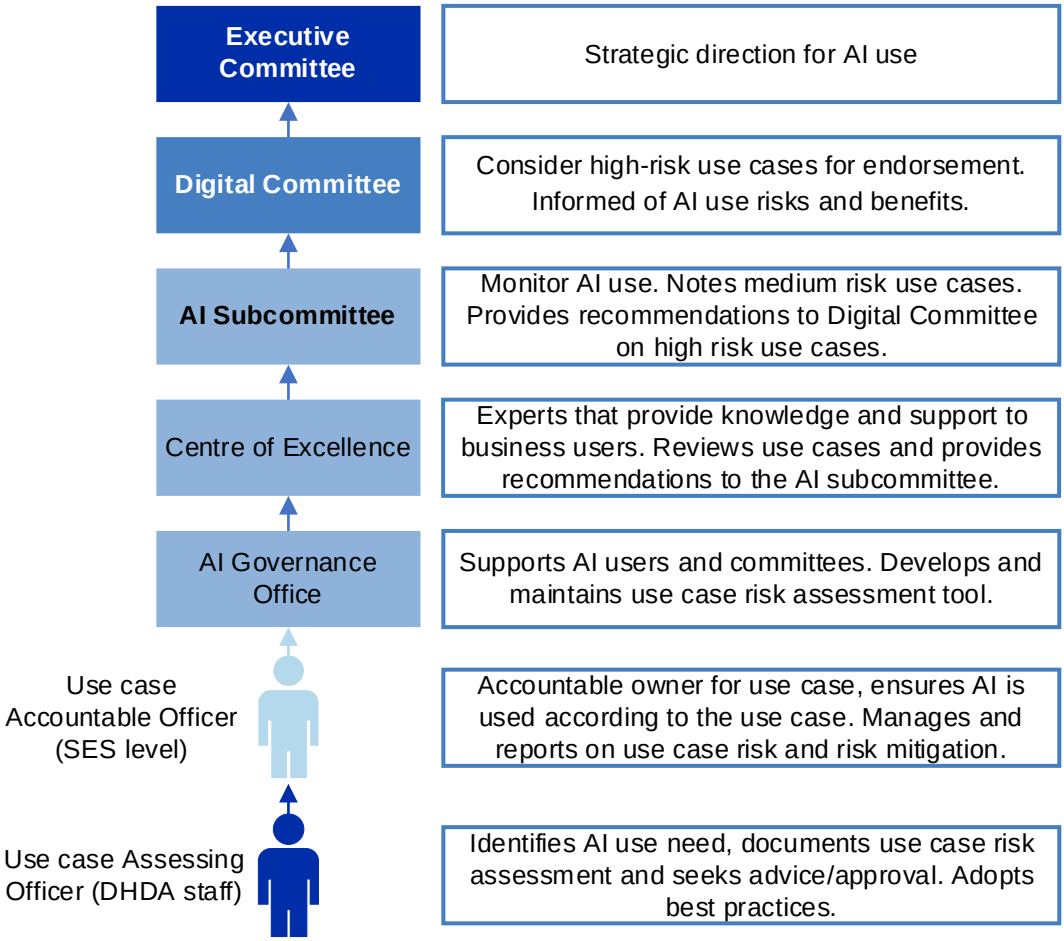
68 DTA, *AI Plan for the Australia Public Service*, p. 19.

69 Finance, *Establishing Chief AI Officers for the APS*.

70 The Chief Digital Information Officer Division and Information Technology Division are separate divisions.

71 Digital Transformation Agency, *Artificial intelligence impact assessment tool*, DTA, Canberra, December 2025, pp. 5–6, available from https://www.digital.gov.au/ai/impact-assessment-tool [accessed 12 May 2026].

Figure 2.1: Draft artificial intelligence governance roles and responsibilities, May 2026



Source: ANAO based on DHDA documentation.

Staff training and communications on artificial intelligence

2.22 Version 1.1 of the *Policy for the responsible use of AI in government* strongly recommended that agencies implement AI fundamentals training within six months of the policy taking effect (that is, by 1 March 2025).[72] The February 2025 internal audit recommended providing training on AI fundamentals. Version 2.0 of the *Policy for the responsible use of AI in government* required agencies to implement mandatory training for all staff on responsible AI use within 12 months of the policy taking effect (that is, by 15 December 2026).[73] The DTA's *Guidance for staff training on AI* (December 2025) also suggested that agencies consider if it is appropriate for staff to complete annual refresher training.[74]

2.23 In September 2025 DHDA closed the internal audit training recommendation on the basis of it undertaking 'a comprehensive approach to raise awareness of responsible AI use and provide foundational training for all staff.' From November 2025, all DHDA staff were required to complete AI fundamentals training. As of May 2026, 92.4 per cent of all staff had completed the training.

72 DTA, *Policy for the responsible use of AI in Government*, version 1.1, p. 13.

73 DTA, *Policy for the responsible use of AI in Government*, version 2.0, pp. 10 and 13.

74 Digital Transformation Agency, *Guidance for staff training on AI*, DTA, Canberra, December 2025, p. 4, available from https://www.digital.gov.au/ai/ai-in-government-policy/staff-training [accessed 12 May 2026].

2.24 The February 2025 internal audit recommended undertaking a training needs analysis. The Executive Committee endorsed a training needs analysis in March 2026, which included a skills gap analysis. The analysis identified five key training-related risks: lack of knowledge; low trust in AI outputs; data privacy and security concerns; ethical and accountability challenges; and overreliance leading to deskilling. The analysis recommended a phased learning model aligned with the *GovAI Skills Framework* and prioritising senior executive service AI leadership development.[75] The analysis proposed quarterly monitoring and annual reviews to measure AI literacy and confidence and assess whether targets had been achieved. The internal audit recommendation was closed in July 2026.

2.25 Version 2.0 of the *Policy for the responsible use of AI in government* required agencies to 'communicate their strategic position on AI to give staff clear direction on AI adoption'. DHDA developed communication and learning plans for a Microsoft 365 Copilot rollout between August and November 2025 and in September 2025 finalised an internal communications and engagement strategy. Over 2025 DHDA communicated regularly to staff about using AI, particularly Microsoft 365 Copilot. DHDA has intranet guidance including: approved AI tools and uses of AI; ethical and responsible use of AI; evaluating whether to use AI; the role of the accountable authority; instructions for accessing and using AI tools; principles for protecting sensitive information; and steps for registering new AI use cases and risk assessments.

75 Department of Finance, *GovAI*, Finance, Canberra, 2025, available from https://www.govai.gov.au/ [accessed 12 May 2026].

3. Artificial intelligence use by health providers

Areas examined

This chapter examines whether the Department of Health, Disability and Ageing (DHDA) has fit-for-purpose risk management and assurance arrangements over the adoption of artificial intelligence (AI) by health providers.

Conclusion

DHDA has partly fit-for-purpose risk management and assurance arrangements over the adoption of AI by health providers. AI-enabled software is increasingly available to health providers, including tools that support Medicare Benefits Schedule (MBS) billing. At a high level, DHDA and other Australian Government entities have identified risks associated with AI use in healthcare settings, including in health provider billing. These AI risks include: potential for bias; erroneous outputs; patient data exposure; low practitioner AI literacy; insufficient performance monitoring; and patient consent issues. Services Australia has expressed concern to DHDA about providers using AI to test MBS eligibility for multiple items and suggest billing options. DHDA has not yet systematically identified, assessed and established treatments for AI risks. Governance committees have considered some of the risks and further analysis is underway.

Areas for improvement

The ANAO made one recommendation aimed at assessing risks associated with the use of AI in healthcare settings, including the risks to health provider compliance, and identifying treatments for risks that are outside of tolerance.

3.1 A June 2026 Five Eyes cyber security agencies statement *The AI shift in cyber risk: why leaders must act now* has a call to action for leaders to 'understand and assess risk, readiness and accountability'.[76] The Productivity Commission's December 2025 report *Harnessing data and digital technology* identified health services as a particularly high risk scenario for AI.[77] DHDA has identified that AI has the potential to impact multiple facets of healthcare, including clinical care; insurance; digital systems; consent and privacy; health data; training, literacy and competency; liability and responsibility; and billing. It has identified that AI is already in use in healthcare settings; for example, in disease screening; residential aged care; use of scribes; supporting clinical decisions; surgical tools; and medical records.[78]

76 Five Eyes, *The AI shift in cyber risk: why leaders must act now*, Five Eyes, June 2026, available from https://www.cyber.gov.au/about-us/view-all-content/news/five-eyes-cyber-security-agencies-statement [accessed 25 June 2026].

77 Productivity Commission, *Harnessing data and digital technology*, Inquiry report no. 111, PC, Canberra, 2025, Recommendation 1, pp. 13–14, 16, 20, and 67, available from https://www.pc.gov.au/inquiries-and-research/data-digital/report/ [accessed 12 May 2026].

78 Department of Health, Disability and Ageing, *Safe and Responsible Artificial Intelligence in Health Care - Legislation and Regulation Review*, DHDA, March 2025, pp. 8 and 10, available from https://www.health.gov.au/sites/default/files/2025-07/safe-and-responsible-artificial-intelligence-in-health-care-legislation-and-regulation-review-final-report.pdf [accessed 12 May 2026].

3.2 The *Public Governance, Performance and Accountability Act 2013*[79], *Commonwealth Risk Management Policy*[80] and *Commonwealth Fraud and Corruption Framework*[81] all establish requirements to manage risk, including fraud risk. DHDA's Assurance Framework (see paragraph 4.18) is designed to provide confidence to leaders and decision makers that aspects of DHDA's business are being managed within expectations and in accordance with legal and policy frameworks.

3.3 This chapter examines whether DHDA has: arrangements to manage risks related to the use of AI by health providers; and assurance over the appropriate use of AI by health providers. Chapter 2 assesses whether DHDA has fit-for-purpose enterprise level arrangements to identify and manage risks related to the department's use of AI.

DHDA has identified risks related to the use of AI by health providers at a high level, but there has been little risk assessment and treatment.

3.4 DHDA advised the ANAO in May 2026 that the primary external risks associated with health provider use of AI sit largely within functions administered by Services Australia. A compliance protocol (September 2024) between DHDA and Services Australia requires the two entities to jointly manage risks and requirements for the MBS, Pharmaceutical Benefits Scheme (PBS) and Child Dental Benefits Schedule (CDBS) (see paragraph 1.18). Services Australia and the National Disability Insurance Agency jointly lead the Fraud Fusion Taskforce, of which DHDA is a participant. In DHDA the Benefits Integrity Division is responsible for the compliance of health providers under the MBS, PBS, and CDBS. The Medicare Benefits and Digital Health Division is responsible for AI in healthcare policy. The AI subcommittee to the Digital Committee (see Appendix 3) has responsibility for the stewardship of AI.

3.5 A February 2025 Enterprise Fraud and Corruption Risk Assessment provided to DHDA's Audit and Risk Committee stated that external fraud against DHDA represented the majority of fraud allegations received and investigated in 2023–24 and that 24 per cent related to the MBS. The risk assessment included a general discussion of the emergence of AI and new technologies, which highlighted that increasingly sophisticated methods may be used to identify and exploit vulnerabilities. Risk mitigations included investing in advanced AI technologies and infrastructure.

3.6 The Medicare Benefits and Digital Health Division identified risks related to the use of AI in healthcare settings through a March 2025 *Safe and Responsible AI in Health Care — Legislation and Regulation Review*. The review states that stakeholders highlighted that AI 'poses significant, and potentially irreversible risks like physical harm, death, and the long-term pollution of health records' and healthcare is a high risk setting for AI use.[82] AI risks included: potential for bias; erroneous outputs; patient data exposure; low practitioner AI literacy; insufficient performance monitoring;

79 *Public Governance, Performance and Accountability Act 2013*, section 16, available from https://www.legislation.gov.au/C2013A00123/latest/text [accessed 12 May 2026].

80 Finance, *Commonwealth Risk Management Policy*.

81 Attorney-General's Department, *Commonwealth Fraud and Corruption Control Framework*, AGD, Canberra, 2024, available from https://www.counterfraud.gov.au/library/framework-2024 [accessed 12 May 2026].

82 DHDA, *Safe and Responsible Artificial Intelligence in Health Care - Legislation and Regulation Review*, pp. 7 and 19.

and patient consent issues. The review considered mitigation through regulation[83] and non-regulatory initiatives (such as guidance and industry incentives). The review stated DHDA should ensure that statutory frameworks impacting regulation (such as billing compliance) 'reflect nascent AI norms'[84], however the review did not expand on this or examine in detail health provider compliance risks. In August 2025 DHDA briefed the Minister for Health and Ageing on the review.

3.7 Services Australia lists practice management software on its website that integrate with MBS claiming channels (see paragraph 1.23).[85] On software websites, approximately one-fifth refer to using AI, particularly AI scribes. Practice management and MBS billing software websites often refer to optimising billing processes, identifying missed billing opportunities, increased billing volumes, and in one case, suggesting the most lucrative combination of MBS item numbers.[86]

3.8 In June 2025 the Benefits Integrity Division started drafting a 'prompted billing software including AI' scoping paper for internal use[87], which listed four potential risks from AI-enabled billing software: MBS item descriptors; practitioner complacency; full automation; and the clinical appropriateness of billing items. The draft paper noted an increase in software packages maximising MBS claiming by using AI to generate MBS item suggestions.

3.9 In October 2025 Services Australia expressed concern to DHDA about providers using AI to test MBS eligibility for multiple items and suggest billing options. This risk was not recorded in shared risk registers between Services Australia and DHDA for MBS compliance.

3.10 In May 2026 the Benefits Integrity Division drafted a 'use of prompted billing software in Medicare' strategic intelligence report for internal use, identifying several risks to compliance associated with health providers using prompted billing tools. The report identified prompted billing software as an emerging issue requiring monitoring, noting the emerging use of AI by practitioners to analyse clinical consultation notes with four commercial tools identified. The draft strategic intelligence report stated that existing capability does not enable the identification of practices or practitioners using prompted billing functionality (including those that use AI), but that most inappropriate claiming should be detectable through existing capability. The draft report proposed initiatives to identify the use of this type of software. As of August 2026 the report had not been finalised.

3.11 In addition to risks associated with AI-enabled billing software, DHDA advised the ANAO in May 2026 of other 'AI-adjacent, technology-enabled' risks including: misuse of provider numbers

83 The Productivity Commission's December 2025 report *Harnessing data and digital technology* recommended enabling productivity growth from within existing legal foundations and that AI-specific regulations should be a 'last resort'.
PC, *Harnessing data and digital technology*, Inquiry report no. 111, Recommendation 1, p. 2.

84 DHDA, *Safe and Responsible Artificial Intelligence in Health Care — Legislation and Regulation Review*, p. 12.

85 Services Australia, *Software for Medicare Online, ECLIPSE and the AIR*, Services Australia, Canberra, 2026, available from https://www.servicesaustralia.gov.au/software-for-medicare-online-eclipse-and-air [accessed 12 May 2026]; and
Services Australia, *Software vendors for Medicare Easyclaim*, Services Australia, Canberra, 2024, available from https://www.servicesaustralia.gov.au/software-vendors-for-medicare-easyclaim [accessed 12 May 2026].

86 Each service listed on the MBS has an item number, which is a descriptor that outlines the type and scope of the service, the MBS schedule fee and the MBS benefit (rebate).

87 DHDA defines prompted billing as software that uses data analytics and/or AI to suggest MBS item numbers that could be applicable for billing.

by non-clinicians; weaknesses in identification and authentication pathways; vulnerabilities within MBS payment systems and channels; and technology-enabled fraud through exploitation of automatic payment rules. DHDA stated that 'AI and robotics in the wrong hands exploiting any of these vulnerabilities is a significant risk'.

3.12 Although risks and potential treatments have been identified at a high and preliminary level in the discussion papers and draft analyses described in paragraphs 3.5 to 3.10, there has been little formal and systematic identification and assessment of AI risks as they relate to health provider compliance by responsible business areas within DHDA.

- The Integrity and Assurance Division, which included the Fraud and Integrity Branch until February 2026[88], did not identify any risks associated with the use of AI by health providers in planning and risk artefacts.
- The Medicare Benefits and Digital Health Division's 2025–26 business and risk plan lists the priority 'Lead policy advice on the use of AI in Health care, including consideration of genomics, to support productivity'; and an opportunity and challenge related to the use of AI by health providers. The plan does not identify or assess specific risks related to AI use in healthcare settings.
- Shared risk registers between Services Australia and DHDA for MBS compliance do not make reference to AI risks.
- The Benefits Integrity Division 2025–26 business and risk plan did not consider AI use by health providers. The division's January 2026 Compliance Risk Register did not contain anything explicitly related to AI risks. As of August 2026, the Benefits Integrity Division was drafting its 2026–27 business plan to include an AI risk, and an intention to develop a coordinated approach with Services Australia to map and monitor AI related risks and opportunities, with a focus on strengthening MBS integrity.

There is some governance oversight, however assurance activities over the use of AI by health providers lack momentum.

3.13 The March 2025 *Safe and Responsible AI in Health Care — Legislation and Regulation Review* (see paragraph 3.6) considered 'cornerstone' federal health legislation including that governing the MBS and PBS. The review noted that while the current regulatory system was generally not fit for purpose[89], the regulatory frameworks administered by DHDA (which are narrower in scope and primarily administrative in nature) were largely able to accommodate AI in healthcare and operate as intended, with minor technical and definitional amendments.[90] DHDA advised the ANAO in May 2026 that it 'is aware of the impact of AI on health legislation and regulation and will consider minor amendments as necessary on a case by case basis as AI is more widely adopted across health care.'

3.14 The Therapeutic Goods Administration (TGA) is responsible for the regulation of medical devices, including those using AI. Digital scribe or practice management software is subject to TGA regulation if it meets the definition of a medical device. In a 2025–26 internal business and risk plan, the TGA recognised a risk related to the increasing use of AI and automation by pharmaceutical

88 In February 2026 the Fraud and Integrity Branch moved to the Benefits Integrity Division.

89 DHDA, *Safe and Responsible Artificial Intelligence in Health Care — Legislation and Regulation Review,* p. 3.

90 ibid., p. 12.

companies resulting in the TGA experiencing increased workloads from larger volume and higher complexity submissions. In June 2025 the TGA established a committee to review three domains: the regulation of AI products; the use of AI by sponsors and manufacturers in submissions; and the internal use of AI at the TGA. A July 2025 report, *Clarifying and strengthening the regulation of medical device software including AI*, reviewed the *Therapeutic Goods Act 1989* and regulations to ensure they are fit for purpose given the increasing use of medical software and AI across the healthcare sector. The report concluded that the legislative framework is largely fit for purpose and identified possible improvements.[91]

3.15 DHDA advised the ANAO in March 2026 that it cannot analyse claiming by health providers using AI-enabled prompted billing software due to a lack of data to confirm whether a health provider has used an AI billing assistant. DHDA stated that it knew of free software, offered without any proof of identity that may have been used to commit fraud, that Services Australia and DHDA have no visibility of software products once in use, and there are no regulatory requirements in place to enforce compliance.

3.16 In June 2025 the Medicare Integrity Reform Steering Group (see Appendix 3) discussed MBS reform ideas, including problems with the use of commercial software packages aimed at maximising MBS billing. The steering group agreed to look into software packages with prompted billing and perform data and analytical modelling to identify unusual item co-claiming combinations. This work included the draft scoping paper described in paragraph 3.8 and an 'agile' team stood up to look into AI billing. The draft strategic intelligence report described in paragraph 3.10 was provided to the Medicare Integrity Reform Steering Group in May 2026. DHDA advised the ANAO in April 2026 that it anticipated completion of data and analytical modelling by the end of 2026.

3.17 Terms of reference for the AI subcommittee include stewarding DHDA's approach to AI, including its use and regulation. In March 2026 the AI subcommittee discussed potential implications for DHDA arising from the Productivity Commission's 2025 report on *Harnessing Data and Digital Technology*, including measuring the productivity impact of AI in healthcare; scoping a national 'AI in health' plan; ongoing monitoring of AI given rapid market development; and stakeholder concerns with AI and patient privacy. The subcommittee created an action item to consider the Productivity Commission Report recommendations. DHDA advised the ANAO in August 2026 that it was continuing to assess the recommendations.

3.18 DHDA advised the ANAO in January 2026 that the Medicare Benefits and Digital Health Division does not monitor AI use but engages with the sector to understand how providers are using AI. Since consultation with stakeholders in August and September 2024 under the *Safe and Responsible AI in Health Care — Legislation and Regulation Review*, the division has met with two stakeholders, participated in one roundtable and held two webinars.

3.19 DHDA advised the ANAO in April 2026 that the Benefits Integrity Division was working with Services Australia and the Australian Digital Health Agency to improve systems and support to manage practice management software developers. In the 2026–27 federal Budget, the

91 Department of Health, Disability and Ageing, *Report: Clarifying and strengthening the regulation of Medical Device Software including Artificial Intelligence (AI)*, DHDA, Canberra, 2025, available from https://www.tga.gov.au/sites/default/files/2026-02/report-clarifying-strengthening-regulation-medical-device-software-including-artificial-intelligence-ai.pdf [accessed 12 May 2026].

government announced $3.5 billion in measures to strengthen Medicare.[92] This included funding to support Services Australia in its oversight of Medicare.

Recommendation no. 1

3.20 The Department of Health, Disability and Ageing work with other government entities and sector stakeholders to identify and assess: the risks associated with the use of artificial intelligence in healthcare settings, including from health providers using artificial intelligence in Medicare Benefits Schedule claiming; whether current regulatory and other controls are effective in mitigating risks; and possible treatments for artificial intelligence risks outside of tolerance.

Department of Health, Disability and Ageing response: *Agreed*

3.21 *The Department of Health, Disability and Ageing acknowledges the risks and opportunities that artificial intelligence adoption creates across healthcare settings. Artificial intelligence applications continue to expand across the health system. The department will consider these matters through existing governance and risk management processes drawing on the expertise of responsible business areas and, where appropriate, engagement with other government entities, delivery partners and sector stakeholders. The department will review and update departmental frameworks, guidance and supporting resources to promote consideration of artificial intelligence-related risks and opportunities across the department's functions and responsibilities.*

3.22 *Consistent with the findings of this audit, the department will build on existing Medicare integrity arrangements with Services Australia to identify, assess and manage risks associated with the use of artificial intelligence that may affect health benefits integrity and provider claiming compliance. While artificial intelligence is not currently assessed as a demonstrated Medicare integrity risk in its own right, artificial intelligence-enabled technologies may increase the scale, speed or sophistication with which existing integrity risks manifest. In relation to Medicare benefits integrity, the department's focus will remain on preventing and responding to incorrect, inappropriate and fraudulent claiming.*

92 Minister for Health and Ageing, 'Budget 2026-27: A stronger care system for all Australians', media release, 12 May 2026, available from https://www.health.gov.au/ministers/the-hon-mark-butler-mp/media/budget-2026-27-a-stronger-care-system-for-all-australians [accessed 3 September 2026].

4. Design, development, deployment and assurance of artificial intelligence in the department

Areas examined

This chapter examines whether the Department of Health, Disability and Ageing (DHDA) has fit for purpose arrangements for the design, development, deployment and assurance of artificial intelligence (AI) models, with a focus on the Medicare Benefits Schedule (MBS) fraud and non-compliance detection system (fraud detection system).

Conclusion

Arrangements for the design, development and deployment of AI models are maturing.

- DHDA has established processes for use case registration, consideration of ethical risks, information security and privacy assessment that are largely or fully aligned with whole-of-government AI governance requirements. As of April 2026 most registered AI use cases related to Microsoft Copilot.
- DHDA's AI use case assessment process is continuing to develop to meet whole-of-government requirements, some of which are not mandatory until later in 2026 and 2027. DHDA is maturing AI policies and procedures to ensure that legal and cyber security risks are considered and treated, and that the *Technical standard for government's use of artificial intelligence* is applied to use cases.
- DHDA's development and deployment of an AI-enabled MBS fraud and serious non-compliance detection system, which pre-dated new whole-of-government requirements for AI use cases, partly aligned with better practice for AI development and deployment. There was no considered assessment prior to development and deployment of ethical risks, legal risks, data suitability, sensitivity, privacy or cyber security. During development and deployment, there were deficiencies in system validation, approval and monitoring. Process improvements are planned and underway.
- Assurance planning and processes are also developing. Departmental incident management policies have been partly updated to reflect new risks. DHDA has identified some unrestricted and unapproved use of AI, including through an AI stocktake completed in June 2026. There is a draft AI Assurance Framework. As of June 2026 there is incomplete assurance that AI use is being managed within expectations and in accordance with legal and policy frameworks.

Areas for improvement

The ANAO made two recommendations aimed at improving use case assessment, approval and authorisation processes; and strengthening assurance over AI use, including by ensuring cyber security policies reflect AI risks. There was one opportunity for improvement related to AI development and deployment processes.

4.1 DHDA published a Fraud and Corruption Control Plan 2025–27, which includes increasing fraud and corruption prevention and detection capability through data monitoring and analytics.[93] In August 2023 DHDA began developing a system to detect potential MBS fraud and serious non-compliance by analysing provider claiming data. An AI-enabled model in the fraud detection system was used from July 2024 to December 2025.

4.2 In October 2023 the Medicare Integrity Reform Program Board (see Appendix 3) discussed work being undertaken between DHDA and Services Australia on potential uses of AI. In March 2024 Services Australia proposed using AI to detect fraud and non-compliance to the board. The board did not endorse the proposal, asking for model refinement before the next federal Budget. In September 2025 Services Australia advised the board that it was working on detecting 'consumer' fraud using AI and machine learning, which might inform similar options for provider fraud.

4.3 AI systems used in operational settings can introduce risks and assurance challenges across the system's lifecycle.[94] Australian Government and international better practice guidance emphasises entities establishing controls to enable transparency, traceability and risk management throughout the lifecycle, and tailored to the system's purpose, complexity and potential impacts.

- The *Policy for the responsible use of AI in government* outlines the requirement to ensure AI is being designed, developed, deployed and monitored effectively. Principles include that 'AI use is lawful, ethical, responsible, transparent and explainable to the public.'[95]
- The *Australian Government AI technical standard* 'sets consistent practices for government agencies adopting [AI] systems across the AI lifecycle'.[96]
- The Organisation for Economic Co-operation and Development report *Advancing Accountability in AI* recommends five elements of risk management and governance across the AI lifecycle: monitoring and reviewing; documenting; communicating; consultation; and embedding risk management culture.[97]

4.4 This chapter examines whether DHDA has fit-for-purpose arrangements for the AI lifecycle, including: AI system design, development and deployment; and assurance over AI system use.

93 Department of Health, Disability and Ageing, *Fraud and Corruption Control Plan 2025–27*, DHDA, 2025, available from https://www.health.gov.au/resources/publications/fraud-and-corruption-control-plan-2025-27 [accessed 12 May 2026].

94 The AI lifecycle is 'the sequence of phases that an AI system goes through, from its conception, all the way through its development, testing, deployment, use, and eventual retirement.'
National Artificial Intelligence Centre, *Guidance for AI Adoption: implementation guidance*, National AI Centre, May 2026, p. 22, available from https://www.ai.gov.au/staying-safe-and-responsible/essential-ai-practices/guidance-ai-adoption-implementation-guidance [accessed 12 May 2026].

95 DTA, *Policy for the responsible use of AI in government*, version 2.0, p. 14.

96 The technical standard is voluntary.
DTA, *Australian Government AI Technical Standard,* version 1, p. 8.

97 The Organisation for Economic Co-operation and Development, *Advancing Accountability in AI; Governing and Managing Risks Throughout the Lifecycle for Trustworthy AI*, OECD Digital Economy Papers, February 2023, No. 349, p. 10, available from https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/02/advancing-accountability-in-ai_753bf8c8/2448f04b-en.pdf [accessed 12 May 2026].

The AI use case assessment process is developing to meet whole-of-government requirements. Consideration of legal and cyber security risks is not yet sufficient.

4.5 The *Policy for the responsible use of AI in government* defines an AI use case as 'specific application of an AI system or systems to achieve certain objectives or perform certain tasks.'[98] DHDA has three categories of use cases: (1) general productivity and personal research; (2) defined business process or decision process with internal impact; and (3) defined business process or decision process with external impact.

4.6 Table 4.1 summarises whole-of-government requirements for AI use cases, how they were implemented in DHDA policies, and how they had been applied to the fraud detection system as of May 2026. Different whole-of-government requirements and better practice applied at different times, with most requirements not becoming mandatory until December 2026 or later. The *Policy for the responsible use of AI in government* states that where practicable, entities should implement requirements ahead of deadlines.

4.7 At a high level, DHDA established arrangements to implement applicable whole-of-government requirements in its policy framework, including an AI use case registration process, risk assessment processes and an AI stocktake. Some areas of implementation were incomplete or evolving. In particular, the use case register did not contain all information required under December 2025 policy updates, and staff were not required to assess legal risks or legislative bases for AI use cases. As of May 2026 DHDA was updating its use case registration and risk assessment processes to align with updated whole-of-government requirements.

4.8 The fraud detection system pre-dated DHDA's enterprise AI governance arrangements. In November 2024 a use case assessment was completed for the system as part of a whole-of-government AI pilot before the introduction of the *Policy for the responsible use of AI in government*. The assessment was not recorded in DHDA's AI use case register. Although the system used personal information, the system was assessed as having low inherent ethical risk. As a result, privacy and legal risks were not subject to more detailed assessment, and legal advice was not sought. In May 2026 DHDA completed a privacy threshold assessment that identified high-risk factors for the system and as of August 2026 was seeking to have this reviewed by the Australian Government Solicitor.

98 DTA, *Policy for the responsible use of AI in government*, version 2.0, p. 19. Version 1.1 of the policy (1 September 2024) did not define a use case.

Table 4.1: Arrangements for the design of artificial intelligence systems, including the fraud detection system, as of May 2026

Design elements	Whole-of-government policy requirements / guidance	Implementation of whole-of-government requirements in DHDA policy framework	Application to the fraud detection system[a]
Use case registration	Version 1.1 (September 2024) of the *Policy for the responsible use of AI in government* (the policy) suggested agencies develop an internal register of AI use. Version 2.0 (December 2025) required agencies to create a register of in-scope AI use cases, including minimum information, by December 2026 and share the register with the Digital Transformation Agency (DTA) every six months, once the register is created.[b] If an AI tool was already in use entities are required to determine whether the tool is in scope of the policy and, if so, apply all relevant policy actions by 30 April 2027.	◆ A February 2025 DHDA internal audit on Readiness for Artificial Intelligence Use recommended creating and maintaining a register to capture all AI products in use. From March 2025, DHDA staff were required to register new AI uses. The register includes the status of AI use cases. As of April 2026 there were 55 registered AI use cases (see paragraph 4.9). The findings of an AI stocktake were presented to the AI subcommittee in June 2026.	The fraud detection system is not listed in DHDA's AI use case risk register. As the fraud detection system was already in use at the time the whole-of-government policy was released in December 2025, it is not required to comply with the policy's AI use case registration process until April 2027 if the fraud detection system again uses an AI-enabled model in the future.
Use case impact assessment	Version 1.1 of the policy suggested Australian Government entities monitor use cases for unintended impacts. Version 2.0 required entities by 15 December 2026 to: designate a use case owner for each in-scope use case; assess and document all new AI use cases against certain criteria to determine if they are in scope of the policy[c]; and for in scope cases, conduct impact assessments using the *AI impact assessment tool*[d] or an internal process integrating all provisions of the tool, and update use cases as required. The *Standard for accountability*[e] (December 2025) supports implementation of the policy by outlining the responsibilities of use case owners and the minimum information.	▲ A use case submission form in use from March 2025 includes: name of approver; purposes; consideration of non-AI solutions; security classification of data; usage pattern; disclosure processes; and review frequency. The use case register did not contain all of the minimum information required to align to the *Standard for Accountability* including: the criteria the use case met to be in scope of the policy; the AI technology type; lifecycle stage; and whether the *Technical standard for government's use of artificial intelligence* was applied.	DHDA had not determined whether the fraud detection system is in scope of the policy. The fraud detection system is designed to use personal or sensitive data, making it in scope. Although not listed in the register, in November 2024 a use case assessment was completed as part of a whole-of-government AI pilot.[f] The assessment details: use; the system was at the 'operation and monitoring' stage; and contact officer and executive sponsor. The assessment contains the minimum information required by the *Standard for accountability* and *Artificial intelligence impact assessment tool*.

Design elements	Whole-of-government policy requirements / guidance	Implementation of whole-of-government requirements in DHDA policy framework	Application to the fraud detection system[a]
Ethics risk assessment	The 2024 *APS Data Ethics Framework*[g] provides guidance on the ethical use of data and analytics, including that, if AI is involved, *Australia's AI Ethics Principles*[h] (November 2019, updated December 2025) apply. Version 1.1 of the policy provided an example risk assessment which included the ethics principles. The *AI impact assessment tool* (required to be completed by 15 December 2026 for all new use cases) was designed to assist entities to identify, assess and manage ethical risks including to: environmental wellbeing; human-centred values; fairness; privacy protection and security; reliability and safety; transparency and explainability; contestability; and accountability. If 'inherent' risks are rated medium or high, a full risk assessment and management plan must be completed. Version 2.0 of the policy states that when deploying an in-scope use case, the impact assessment must be re-validated when there is a material change in scope, usage or operation.	 Prior to March 2025, DHDA did not require risk assessment, including ethical risk assessment, for AI use cases. The February 2025 internal audit recommended completing a risk assessment for each AI product in use. From March 2025, DHDA staff were required to include a risk assessment in the use case register, which required staff to consider, the eight ethics principles in design, including: who the output serves; mechanisms for stakeholders to challenge outputs; and whether the AI use case involves surveillance. The use case approver (recommended to be at the senior executive service (SES) level, in line with DTA policy) endorses the risk assessment. Medium and high risk cases require a 'notification of assessment' from DHDA's AI Governance Office and further SES approval before proceeding. In September 2025 DHDA closed the internal audit recommendation.	The November 2024 fraud detection system use case assessment completed as part of a whole-of-government AI pilot included a high-level ('inherent') risk assessment that included a general ethical assessment. This process required a more detailed ethical risk assessment if the inherent assessment was rated medium or high. Despite the use of personal information, DHDA assessed the fraud detection system as having low inherent ethical risk in November 2024. As such, the more detailed ethical risk assessment was not required. Ethical risks associated with the fraud detection system have not been re-assessed since November 2024.

Design elements	Whole-of-government policy requirements / guidance	Implementation of whole-of-government requirements in DHDA policy framework	Application to the fraud detection system[a]
Legal risk assessment	Version 1.1 of the policy did not have any guidance for obtaining legal advice. The *AI impact assessment tool* states that seeking legal advice is an important part of managing risk, requires entities to record if legal advice was sought and suggests: seeking legal advice on whether the proposed AI use is compliant with laws and regulations if the inherent risk rating is medium or high; aligning with relevant legislation and regulatory instruments; and, if AI enabled automated decision-making is used for an administrative decision under legislation, seek legal advice regarding legislative authority. In April 2026 the Federal Court of Australia released a practice note on the use of generative AI requiring persons using it to: have a basic understanding of its capabilities; not adversely use it to affect the administration of justice; and disclose its use.[i]	 DHDA's AI transparency statement asserts that it does not use 'AI to automate decisions'.[j] DHDA's Legal Division presented a paper at the October 2025 AI subcommittee meeting, which stated that 'Teams considering a medium or high risk use case should seek early legal advice, so they are informed of legal risk and implement mitigation measures where appropriate.' The paper refers to legal considerations including: privacy; intellectual property; administrative decision making; duty of care; freedom of information; and record keeping. DHDA's AI use case assessment guide requires staff to consider obtaining legal advice but the risk assessment does not require staff to consider legal risks or legislative bases for AI use.	The November 2024 high-level 'inherent' risk assessment completed as part of a whole-of-government AI pilot did not require consideration of legal risk. A question about legal risk was part of the more detailed risk assessment that would have been required if the system had been rated medium or high risk. As the system was rated low risk this question was never considered. DHDA did not seek legal advice for the fraud detection system.
Information security and privacy assessment	The *Protective Security Policy Framework* requires all technology systems to be authorised.[k] A March 2024 *Information security manual* governing principle is 'Security risks are identified, documented, managed and accepted both before systems and applications are authorised for use, and continuously throughout their operational life.'[l] In December 2025 the updated manual stated: '[AI]-specific documentation, including model and system cards (or equivalent artefacts), is used to document model characteristics, system architectures, use cases and security risks.'[m] The Office of the Australian Information Commissioner requires a 'privacy threshold'	 DHDA's AI use case assessment requires staff to identify: the type of data used; data security classification; compliance with the *Privacy Act 1988*; whether a privacy threshold or impact assessment has or should be done; and whether there are security risks. The Benefits Integrity Division Compliance Data Management Framework requires compliance with AI ethics principles, the protection of privacy and the securing of sensitive data through robust encryption, access controls and adherence to data protection laws.	The November 2024 high-level 'inherent' risk assessment completed as part of a whole-of-government AI pilot did not require consideration of data, cyber security or privacy risk. Questions about data suitability, sensitivity, and privacy impact were part of the more detailed risk assessment that would have been required if the system had been rated medium or high risk, however as the system was rated low risk, these questions were never considered. In May 2026 DHDA prepared a draft privacy threshold assessment which noted high-risk factors for the system. These related to using and disclosing

Design elements	Whole-of-government policy requirements / guidance	Implementation of whole-of-government requirements in DHDA policy framework	Application to the fraud detection system[a]
	assessment to be undertaken if a project involves new or changed ways of handling personal information and a 'privacy impact' assessment for all high privacy risk projects.[n] Version 2.0 of the policy required an AI use case if personal or sensitive data or security classified information was used. The *AI impact assessment tool* suggests considering data throughout impact assessment.	DHDA relies on a whole-of-government privacy impact assessment for staff use of Microsoft 365 Copilot.	personal information to profile or predict behaviours of individuals. In July 2026 DHDA was intending to seek legal advice from the Australian Government Solicitor on the privacy threshold assessment. There was limited documentation of cyber security considerations for the fraud detection system, such as a system security plan, model or system cards, and other documentation that assessed security risks and associated controls. DHDA advised the ANAO in March 2026 that development of the fraud detection system predated the establishment of enterprise AI governance arrangements and had not been managed within DHDA's enterprise governance and security framework. Teams responsible for cyber security were unaware of the fraud detection system's operation and a cyber security risk assessment had not been completed.

Key: ■ Not implemented ▲ Partly implemented/applied ◆ Largely or fully implemented/applied

Note a: The AI-enabled model of the fraud detection system was switched to a non-AI logistic regression model in December 2025. DHDA advised the ANAO in March 2026 that it intends to use AI-enabled models in the fraud detection system in the future.

Note b: Digital Transformation Agency, *Policy for the responsible use of AI in government*, DTA, Canberra, December 2025, p. 11, available from https://www.digital.gov.au/ai/ai-in-government-policy [accessed 12 May 2026].

Note c: The criteria are: the use, misuse or failure of AI could lead to more than insignificant harm to individuals, communities, organisations, the environment or the collective rights of cultural groups including First Nations peoples; the use of AI will materially influence administrative decisions that affect individuals, communities, organisations, the environment or the collective rights of cultural groups including First Nations peoples; it is possible the public will directly interact with, or be significantly impacted by, the AI or its outputs without human review; the AI is designed to use personal or sensitive data or security classified information; it is deemed an elevated risk AI use case as directed by the DTA.

Note d: Digital Transformation Agency, *Artificial intelligence impact assessment tool*, DTA, Canberra, December 2025, available from https://www.digital.gov.au/ai/impact-assessment-tool [accessed 12 May 2026].

Note e: Digital Transformation Agency, *Standard for accountability*, DTA, Canberra, December 2025, available from https://www.digital.gov.au/ai/ai-in-government-policy/accountability [accessed 12 May 2026].

Note f: The pilot ran from September to November 2024, with 21 entities testing a draft AI impact assessment tool, which was designed to identify, assess and manage potential AI impacts and risks. More information available from https://www.digital.gov.au/policy/ai/pilot-ai-assurance-framework [accessed 12 May 2026].

Note g: Department of Finance, *APS Data Ethics Framework*, Finance, Canberra, 2024, available from https://www.finance.gov.au/government/public-data/public-data-policy/data-ethics-framework [accessed 12 May 2026].

Note h: Department of Industry, Science and Resources, *Australia's AI Ethics Principles* [Internet], DISR, Canberra, 2025, available from https://www.industry.gov.au/publications/australias-ai-ethics-principles [accessed 12 May 2026].

Note i: Chief Justice D S Mortimer, *Use of Generative Artificial Intelligence Practice Note*, Federal Court of Australia, Canberra, April 2026, available from https://www.fedcourt.gov.au/law-and-practice/practice-documents/practice-notes/gpn-ai [accessed 12 May 2026].

Note j: Department of Health, Disability and Ageing, *Artificial intelligence (AI) transparency statement* [Internet], DHDA, Canberra, 2026, available from https://www.health.gov.au/about-us/corporate-reporting/our-commitments/ai-transparency-statement [accessed 12 May 2026].

Note k: Department of Home Affairs, *Protective Security Policy Framework*, Home Affairs, Canberra, 2025, Section 13.3, available from https://www.protectivesecurity.gov.au/system/files/2025-07/pspf-release-2025.pdf [accessed 12 May 2026].

Note l: Australian Signals Directorate, *Information security manual*, ASD, Canberra, March 2024, p. 5, available from https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/archived-ism-releases [accessed 12 May 2026].

Note m: Australian Signals Directorate, *Information security manual*, ASD, Canberra, March 2026, p. 163, available from https://www.cyber.gov.au/sites/default/files/2026-03/Information%20security%20manual%20%28March%202026%29.pdf [accessed 12 May 2026].

Note n: A privacy threshold assessment is a preliminary assessment to determine a project's potential privacy impacts and give a sense of the risk level. A privacy impact assessment is a 'systematic assessment that identifies the impact that a project might have on the privacy of individuals, and sets out recommendations for managing, minimising, or eliminating that impact.' Office of the Australian Information Commissioner, *When do agencies need to conduct a privacy impact assessment?* [Internet], OAIC, Canberra, September 2020, available from https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/government-agencies/australian-government-agencies-privacy-code/when-do-agencies-need-to-conduct-a-privacy-impact-assessment [accessed 12 May 2026].

Source: ANAO analysis.

4.9 As of April 2026 all of the 55 registered AI use cases were assessed as low risk. Thirty use cases involved Microsoft Copilot. Most use cases were categorised as 'workplace productivity' (45 use cases) or 'analytics for insight' (14 use cases) and occurred in the domains 'corporate and enabling' (37 use cases) and 'service delivery' (20 use cases).[99] In April 2026 DHDA identified that the impact assessment for 22 in-scope use cases had not been appropriately approved. In addition, an AI stocktake completed in June 2026 identified 10 unapproved AI tools, nine machine learning use cases requiring further assessment and 'significant' use of AI by the department's vendors, consultants and grantees. The AI subcommittee endorsed next steps, which included assessment of unapproved tools or cessation of use where appropriate.

Recommendation no. 2

4.10 The Department of Health, Disability and Ageing strengthen compliance with whole-of-government policy by:

(a) incorporating the consideration of legal risks in revised use case assessment processes;

(b) ensuring that all artificial intelligence systems in use in the department have appropriate authorisation and that security risks are identified, documented, managed and accepted before systems and applications are authorised for use; and

(c) implementing controls to ensure that approval processes for use cases are followed.

Department of Health, Disability and Ageing response: *Agreed*

4.11 *The Department of Health, Disability and Ageing is strengthening its artificial intelligence governance arrangements by incorporating legal risk considerations into use case assessment processes, supported by legal guidance and oversight through the Artificial Intelligence Centre of Excellence. The department has established cyber security and system authorisation processes. These processes require security risks are identified, documented, managed and accepted before artificial intelligence systems and applications are authorised for use.*

4.12 *The department will implement governance, workflow and assurance controls through the Artificial Intelligence Assurance Framework and Use Case Registration Tool. These controls will ensure approval processes are followed and use cases only proceed once all required approvals are obtained and recorded.*

DHDA's development of an AI-enabled system was partly aligned with better practice. Process improvements are planned and underway.

4.13 DHDA started developing the fraud detection system in 2023 to assist with the detection of MBS fraud and serious non-compliance by analysing provider claiming data. Better practice for managing the development of AI models is drawn from the DTA *Technical standard for government's use of artificial intelligence* and the International Organization for

99 DHDA's use case registration process allows use cases to have more than one selection for the usage pattern and domain.

Standardization (ISO) and International Electrotechnical Commission (IEC) 42001:2023 *Information technology — Artificial intelligence — Management system.*[100]

4.14 Table 4.2 shows that DHDA's development of the fraud detection system was partly aligned to better practice. The fraud detection system had established arrangements for data quality and auditability. Roles and responsibilities for the development lifecycle were documented late; model training and evaluation documentation was inconsistent; fairness or bias metrics were not implemented; and governance, risk management and model development requirements were not consistently followed or evidenced. DHDA is developing processes, which could be strengthened by improved process documentation and consistent application.

Table 4.2: Assessment of the development of the fraud detection system against better practice, as of May 2026

Component	DTA better practice	ANAO assessment[a]	
Roles and responsibilities	Key roles, responsibilities and accountable parties are defined across the AI lifecycle.	▲	Roles and responsibilities for stages of the fraud detection system development lifecycle were belatedly documented and finalised in January 2026. In February 2026 the Benefits Integrity Division finalised a Requirements and Change Management Framework, which outlines structured processes, defined roles, approval points and validation mechanisms for new developments. DHDA advised the ANAO in February 2026 that implementation of the framework was underway.
Data collection and preparation	Data sources and data preparation processes are documented, traceable, and subject to defined data quality controls across the AI lifecycle.	◆	The primary data sources for the fraud detection system are clearly identified. DHDA relies on Services Australia to provide assurance over the completeness and accuracy of source data. DHDA has automated and manual validation and integrity controls during data preparation processes. Data provenance[b] for the fraud detection system is traceable; and data lineage[c], which fosters transparency and trust in AI systems, is maintained through documentation of automated and manual processes.

100 ISO develops voluntary international standards across various industries. IEC prepares and publishes standards for electrical, electronic and related technologies.

Component	DTA better practice	ANAO assessment[a]	
Modelling	System choice aligns with business needs and data suitability. System training and evaluation processes are documented, implemented, and risk based.	▲	DHDA advised the ANAO in January 2026 that model selection within the fraud detection system is driven by business requirements, with a preference for the simplest solution. Multiple methods were explored during the development of the AI-enabled model within the fraud detection system, which were not all documented. DHDA advised the ANAO in February 2026 that an AI model was selected based on its performance. The rationale for and process involved in model selection, training and tuning was not formally documented. More consistent documentation of these processes would improve DHDA's ability to reperform and monitor the model.
Bias and fairness	AI systems are designed, developed, deployed and monitored in a manner that identifies, mitigates, and manages bias, and supports fair outcomes.	▲	DHDA has not implemented metrics to assess fairness or bias within the fraud detection system. The November 2024 fraud detection system risk assessment (see Table 4.1) identified 'unfairly discriminating against individuals, communities or groups' as a low risk. The risk assessment indicated that the risk was managed through focused development scopes based on characteristics of known fraud, validation of results prior to the approval of models, and staff review of model outputs before any action is undertaken to further investigate potential fraud or serious non-compliance. DHDA advised the ANAO in March 2026 that consideration of model behaviour occurred but was largely undocumented. DHDA also advised it had drafted a monitoring framework that proposes standardised metrics to alert for over-representation of certain groups in results, including required actions when this occurs, but that these improvements will not be implemented for the fraud detection system until software is approved.
Evaluation	System validation is conducted using fit-for-purpose evaluation methods with appropriate governance processes.	▲	See paragraphs 5.9 to 5.13 for fraud detection system validation findings.
Auditability and reproducibility	AI systems are designed and operated to enable end-to-end auditability, supported by traceability, audit logging and version control to allow reconstruction and inspection of AI system states, decisions and outcomes at a point in time.	◆	DHDA logs processing outcomes, inputs and code changes within the fraud detection system. Manual processes during data collection and processing prior to ingestion into the fraud detection system are documented. Code version control is applied within the fraud detection system, and snapshots of data inputs are saved at each run. Outputs of the fraud detection system are reproduceable using version-controlled models and retained data snapshots.

Component	DTA better practice	ANAO assessment[a]	
Peer review and assurance	Appropriate peer review and assurance arrangements are implemented within the development process to ensure AI systems meet operational requirements and outputs are correct, consistent and complete.	▲	A November 2024 fraud detection risk assessment was completed as part of a whole-of-government AI pilot. There is an undated model development framework that sets out requirements for quality assurance, end-user review, documentation, and agreed governance procedures. The framework states that actual processes 'may be nebulous and not follow this path'. As discussed in Table 4.3, DHDA advised ANAO in April 2026 that these requirements have been inconsistently followed and documented.

Key: ■ Not aligned ▲ Partly aligned ◆ Largely or fully aligned

Note a: The AI-enabled model of the fraud detection system was switched to a non-AI logistic regression model in December 2025. DHDA advised the ANAO in March 2026 that they intend to use AI-enabled models in the fraud detection system in the future.

Note b: Data provenance 'involves creating an audit trail to assign custody and trace accountability for issues. It provides assurance of the chain of custody and its reliability, insofar as origins of the data are documented.'

Note c: Data lineage 'involves documenting data origins and flows to enable stakeholders to better understand how datasets are constructed and processed.'

Digital Transformation Agency, *Pilot AI assurance framework guidance*, DTA, Canberra, undated, available from https://www.digital.gov.au/policy/ai/pilot-ai-assurance-framework/guidance/step-5 [accessed 12 May 2026].

Source: ANAO analysis informed by better practice drawn from AS ISO/IEC 42001:2023 *Information technology — Artificial intelligence — Management system* and the DTA's *Technical standard for government's use of artificial intelligence*.

DHDA's deployment of an AI model was partly aligned with better practice. Validation, approval and monitoring process improvements are planned and underway.

4.15 DHDA began using the AI-enabled model within the fraud detection system in July 2024. In December 2025, DHDA replaced the AI model with a non-AI logistic regression model to reduce the volume of flagged providers (see Chapter 5).

4.16 Table 4.3 shows that DHDA's deployment of the fraud detection system was partly aligned to better practice. Evidence that outputs of the AI model had been validated and approved were not consistently documented. Documentation of testing, approval and planning before the AI model was deployed was limited. While system logs supported investigation of failures, monitoring of the AI model's performance was informal, occurred irregularly, and largely relied on user feedback. DHDA is developing processes to support better practice deployment for future use cases (see paragraph 5.14), which could be strengthened by better process documentation and consistent application.

Table 4.3: Assessment of deployment of the fraud detection system against better practice, as of May 2026

Component	DTA better practice	ANAO assessment[a]	
Business validation and approval	Business end-users have verified and validated outputs to ensure they meet operational requirements and follow expected behaviour. Business approval has been provided and documented for deployment of the AI system.	■	DHDA advised the ANAO in April 2026 that evidence of verification and validation of model outputs was not consistently captured. DHDA advised that business approval prior to deployment, and for changes, was not consistently captured. In some cases, approval was provided verbally only. The February 2026 Requirements and Change Management Framework and a July 2026 Governance Framework and Agreement establish requirements and expected practice for capturing business approval within the change and release workflow.
Technical validation and approval	The technical authority has performed verification and validation activities to verify the correctness, consistency and completeness of the AI system. Technical approval has been provided and documented for deployment of the AI system.	▲	DHDA advised ANAO in March 2026 that technical testing of code quality, logic, and alignment with business rules is expected before technical approval of changes. Technical approval for the initial deployment was documented within the fraud detection system's code release management solution, however specific testing steps were not documented. DHDA advised the ANAO in April 2026 that system configurations to enforce mandatory approval of changes to the fraud detection system prior to deployment were not fully implemented until early 2026. DHDA advised it had identified deployed changes to models without corresponding technical approval or testing before this point. The February 2026 Requirements and Change Management Framework does not require formal recording of testing outcomes.
Deployment and change management	AI system deployments are planned, documented, approved, and controlled prior to release, and align with the agency's established governance, change management and delivery processes.	▲	Deployment of models in the fraud detection system is supported through staged development, testing and production environments with rollback capabilities. Technical testing of changes is expected before approval, and system configurations as of early 2026 required technical approval of changes prior to deployment. Formal documentation of deployment planning, testing and approval prior to AI model deployment was limited. DHDA advised the ANAO in April 2026 they had identified deployed changes to models without corresponding technical approval or testing. While the February 2026 Requirements and Change Management Framework and July 2026 Governance Framework and Agreement require testing and approval of changes, they do not consider planning for and approving deployments.

Component	DTA better practice	ANAO assessment[a]	
Operational monitoring in production	Operational metrics and risk management are in place to continuously monitor system performance and manage risks.	▲	Logging within the fraud detection system is primarily designed for traceability to support manual investigation of failures. DHDA advised the ANAO in January 2026 that it is planning to implement standardised performance metrics to better support monitoring of AI systems. Incorporating metrics would assist in establishing structured real-time processes to assess model performance and help with the early detection of performance degradation and ongoing reliability. DHDA advised the ANAO in August 2026 that planned real-time monitoring enhancements were not yet implemented.
Ongoing testing and continuous improvement	AI systems are monitored during operation to ensure they continue to operate as intended and remain suitable for their purpose.	▲	Model performance is monitored through informal and irregular analysis of end user feedback of fraud detection outputs. See paragraphs 5.9 to 5.13 for fraud detection system evaluation findings. Monitoring informed a December 2025 decision to transition from the AI-enabled model to a non-AI logistic regression model in the fraud detection system. Documentation of historical model refinements and analysis of this feedback is limited. DHDA advised the ANAO in January 2026 that it is planning to implement capabilities for real time monitoring of end user feedback. Integrating structured continuous performance monitoring will assist with the early detection of degradation in performance to ensure ongoing reliability and relevance.

Key: ■ Not aligned ▲ Partly aligned ◆ Largely or fully aligned

Note a: The AI-enabled model of the fraud detection system was switched to a non-AI logistic regression model in December 2025. DHDA advised the ANAO in March 2026 that they intend to use AI-enabled models in the fraud detection system in the future.

Source: ANAO analysis informed by better practice drawn from AS ISO/IEC 42001:2023 *Information technology — Artificial intelligence — Management system* and the DTA's *Technical standard for government's use of artificial intelligence*.

Opportunity for improvement

4.17 DHDA could implement controls for:

- the development of AI systems through: (a) strengthening system training, evaluation, and risk assessment practices; (b) developing and applying fairness assessments, including quantitative metrics; and (c) improving documentation across the artificial intelligence lifecycle, including in the development phase; and
- the deployment of AI systems through having appropriate approvals, and monitoring and operation plans in place, before deployment.

Assurance that enterprise-wide AI use is being managed within expectations and in accordance with legal and policy frameworks is incomplete. Assurance planning and processes are developing.

4.18 DHDA has an entity-wide Assurance Framework (September 2021) that 'provides detailed guidance for staff at all levels to understand and deliver their assurance responsibilities' and states that:

> Assurance … is designed to provide confidence to leaders and decision makers that aspects of [DHDA's] business are being managed within expectations and in accordance with legal and policy frameworks.

The framework identifies activities based on the level of assurance confidence needed and sets out six phases to prioritise activities based on risk. Forms of assurance can include: risk analyses; internal audit; performance reporting; forecasts; actual-to-budget comparisons; control or transactional data reporting; surveys; live assurance; project gate reviews; evaluations; independent reviews; and post implementation reviews. The framework states that it is the responsibility of business areas to identify assurance need, conduct assurance, implement any recommendations and communicate these actions to decision-makers.

4.19 DHDA identified an AI-related risk to the protection of personal data in July 2023 (see paragraph 2.9) and the Executive Committee discussed the risk of uncontrolled AI use by staff in June 2024. In February 2025 DHDA completed an internal audit on Readiness for Artificial Intelligence Use, the objective of which was to:

> assess whether the department has effective risk management, governance structures, and compliance frameworks in place to guide and control the transparent, ethical and secure implementation of AI technologies.

The internal audit concluded that DHDA 'is gathering data, resources, and expertise, to support successful AI integration' and made six recommendations. As of August 2026 four recommendations were closed (performing risk assessments (see Table 4.1), AI incident management practices (see paragraph 4.20), training (see paragraph 2.23) and training needs analysis (see paragraph 2.24)), and two remained open (AI policy (see paragraph 2.15) and use case register (see Table 4.1)).

4.20 A June 2026 Five Eyes cyber security agencies statement *The AI shift in cyber risk: why leaders must act now* emphasised urgency around AI stating 'AI is not a future consideration – it is already here.'[101] Version 1.1 of the *Policy for the responsible use of AI in government* suggested agencies integrate AI considerations into existing entity frameworks for privacy, protective security, record keeping, cyber and data. The internal audit recommended integrating AI-related incident management practices into DHDA's existing incident management frameworks. DHDA closed the recommendation in November 2025 following a review of relevant policy documentation and the addition of 'explicit AI incident requirements across the full-service operation lifecycle.' Four DHDA incident management policies were updated in January 2026 to include general references to AI and to state that the department would adhere to the *Policy for responsible use of AI in government.* A cyber security incident management policy was not updated. Recommendation closure documentation stated that residual risk would be tracked through quarterly AI incident key performance indicators, with results reported to IT governance forums. DHDA advised the ANAO in May 2026 that there is no risk reporting to IT governance forums as AI is not currently used for incident, event, problem or service management and that 'As AI is not currently being used … it is not beneficial for the Department to introduce metrics that cannot be measured'.

Recommendation no. 3

4.21 The Department of Health, Disability and Ageing strengthen assurance by:

(a) ensuring its cyber security policies reflect the unique risks posed by artificial intelligence and are updated in a considered way; and

(b) ensuring closure documentation for internal and external reviews and audits is clear, comprehensive and relevant to ensure that decision-makers have full visibility of the basis for closure.

Department of Health, Disability and Ageing response: *Agreed*

4.22 *The Department of Health, Disability and Ageing will review relevant cyber security policies, incident management documentation and response playbooks to ensure cyber security AI-related risks, incidents, escalation pathways and accountabilities are appropriately considered. The department will align this work with its broader artificial intelligence policy and governance arrangements. This will ensure cyber security controls align with emerging risks and whole-of-government requirements. Additionally, the department will strengthen its reporting arrangements for internal and external audits to support clear, consistent and evidence-based closure decisions.*

4.23 In November 2025 the Digital Committee (see Appendix 3) was advised that DHDA did not have good AI 'enforcement', with users having 'unrestricted access to AI via web browsers.' By January 2026 DHDA had identified several incidents involving the misuse of AI, including uploading of protected documents to public AI platforms and breaches by third-party providers resulting in

101 Five Eyes, *The AI shift in cyber risk: why leaders must act now*.

the exposure of personal and health information.[102] The Digital Committee was advised to introduce controls over staff use of external AI tools in two stages: a soft block on unapproved AI sites (redirecting users to guidance and allowing temporary access) followed by a hard block after a defined period. Suggested controls limiting the use of unapproved AI tools included: web filtering and site blocking; review and approval of software and web browser extensions before use; security awareness and training of staff; and AI governance frameworks. Once controls were implemented, DHDA planned to have ongoing monitoring of usage and access requests. The AI subcommittee endorsed the approach in January 2026 and the Digital Committee endorsed the approach in April 2026. As of August 2026 DHDA was undertaking a phased implementation approach with a pilot group participating in a soft-block trial and communications being developed for a broader rollout to all staff.

4.24 In January 2026 DHDA identified unapproved AI being used to automate 955 business or service delivery processes in a 'default' environment[103] that is unmonitored by DHDA. DHDA advised the ANAO in May 2026 that: the environment is used for learning and experimentation; is not centrally managed; does not meet DHDA's requirements for running live or business-critical systems; and is not a live production environment. The issue was identified to Digital Committee subcommittees in March and April 2026, including the AI subcommittee, and to the Audit and Risk Committee in April 2026. In response, DHDA planned to: implement a forum to regularly review features and controls in place for external AI systems in use in the department; review the list of business processes involved to migrate them to an appropriate environment; review how to strengthen and monitor controls; and consider regularly cleaning out the default environment. DHDA advised the ANAO that as of July 2026 a 'discovery phase' was in progress to determine required processes, with unrequired business or service delivery processes in the default environment to be deleted and required processes to be moved to a managed environment.

4.25 In 2025 a draft AI Assurance Framework set out planned assurance activities, which included: documenting AI use; reviewing use case risk assessments; governance oversight and approvals; and monitoring AI use, risks, outcomes and value. The draft framework stated that it applied only to the 'problem definition' stage (that is, the establishment of AI use cases) and stated that the Centre of Excellence and AI subcommittee would receive AI use case monitoring reports half yearly (for medium risk use cases) or quarterly (for high risk use cases). The draft framework was endorsed by the AI subcommittee in October 2025 and provided to the Digital Committee for endorsement in February 2026. The Digital Committee did not endorse the framework and requested that it better align with DHDA's entity-wide Assurance Framework, particularly the latter's emphasis on the 'three lines of defence' (business; enabling functions/committees; and internal audits). DHDA redrafted the framework to align to DHDA's overall assurance framework, to include reference to the full lifecycle and controls and monitoring arrangements to provide assurance that use of all internal and external artificial intelligence systems and tools is consistent

102 DHDA advised the ANAO in March 2026 that internal staff who misused AI tools were notified of the breach, reminded of their obligations under departmental policies, and referred to internal mandatory training for AI and other internal resources, and that their managers were informed. For third party incidents, DHDA advised that cyber security personnel 'actively engaged' with the parties to understand the impact, advise on management and require the parties to demonstrate uplift in internal processes, awareness and AI training.

103 A default environment (otherwise described as a 'sandbox') is a shared workspace typically used for developing prototypes or experimenting. If it lacks normal enterprise security or controls, it should not be used for sensitive data or critical functionality.

with relevant policies and guidance. In June 2026 the Digital Committee endorsed the framework in principle, agreeing to further refinement 'to ensure it is practical, scalable and proportionate to operational demand'.

4.26 DHDA advised the ANAO in January 2026 that assurance mechanisms included its: ICT Acceptable Use Policy; draft AI Assurance Framework; use case register process; acknowledgement of terms and conditions for Microsoft 365 Copilot access; and the Centre of Excellence. As of August 2026 DHDA had not established a start date for the use case assurance activities set out in the draft AI Assurance Framework or reporting to oversight committees.

5. Monitoring, evaluating and reporting the impact of artificial intelligence

Areas examined

This chapter examines whether the Department of Health, Disability and Ageing (DHDA) effectively monitored, evaluated and reported on the impact of the use of artificial intelligence (AI), with a focus on the Medicare Benefits Schedule (MBS) fraud and non-compliance detection system (fraud detection system).

Conclusion

Monitoring, evaluation and reporting on the cost and impact of AI use in the department has been largely limited to a Microsoft Copilot rollout. DHDA considers the evaluation of business area AI use cases to be the responsibility of individual use case owners.

Whole-of-government and DHDA AI policies do not require the development of cost-benefit analyses for AI use cases. There has been no analysis of the costs of developing the MBS fraud detection system, including the costs of developing the AI-enabled model within it. There has been some analysis of the system's benefits in terms of new potential fraud matters identified (and potential net recoveries), which does not specifically examine the tangible and intangible benefits of AI use.

Eight potential non-compliance or fraud matters were created and referred for preliminary analysis using, in part, the AI-enabled model in the MBS fraud detection system. While ad hoc preliminary performance analysis showed the AI-enabled model was efficacious, it was not used after December 2025, when it was determined that resourcing required for manual assessment of fraud and non-compliance 'signals' could not keep up with the volume of potential matters generated. There was no corresponding assessment of the benefits and costs of this decision. There has been some reporting to governance committees about the performance of the MBS fraud detection system, which has not specifically examined the role of AI in the system. DHDA's compliance activity remains limited relative to the estimated cost of MBS provider non-compliance.

Areas for improvement

There was one opportunity for improvement aimed at supporting assessment of benefits realisation of AI use cases.

5.1 The *Policy for the responsible use of AI in government* states that entities must 'regularly monitor and evaluate their use case to ensure it is operating as intended and that risks are being effectively managed.'[104] DHDA has an entity-wide Assurance Framework (see paragraph 4.18), which includes program and project evaluation.

5.2 With a particular focus on the MBS fraud detection system, this chapter examines whether DHDA is effectively: monitoring and evaluating the efficiency and effectiveness of AI use; and reporting on the impact of its AI use.

104 DTA, *Policy for the responsible use of AI in government*, version 2.0, p. 15.
Version 1.1 of the policy suggested entities monitor AI use cases to assess for unintended impacts. DTA, *Policy for the responsible use of AI in Government*, version 1.1, p. 13.

DHDA has not analysed costs, benefits and net returns from the fraud detection system. There has been some analysis of the AI-enabled model in the fraud detection system.

Cost-benefit analysis

5.3 Objectives of DHDA's October 2025 AI Strategy and Roadmap (see paragraph 2.14) include tracking AI use case value. Whole-of-government and DHDA AI policies do not require the development of cost-benefit analyses for AI use cases (see Table 4.1). Whole-of-government frameworks do not discuss documenting the costs of AI use. Cost analyses improve understanding of the resources involved in developing and implementing AI use cases to inform cost/benefit and overall value-for-money assessments.

5.4 Auditor-General Report No.17 2020–21 *Managing Health Provider Compliance* found that DHDA did not estimate or monitor the cost of its compliance activities and consequently could not calculate the net return on investment. The audit recommended costing health provider compliance activities to enable calculations of net return.[105] DHDA agreed to the recommendation, developed a compliance cost model (incorporating a costing methodology and tool) and closed the recommendation in June 2021. DHDA advised the ANAO in April 2026 that the compliance cost model was not actively maintained.

5.5 Between July 2024 and December 2025, analysis identified that eight[106] potential non-compliance or fraud matters were created and referred for preliminary analysis using, in part, the AI-enabled model. As of February 2026, three had a detection report finalised and were awaiting analysis and five had been analysed and confirmed to be potential fraud (1) or non-compliance (4). The five confirmed cases were referred for further investigation or audit. DHDA advised the ANAO in February 2026 that no money had yet been recovered. In 2024–25, $44,665,565 of debt was raised against 3,779 identified cases of MBS fraud and non-compliance.

5.6 There has been no analysis of costs, and an unclear analysis of benefits and net returns, from the investment in the fraud detection system, including the AI-enabled model.

- Calculation of costs — DHDA did not use the compliance cost model to calculate the cost of developing and using the fraud detection system, including the AI-enabled model. The 2023–24 federal Budget measure *Strengthening Medicare — improving Medicare integrity* included costings at a high level but did not specify costs for developing the fraud detection system. DHDA advised the ANAO in April 2026 that the compliance cost model had not been updated to include relevant data that would have allowed for its use in this instance due to structural changes and a review of the broader Benefits Integrity Division operating model. DHDA did not otherwise develop a budget for its work on the fraud detection system or calculate the actual cost of its development or use.
- Calculation of benefits — The value of potential fraud or non-compliance associated with the eight matters was estimated to be $5,253,601. Analysis identified that the eight matters combined results from different models, including non-AI models (see

105 Auditor-General Report No.17 2020–21 *Managing Health Provider Compliance*.

106 DHDA advised the ANAO in February 2026 that other cases identified through fraud detection system models had already been identified and referred for treatment through another mechanism, such as tip-offs.

Figure 1.3), and results reporting did not differentiate. The analytic approach therefore did not generate useful insights into the unique benefits of AI usage in the system.

- Comparison of costs and benefits — The Benefits Integrity Division had an average staffing level of 358 in April 2026 and an operating budget of $42.77 million for 2025–26. DHDA did not compare the cost of developing and using the AI-enabled model against potential net recoveries[107] or other intangible benefits. Patterns or data anomalies detected using the fraud detection system have informed policy considerations, including 2026–27 federal Budget proposals.

5.7 Through portfolio budget statements Program 2.6 (Health Benefit Compliance), DHDA aims to '[s]upport the integrity of health benefit claims through prevention, early identification and treatment of incorrect claiming, inappropriate practice and fraud.'[108] Performance measure 2.6A ('[p]ercentage of completed audits, practitioner reviews and investigations that find non-compliance') does not address supporting the integrity of health benefit claims and treating non-compliance for the MBS, Pharmaceutical Benefits Scheme or Child Dental Benefits Schedule.

Opportunity for improvement

5.8 DHDA could consider an approach to benefits realisation that includes criteria for identifying which AI use cases warrant benefits realisation analysis, supported by proportionate requirements for undertaking that analysis.

Analysis of AI model performance

5.9 In December 2023 DHDA calculated the number of health providers exhibiting benefits claiming behaviours known to be associated with fraud. Higher volumes of providers were identified than could be manually assessed. DHDA identified an opportunity to focus on riskier providers through the fraud detection system by developing the AI-enabled model.

5.10 In January 2024 DHDA tested prototype model outputs to confirm the model's efficacy at identifying possible fraud matters.

5.11 The AI-enabled model was deployed from July 2024 to December 2025. Monitoring of AI model performance was irregular and inconsistently documented. Preliminary analysis of the six models within the fraud detection system, each of which cover different claiming behaviours or characteristics (see Figure 1.3), was undertaken in August 2025 to 'identify well performing and potentially redundant model [and] further model development and consolidation'. This showed that the AI-enabled model accurately identified matters 22 per cent of the time (Table 5.1).

107 DHDA advised the ANAO in May 2026 that recovery of debt is contingent on the finalisation of compliance action or prosecutions, which can take many years.

108 DHDA, *Department of Health, Disability and Ageing 2024–25 Annual Report*, pp. 100–103.

Table 5.1: Analysis of MBS fraud detection system model performance during the period August 2023 to August 2025

	Potential matters identified[a]	Potential matters reviewed	Review rate	True positive[b]	False positive	True positive rate[c]
Model 1 (AI-enabled)	**597**	**82**	**14%**	**18**	**64**	**22%**
Model 2	990	119	12%	12	107	10%
Model 3	600	287	48%	251	36	87%
Model 4	675	272	40%	16	256	6%
Model 5	1,016	345	34%	158	187	46%
Model 6[d]	598	127	21%	63	64	50%
Model 7[d]	344	87	25%	41	46	47%

Note a: Number of potential matters identified for manual processing (see Figure 1.4 for the process). Potential matters identified can include multiple matters identified at different times for the same provider.

Note b: The eight cases of potential non-compliance or fraud matters created and referred for preliminary analysis using, in part, the AI-enabled model (see paragraph 5.5) fall within the 'true positive' category.

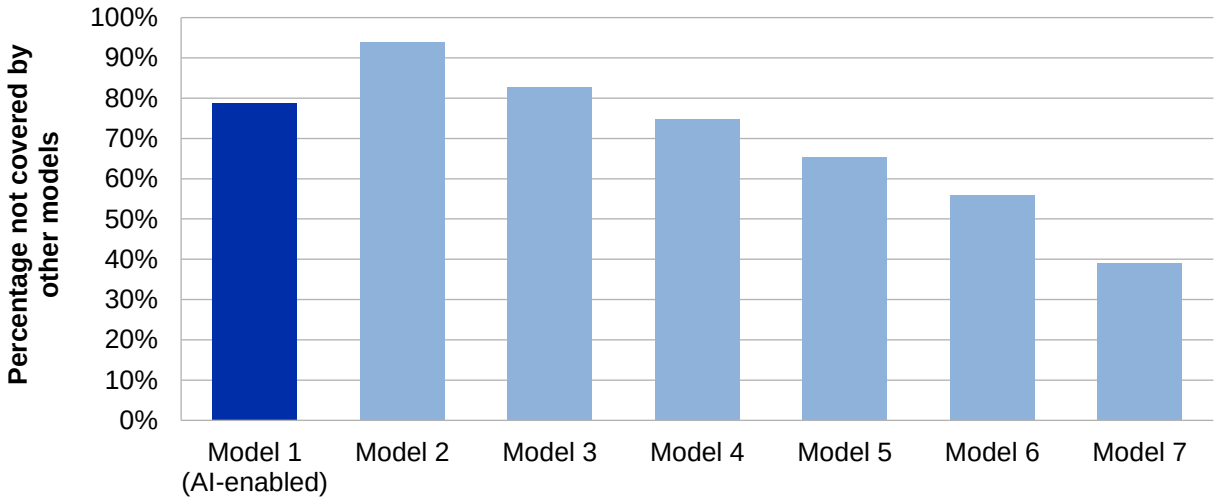
Note c: DHDA advised the ANAO in May 2026 that it is not appropriate to compare the true positive rates of different models as they are searching for different behaviours. The nature and characteristics of different fraud typologies mean that some behaviours are more difficult to clearly identify in data alone.

Note d: Models 6 and 7 are versions of the same model used over different time periods.

Source: Adapted by ANAO from DHDA documentation.

5.12 A preliminary 'model overlap' analysis undertaken at the same time showed that the AI-enabled model uniquely identified 'new' providers (that is, providers not identified by other models within the fraud detection system) approximately 80 per cent of the time (Figure 5.1).

Figure 5.1: Analysis of MBS fraud detection system model performance overlap during the period August 2023 to August 2025[a]



Note a: The analysis examined the number of providers identified uniquely through each model. Multiple matters could be identified for the same provider. DHDA advised the ANAO in May 2026 that it is not appropriate to compare overlap rates given the models are searching for different behaviours and a health provider may be demonstrating multiple characteristics of known fraud typologies. Models 6 and 7 are versions of the same model used over different time periods.

Source: Adapted by ANAO from DHDA documentation.

5.13 In December 2025 DHDA concluded that the AI and non-AI models 'performed well' but the AI-enabled model was a 'drain on the resources' as it generated 'more selections' of potential fraud or serious non-compliance for manual assessment. DHDA did not document a formal analysis to inform this conclusion. DHDA advised the ANAO in February 2026 that in December 2025 a decision was made to cease using the AI-enabled model in favour of a logistic regression model because the logistic regression model also performed effectively, and had the benefit of using additional parameters and a threshold to enable direct control over the volume of selections for manual assessment. DHDA did not assess benefits and costs of the decision nor document the change from the AI-enabled model to the logistic regression model. DHDA advised the ANAO in May 2026 that a business decision was subsequently made to use the logistic regression model based on the model's comparable efficacy and the available resourcing to perform manual assessment. DHDA did not compare efficacy of the models nor assess model output against available resourcing.

5.14 DHDA advised the ANAO in March 2026 that the performance of the AI-enabled model was continuing to be assessed and it was 'yet to be decided' whether the AI model would be retrained for future use. DHDA advised that it planned to implement other AI-enabled models in the fraud detection system, which it anticipated would be useful for targeting complex fraud.

Project evaluation

5.15 As of February 2026, a Microsoft 365 Copilot (Copilot) rollout across DHDA was 99 per cent completed, with a budget underspend. In November 2025 DHDA completed a Copilot experience and usage survey about adoption, perceived time savings, trust, confidence, satisfaction, ethical use, stress reduction, empowerment, workload control, concerns, and managerial perspectives. The majority of respondents estimated that they saved 30 minutes or more per week through Copilot use. The survey report recommended investing in advanced training, enforcing governance protocols and implementing trust-building measures.

5.16 DHDA advised the ANAO in May 2026 that as no other enterprise level AI tools are in use, no other evaluations are planned or in process, and that evaluation of individual use cases is the responsibility of use case owners.

There has been limited reporting on AI value and impact to governance committees.

5.17 Between June 2025 and February 2026, DHDA monitored and reported on the Copilot rollout to the project's Senior Responsible Officer[109] via monthly internal project reporting mechanisms. Updates on AI to the Audit and Risk Committee focused on implementation of the Copilot trial. The Executive Committee received updates on the Copilot trial in June 2024 and April 2025. Copilot survey results were presented to the Corporate Operations Board, responsible for overseeing the Copilot rollout, in November 2025.

5.18 Internal monthly reporting via standard reporting mechanisms to the Senior Responsible Officer[110] and Corporate Operations Board[111] for the *Strengthening Medicare — improving*

109 The Senior Responsible Officer for the Copilot project was an assistant secretary in the Information Technology Division.

110 The Senior Responsible Officer is the First Assistant Secretary of the Benefits Integrity Division.

111 The Corporate Operations Board monitors corporate project delivery and benefits realisation.

Medicare integrity federal Budget measure included reporting on the implementation of fraud detection methods. The reporting included content on the development of models within the fraud detection system and on suspected fraud matters identified using data analytics. There was no specific focus in reporting on the use of AI.

5.19 As of April 2026 the Digital Committee and AI subcommittee were largely focused on establishing AI governance and assurance frameworks and neither they nor the Executive Committee had received any reporting on the efficiency and effectiveness of other AI implementation in DHDA.

Dr Caralee McLiesh PSM
Auditor-General

Canberra ACT
2 September 2026

Appendices

Appendix 1 Entity response

Australian Government

Department of Health, Disability and Ageing

Acting Secretary

Dr Caralee McLiesh PSM
Auditor-General for Australia
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Dr McLiesh,

Department of Health, Disability and Ageing's response to the Proposed Audit Report – *Artificial Intelligence and Medicare Benefits Integrity*.

Thank you for providing the Australian National Audit Office's (ANAO) proposed report pursuant to section 19 of the *Auditor-General Act 1997* on the audit of the *Artificial Intelligence and Medicare Benefits Integrity*. I appreciate the opportunity to respond to the report.

The Department of Health, Disability and Ageing welcomes the audit and its focus on ensuring the Australian Government's use and oversight of artificial intelligence continues to evolve in a manner that supports accountability, transparency and public trust. The department agrees with the findings and recommendations and is committed to further strengthening its artificial intelligence governance, risk management and assurance arrangements.

The department welcomes the audit's recognition of the governance arrangements established that support artificial intelligence adoption. The department has taken significant steps to align with emerging whole-of-government requirements. These findings provide a strong foundation on which to continue maturing the department's artificial intelligence capability and assurance arrangements.

The department acknowledges the importance of understanding and managing the broader implications of artificial intelligence use across the health system. While the

Phone: (02) 6289 8400 **Email:** Blair.Comley@health.gov.au
Yaradhang Building, 23 Furzer Street, Woden ACT 2606 - GPO Box 9848 Canberra ACT 2601 - **www.health.gov.au**

audit's scope was focused on Medicare benefits integrity, the opportunities and risks associated with AI adoption extend beyond compliance and integrity considerations. The department will consider these broader issues through relevant programs, functions, regulatory frameworks and department governance and risk management arrangements, drawing on expertise across the department and engagement with external stakeholders.

In responding to Recommendation 1, the department will build on existing Medicare integrity arrangements with Services Australia to identify, assess and manage artificial intelligence-related risks that may affect health benefits integrity and provider claiming compliance. This targeted work will enhance the department's understanding of emerging Medicare integrity risks and the effectiveness of existing controls, while maintaining a focus on preventing and responding to incorrect, inappropriate and fraudulent claiming.

The wording provided for the Summary Response can be found at Attachment A and the response to each recommendation directed to the department can be found at Attachment B.

I would like to thank the ANAO for its professionalism throughout the audit.

If you have any questions regarding the department's response please contact Pat Janek, Assistant Secretary, Assurance Branch on (02) 5132 4774.

Yours sincerely

Celia Street

07 September 2026

Appendix 2 Improvements observed by the ANAO

1. The existence of independent external audit, and the accompanying potential for scrutiny improves performance. Improvements in administrative and management practices usually occur: in anticipation of ANAO audit activity; during an audit engagement; as interim findings are made; and/or after the audit has been completed and formal findings are communicated.

2. The Joint Committee of Public Accounts and Audit (JCPAA) has encouraged the ANAO to consider ways in which the ANAO could capture and describe some of these impacts. The ANAO's corporate plan states that the ANAO's annual performance statements will provide a narrative that will consider, amongst other matters, analysis of key improvements made by entities during a performance audit process based on information included in tabled performance audit reports.

3. Performance audits involve close engagement between the ANAO and the audited entity as well as other stakeholders involved in the program or activity being audited. Throughout the audit engagement, the ANAO outlines to the entity the preliminary audit findings, conclusions and potential audit recommendations. This ensures that final recommendations are appropriately targeted and encourages entities to take early remedial action on any identified matters during the course of an audit. Remedial actions entities may take during the audit include:

- strengthening governance arrangements;
- introducing or revising policies, strategies, guidelines or administrative processes; and
- initiating reviews or investigations.

4. In this context, the below actions were observed by the ANAO during the course of the audit. It is not clear whether these actions and/or the timing of these actions were planned in response to proposed or actual audit activity. The ANAO has not sought to obtain assurance over the source of these actions or whether they have been appropriately implemented.

- In October 2025 the Department of Health, Disability and Ageing (DHDA) finalised an artificial intelligence (AI) Strategy and Roadmap (see paragraph 2.14) and drafted an AI Assurance Framework (paragraph 4.25).
- In November 2025 DHDA mandated AI fundamentals training for all staff (paragraph 2.23).
- In December 2025 DHDA considered the benefits of using an AI-enabled model and a non-AI model in the Medicare Benefits Schedule fraud and non-compliance detection system (fraud detection system) (paragraph 5.13).
- In January 2026 DHDA documented roles and responsibilities for stages of the fraud detection system development lifecycle (Table 4.2).
- In January 2026 DHDA's AI subcommittee endorsed the introduction of controls over staff use of external AI tools (paragraph 4.23).
- In January 2026 DHDA drafted an AI policy (paragraph 2.15).
- In January 2026 DHDA formed the Centre of Excellence (Appendix 3).
- In February 2026 DHDA updated its AI transparency statement (paragraph 2.17).
- In February 2026 DHDA finalised a Requirements and Change Management Framework to improve documentation and other processes related to the development and deployment of AI systems (Table 4.2).

- In March 2026 DHDA 'enforced' the mandatory review and approval of changes to the fraud detection system prior to production release (Table 4.3).
- In March 2026 DHDA finalised a training needs analysis for AI (paragraph 2.24).
- In March 2026 DHDA's AI subcommittee discussed the potential implications for DHDA arising from the Productivity Commission's 2025 report on *Harnessing Data and Digital Technology* and created an action item to consider the recommendations (paragraph 3.17).
- In March 2026 DHDA performed an analysis of changes to billing by different software vendors (paragraph 3.16).
- In April 2026 DHDA's Digital subcommittee endorsed the introduction of controls over staff use of external AI tools (paragraph 4.23).
- In May 2026 DHDA provided the ANAO a draft privacy threshold assessment (Table 4.1).
- In May 2026 DHDA drafted a 'use of prompted billing software in Medicare' strategic intelligence report (paragraph 3.10).
- In May and June 2026 DHDA made amendments to the draft AI Framework drafted in October 2025, to better incorporate the full AI lifecycle and controls and monitoring arrangements (paragraph 4.25).
- In June 2026 DHDA completed an AI stocktake (paragraph 2.16).
- In July 2026 DHDA intended to seek legal advice from the Australian Government Solicitor on a draft privacy impact assessment for the fraud detection system (Table 4.1).
- In July 2026 DHDA finalised a Governance and Framework Agreement for the fraud detection system (Table 4.3).

Appendix 3 Selected governance committees

Table A.1: Selected enterprise level governance committees, as of April 2026

Committee	Objective and functions	Members	Meeting frequency
Executive Committee	Provides strategic direction and leadership to ensure the department delivers its objectives set out in the Corporate Plan and portfolio budget statements. The committee's role includes monitoring and addressing departmental performance and risks.	• Secretary (Chair) • All deputy secretaries • Individuals can attend in an advisory capacity at the discretion of the Chair	Required fortnightly. In practice, the committee met weekly between January and June 2023 and then fortnightly most months between July 2023 and April 2026.
Digital Committee *Established January 2025*	Oversees the Department of Health, Disability and Ageing's (DHDA's) digital, data and ICT functions and capabilities. Functions include the identification of key portfolio risks associated with digital, data and ICT assets and operations, including understanding the impact on business outcomes, approving treatment and mitigation activities and monitoring their effectiveness.	• Chief Medical Officer and Deputy Secretary (Chair) • Chief Digital Information Officer (Deputy Chair) • All deputy secretaries (members but do not count towards quorum) • 10 first assistant secretaries and 1 assistant secretary (core members) There are no members from the Benefits Integrity Division.	Required monthly initially, then every 6 weeks once the committee determines this is appropriate. In practice, the committee met monthly from February to May 2025 and then generally every six weeks to April 2026.
Artificial Intelligence (AI) subcommittee to the Digital Committee *Established June 2025*	Stewards the department's approach to AI and advises the Digital Committee on: • the application of AI; • the use and regulation of AI in the health, disability and aged care sectors; • the use of AI within the department; and • the whole of government approach to AI and the intersection with the health, disability and aged care sector.	• 2 first assistant secretaries (co-chairs) • 38 members from across the department including first assistant secretaries, assistant secretaries, senior medical advisors, directors, branch and group managers and officials at other levels. There are no members from the Benefits Integrity Division.	Required monthly, between meetings of the Digital Committee. In practice, the subcommittee met most months between June 2025 and April 2026.

Committee	Objective and functions	Members	Meeting frequency
	Functions include: • promoting the opportunities and risks of AI, supporting the realisation of benefits and mitigating risks throughout the health and care sector; • advising the Digital Committee on good practice, risk mitigation and related considerations in DHDA under the *Policy for the response use of AI in government*; and • reviewing high risk AI use cases and providing recommendations to the Digital Committee aligned with AI use case governance processes.		
Centre of Excellence *Established January 2026*	Advisory body to the AI subcommittee, including to make governance recommendations. Provides advice on ethical and responsible use of AI to business areas, and analyses medium and high-risk AI use cases.	The draft terms of reference details core members of a chair and secretariat along with subject matter experts for AI policy, ethics, AI technical, legal, enterprise data and analytics, data governance, cyber security, and cyber architecture. There are no members from the Benefits Integrity Division.	Draft terms of reference state that the frequency and duration of meetings is to be determined by members. Four meetings were held between January and March 2026. Meetings were then 'paused' to finalise the AI assurance framework, AI policy, and the new AI use case register.

Source: ANAO analysis of DHDA documentation.

Table A.2: Selected benefits integrity governance committees, as of April 2026

Committee	Objective and functions	Members	Meeting frequency
Strategic Business Committee *Established 2018*	Supports the statement of intent between DHDA and Services Australia. The committee has oversight of the Australian Government's health, disability and aged care program delivery. The committee discusses areas of mutual interest, including cross-program and future priorities such as cyber security, AI and automation.	Senior executive service (SES) Band 1 and 2 officials from DHDA and Services Australia. The First Assistant Secretary for the Benefits Integrity Division is a member.	Required every second month. In practice the committee met every 1–4 months between March 2023 and April 2026.
Medicare Integrity Reform Program Board *Established August 2023*	Formed under the *Strengthening Medicare — improving Medicare integrity* 2023–24 federal Budget measure, the board oversees the progress and implementation of work undertaken by DHDA and Services Australia in delivering the *Strengthening Medicare — Improving Medicare Integrity* program. Functions include acting as a decision-making body ensuring strategic alignment, collaborative delivery of commitments and guiding and coordinating the overall work program.	Chaired by the First Assistant Secretary for the Benefits Integrity Division. Members are DHDA and Services Australia SES Band 1 and Band 2 officials, and an independent member from the National Disability Insurance Agency.	Required every second month. In practice the board met monthly from August 2023 to May 2024, then every 2–3 months.
Medicare Integrity Reform Steering Group *Established February 2025*	Established as an internal forum to support strategic decision-making and collaboration across the Benefits Integrity Division. Its purpose is to engage subject matter experts and support integrity reform initiatives. Functions include: supporting strategic decision making and collaboration in consideration of reform policy; collaborating on reform policy design and prioritisation; working to address complex and challenging reform policy issues, sharing insights, intelligence and best practice; and enabling cohesion and informed contributions to the integrity reform work program.	Members are from the Benefits Integrity Division, and other areas of DHDA as needed.	Required monthly. In practice, the steering group has met monthly since February 2025.

Source: ANAO analysis of DHDA documentation.