Australian Government
Department of Health and Aged Care

Fraud and Corruption Control Plan 2023-25

Secretary's Statement

The Department of Health and Aged Care (the department) is serious about preventing, detecting, and countering fraud and corruption. Public confidence and integrity in our people and the programs we are entrusted to deliver for Australians is vital to our operation.

The department is responsible for approximately $105 billion of administered spending and $1.2 billion in departmental spending.

The scale of these investments exposes the department to significant fraud and corruption risks which can reduce the resources available for delivering our services to the community and undermine public confidence in our programs.

All departmental officials (including staff, contractors and consultants) are required to model the behaviours outlined in the APS Values and Code of Conduct. This includes always being accountable and impartial, and not being influenced by personal interests or greed.

With an increased focus on fraud in other Government programs, and a strengthening of controls in those programs, fraudsters (including organised crime groups) will inevitably shift their operations to programs they perceive as more vulnerable, including potentially the department's programs. It is critical that all departmental officials consider fraud and corruption risks and implement fraud and corruption controls as a key part of their day to day policy design, program management and program delivery functions.

The department's Fraud and Corruption Control Plan (the Plan) documents our fraud and corruption prevention, detection, and response system. It shows how all departmental officials and those who undertake business with the department can recognise current fraud and corruption risks and vulnerabilities, and how they can integrate control strategies in their everyday business.

Professor Brendan Murphy AM

Secretary

June 2023

Fraud and Corruption Policy Statement

The Australian Government expects all Commonwealth officials or persons otherwise engaged through contract by the Commonwealth to collectively prevent, detect and deal with fraud and corruption. All departmental officials are expected to behave with integrity at all times. The department will take action to deal with fraudulent and corrupt behaviour.

Department's Integrity and Security Framework

This Fraud and Corruption Control Plan is a key component of the department's Professional Integrity and Security Framework, which guides the department in addressing key fraud, corruption and security risks that threaten infrastructure and service delivery. The department's Professional Integrity and Security Framework supports a range of prevention, detection and response measures to ensure a systemic and integrated approach to integrity across the department.

Definitions

Fraud

Fraud is defined in the Commonwealth Fraud Control Framework as *"dishonestly obtaining a benefit, or causing a loss, by deception or other means."*

Fraud can be committed by departmental officials, including staff, contractors or consultants, (internal fraud) or by persons or entities external to the department (external fraud). It may also be committed jointly between a departmental official and an outside party. Fraud offences against the Commonwealth may be prosecuted under a number of Commonwealth laws.

Some examples of the type of conduct by departmental officials or third-party providers that fall within the department's definition of fraud include:

- theft or misuse of Commonwealth information, intellectual property or confidential information (including funding proposals, procurement information, personal records)
- misuse of Commonwealth program funding and grants
- misuse of Commonwealth resources, including unlawful use of, or unlawful obtaining of, property, equipment, material or services
- abuse of official position in order to obtain a benefit for oneself or another
- misuse of entitlements (e.g. expenses, leave, travel allowances or attendance records, including abuse of time off in lieu)
- misuse of facilities (e.g. unauthorised use of information technology, mobile devices and telecommunications systems)
- financial or accounting fraud (e.g. unauthorised use of credit cards, false invoices, misappropriation)
- causing a loss, or avoiding and/or creating a liability
- providing false or misleading information to the Commonwealth, or failing to provide information where there is an obligation to do so
- making or using false, forged, or falsified documents
- release, or use of misleading information for the purposes of deceiving, misleading or to hide wrongdoing.

Corruption

Corruption is defined as *"dishonest activity in which a director, executive, manager, employee, member or contractor of an entity acts contrary to the interests of the entity and abuses their position of trust in order to achieve some personal gain or advantage for themselves or for another person or organisation."*[1]

Corruption is the misuse of entrusted power or authority for personal gain. The following list provides examples of types of behaviour that may amount to corruption:

- collusion between a Commonwealth official and a contractor
- bribery (domestic or foreign)
- obtaining, offering, or soliciting secret commissions, kickbacks, or gratuities
- one or more individuals manipulating a procurement process for personal gain
- nepotism: preferential treatment of family members
- cronyism: preferential treatment of friends and associates
- acting (or failing to act) on a conflict of interest
- unlawful disclosure of official or commercially sensitive information
- insider trading: misusing official information to gain an unfair private, commercial or market advantage for self or others.

Non-compliance

Non-compliance is a broad term for any failure to comply with legal requirements. These requirements may be in the form of laws, regulations, agreements, administrative rules, and licensing conditions. An example is the requirement for all officials of Commonwealth entities to comply with the 'General duties of officials' which are set out at sections 25-29 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).

Non-compliance includes activities where parties try to comply but makes mistakes (accidental non-compliance), or where parties exploit ambiguities or opportunities that are non-compliant (opportunistic non-compliance).

Governance

Key responsibilities

All departmental officials should understand what constitutes fraud and corruption, and what to do if they suspect fraudulent or corrupt activity. Building this understanding is supported by Essential Learning training modules, which are mandatory for all staff and contractors to complete.

All officials must comply with legislative requirements and internal policies, behave in accordance with integrity requirements, and identify and report fraud and corruption risks.

There are positions and committees which have additional responsibilities including:

- The **Secretary** is the accountable authority responsible under the PGPA Act for governing the department in a way that promotes the proper use of public resources. This includes taking all reasonable measures to prevent, detect and respond to fraud and corruption relating to departmental officials, service providers or third parties who

[1] Australian Standard (AS) 8001-2021: Fraud and Corruption Control

interact with the department. The Secretary must refer suspected serious or systemic corrupt conduct involving current or former departmental officials to the National Anti-Corruption Commission.

- The **Chief Financial Officer** has accountability for setting the department’s financial framework and ensuring that risks associated with the department's appropriations and expenditure are addressed.
- The **Chief Security Officer** provides strategic oversight and management of security across the department.
- The **Chief Information Security Officer** is accountable to the Chief Security Officer for the performance of the department’s Security Policy Framework and ensures security is considered within fraud and corruption control and awareness.
- The **Assistant Secretary, Fraud Control and Investigation Branch** has corporate responsibility for overseeing the implementation of fraud and corruption prevention and control for the department, in line with Section 10 of the PGPA Rule (the Fraud Rule) and for implementing the requirements of the Commonwealth Fraud Control Framework. This includes delivering a fraud and corruption control program that covers prevention, detection, investigation, recording and reporting strategies.
- The **Audit and Risk Committee (ARC)** oversees the department's system of risk management and internal controls, including fraud and corruption risk, and provides independent advice to the Secretary on their appropriateness, in accordance with section 45 of the PGPA Act.
- The **Executive Committee (EC)** provides strategic direction and leadership to achieve the outcomes set out in the department’s Corporate Plan and Portfolio Budget Statements. This Committee operates in an advisory capacity to the Secretary and promotes effective decision making and governance, monitoring and addressing of departmental performance and risks, shaping of organisational culture and capability development, and strategic advice on recommendations of the department’s senior governance committees.
- The **Security Workforce Integrity Assurance Committee (SWIAC)** provides assurance to the EC and the Secretary that security and workforce integrity risks are being efficiently and effectively managed. This committee also provides strategic oversight of security and integrity related business activities by fostering support to achieve positive security and integrity outcomes.
- **Public Interest Disclosure (PID) Officers** in the course of performing functions under the *Public Interest Disclosure Act 2013*, must refer suspected serious or systemic corrupt conduct involving current or former departmental officials to the NACC.
- **All Senior Executive Officers and managers** are responsible for leading the establishment and maintenance of an ethical culture within their business areas, together with the implementation and operation of governance arrangements. This includes:
  - ensuring that risks of fraud and corruption are considered in the planning and development of programs and the conduct of activities under their control
  - ensuring their staff understand and comply with relevant legislation, regulations, procedures, and policies. Examples are completing all mandatory eLearning essentials modules and declarations of conflicts of interest.
  - assisting relevant officials to conduct fraud control activities including fraud risk assessments.

Enterprise fraud and corruption risks

An Enterprise Fraud and Corruption Risk (EFCR) assessment is reviewed or conducted at least every 2 years and is conducted in accordance with the Commonwealth Fraud Control Framework and the AS/NZ ISO standards. The department's EFCRs are outlined below:

Risk	Examples
Grant funding	Grant recipients inappropriately misuse grant funding - resulting in reputation damage, negative impact on consumers and financial loss.
Provider claims	Providers make false claims, resulting in a financial benefit to which they are not entitled - resulting in reputation damage and financial loss.
Information management	Officials are offered benefits to release, sell and/or misuse data or information which may be sensitive or commercially valuable - impacting integrity of processes, reputation of the department, financial loss and privacy.
Procurement processes	Officials undertake procurement in a manner that benefits themselves or others - impacting value for money procurements.
Identity crime	Fictional individuals/companies are created and used to obtain a grant or make a claim on funds from the department - resulting in reputation damage and financial loss.
External influence	Officials are influenced by external parties to act in a way that provides a benefit, impacting on quality and safety of goods and services and reputation of the department.
Regulatory approvals	Fraud associated with regulatory approval processes, including applying for and granting regulatory licences/approvals/clearances, and misleading information to obtain approval - impacting on quality, safety and reputation of the department.
Conflict of interest	Conflicts of interest of internal and external individuals sitting on decision-making committees. Conflict of interest in employing contractors and engaging consultants - results in departmental mistrust and loss of value for money opportunities.
Credit card and travel fraud	Employee misuse of corporate credit cards and cab charges, and fraudulent claims for travel reimbursements - resulting in financial loss.
Employment-related fraud	Misleading or false information provided by individuals to obtain a position as an official within the department, or to obtain other benefits. Examples of officials providing misleading or false information includes timesheet fraud, falsification of leave forms and fraudulent claims of entitlements.
Misuse of department assets	Officials misappropriate, misuse or steal assets for personal gain - resulting in financial loss.
Misuse of IT systems	Officials misuse, manipulate or change IT systems intentionally to obtain a benefit leading to information, privacy, and security breaches.

Fraud and corruption controls

The department implements key control strategies to ensure an effective fraud and corruption control framework, including prevention, detection, response, and reporting, assurance, and monitoring.

Prevention

Fraud and corruption prevention strategies focus on establishing and maintaining sound governance systems, systems of control and an ethical organisational culture. Prevention strategies are the most cost-effective way to stop fraud and corruption, they prevent or limit the size of the wrongdoing by reducing the likelihood and consequences of fraud and corruption.

Key parts of the department's fraud and corruption prevention strategy include:

Fraud, security, and integrity awareness: all departmental officials must complete the department's Essential Learning Program which includes modules on fraud, security, and integrity. This program aims to ensure that all officials:

- can understand and identify threats or risks and implement controls, and
- are aware of their responsibilities and obligations while working in the department.

The program is to be completed within 30 days of commencement and is to be retaken every 12-24 months. The department monitors completion rates which are also reported to senior governance committees. This training is supplemented by Intranet sites, toolkits, events, and regular communications to raise awareness of fraud and corruption, security, and integrity related matters.

Declaring conflicts of interest: all departmental officials must perform their duties in a fair and impartial way such that personal interests, private affiliations, or the likelihood of personal gain or loss does not influence the performance of those duties. The department's Conflict of Interest Policy outlines the requirements and protocols relating to conflict of interest and aims to ensure that real or apparent conflicts of interest are identified, disclosed and managed in a transparent and accountable manner. All contract managers must ensure that Conflict of Interest declarations are in place, and monitored for contracted personnel, and must monitor the ethical behaviour of suppliers throughout the term of the contract.

Project and program fraud control: during the design stage, each program or project should seek to identify fraud and corruption vulnerabilities which could threaten successful outcomes. Program and project staff need to consider ways to prevent these threats through the implementation of effective controls. Programs and projects should identify what reporting and detection activities are required, how compliance with requirements will be monitored throughout the life of the project or program and their deliverables, and what responsive measures are required to ensure that if fraud or corruption does occur, the program has legislation, policy and processes in place to allow recovery.

Business and risk planning: fraud and corruption risks must be considered as part of the development of annual Divisional Business and Risk Plans. If any applicable enterprise fraud and corruption risks are identified, divisions should ensure appropriate controls are implemented as outlined in the department's EFCR register and this Plan.

Procurement and granting, and associated contract management controls: departmental officials responsible for procurement and granting activities must be satisfied, after reasonable enquiries, that the procurement or grant achieves a value for money outcome.

All officials must ensure and adhere to measures as directed by the Department's Chief Operating Officer and the Department of Finance in May 2023 to strengthen the ethical accountability of entities awarded Government contacts. These measures include adherence to Probity Principals, consideration of a potential supplier's relevant experience and performance history, due diligence activities to ensure information provided by tenderers and suppliers is current and accurate, and additional new clauses such as Notification of Significant Events.

Officials are required to undertake procurement and granting, and associated contract management activities in an efficient, effective, economical, and ethical manner that achieves value for money in a whole-of-process way. Health's Accountable Authority Instruction's (AAI) and applicable Finance Business Rules (FBR's) must be followed in all instances of procurement within the department.

All officials administering grants must comply with the department's Grant Toolkit. The Grant Toolkit steps staff through all the processes and documentation required to approve and draw up the appropriate paperwork for a grant.

Information controls: all departmental officials must take steps to protect departmental information including classifying information with protective markings, applying access controls, keeping a clear desk and being aware of surroundings.

Information Technology controls: the ICT Acceptable Use Policy provides direction and guidance for department personnel on the acceptable use of departmental Information Communication and Technology assets. The department uses a range of cyber security measures to ensure the safety and integrity of our systems and the information contained within it. All people administering or configuring new departmental systems must be aware of mandatory cyber security requirements.

Financial controls: the department maintains a set of financial controls to ensure a true and fair view of the department's financial performance, position and proper use and management of public resources that is consistent with the PGPA Act. A range of assurance initiatives are also in place to help ensure the integrity of financial data and management across the department.

Personnel controls: the Personnel Security Policy outlines the department's personnel security requirements at all employment or engagement stages, including before commencement, during employment or engagement and post-employment. This policy applies to all employment or engagement activities that are conducted by or on behalf of the department.

Detection

Effective systems are necessary to detect fraud and corruption as soon as possible to minimise impact on the department. Measures to detect internal and external fraud, as well as corruption within the department include:

Fraud and corruption reporting channels: the department has in place a range of reporting channels that allow customers, our people, the public, and other entities to report suspected fraud and corruption. Allegations are received in various forms, including feedback, audit and assurance findings, tip-offs, and monitoring activities. They are then assessed to determine if a formal investigation and/or compliance action is required or if fraud or corruption prevention strategies need to be applied. Any person (including members of the public and public officials) can voluntarily refer a corruption issue, or provide information about a corruption issue, to the NACC.

Public Interest Disclosure (PID) Scheme: this scheme provides a legislative framework for the protected disclosure and investigation of serious wrongdoing within the Commonwealth public sector. The department has PID procedures and a PID framework which applies to the disclosure, receipt, assessment, investigation, and response to PIDs made to the department. All officials are encouraged to report suspected wrongdoing meeting the definition of a PID via established reporting mechanisms.

Financial management compliance: the department conducts a range of activities to monitor financial compliance across the department. Fraudulent transactions are assessed and, where appropriate, referred for investigation. The Financial Management and Compliance System (FMCS) is a suite of governance and compliance modules supporting all government agencies operating under the PGPA Act. FMCS provides real time self-service and workflow approval functionality for registering non-compliance, hospitality applications, fringe benefits tax, and gifts and benefits from external parties.

Grant management compliance: the department works closely with the Community Grants Hub, the Business Grants Hub and the National Health and Medical Research Council (NHMRC) to administer grants across all Outcomes and most Programs. In undertaking grant establishment and management activities on behalf of the department, the hubs and the NHMRC refer serious non-compliance and any indications of fraud or corruption to the department for consideration.

Internal audit: an independent internal audit function has been established to conduct reviews into the department’s activities, systems and practices. This provides the department with audit services and a range of assurance activities that give line areas and the department the confidence that programs or functions are operating effectively.

Data analytics: the department uses data analytics to identify fraud and incorrect claiming, including data matching to identify anomalous claiming patterns, trends, and behaviours by health benefits providers.

Data sharing: internal and external data sharing is a powerful tool to prevent and detect fraud and corruption. Data and information sharing arrangements help verify the identity and eligibility of claimants, prevent claimants illegitimately accessing multiple supports and services, and disrupt fraud and corruption networks.

Response

Response controls are a key element in the overall fraud control framework. The primary objective is to ensure perpetrators are identified and appropriate remedies are applied to achieve a deterrent effect. Response strategies include:

Fraud and corruption investigation: all fraud and corruption investigations conducted by the department are undertaken in accordance with the Australian Government Investigation Standards (AGIS). This includes serious or complex criminal investigations, which may be referred to the Australian Federal Police, or corruption issues including PIDs, which may be referred to the NACC. Matters outside the departments' responsibility are referred to the relevant entity. All disclosures involving another agency's activities or programs will accord with the *Privacy Act 1988* and the Australian Privacy Principles.

Prosecution: where sufficient evidence of criminal conduct is identified, investigators will compile and refer briefs of evidence to the Commonwealth Director of Public Prosecutions (CDPP) to consider prosecution action.

Recovery: the department takes all reasonable measures for recovery of fraud losses. This includes formal proceeds of crime action, civil recovery processes and administrative recovery.

Post-incident reviews: reviews of investigations, or incidents related to fraud or corruption, are undertaken with the relevant departmental programs. Reviews include any identified control weaknesses or program design deficiencies that require treatment, and recommendations for remedial and/or alternative administrative actions if fraud or corruption cannot be proven or is deemed not in the public interest to prosecute.

Non-compliance: when opportunistic non-compliance is identified it is referred to the relevant business area for action. These referrals will include key findings and recommendations concerning any relevant risk controls or treatments.

National Anti-Corruption Commission (NACC): The NACC will begin operations on 01 July 2023. The NACC is an independent agency that will prevent, detect, investigate and report on serious or systemic corruption in the Commonwealth public sector. It will also educate the public service, and the public, about corruption risks and prevention. The department's fraud and corruption control activities, policies and procedures will be updated to reflect the NACC's legislative obligations and associated integrity activities.

Reporting, assurance and monitoring

Regular reporting and monitoring provides assurance over the effectiveness of the department's control arrangements in preventing, detecting and responding to fraud and corruption. The department collects information on all allegations of fraud or corruption against the department, current and completed investigations, whether the fraud was proven or not, and whether the matter was dealt with by a criminal, civil or administrative remedy.

The department's reporting, assurance, and monitoring controls include:

Fraud certification and annual report: the department informs the ARC of the activities throughout the financial year that have or are to be undertaken to respond to fraud planning, prevention, detection, and response within the department in accordance with the Fraud Rule.

This assists the ARC to provide advice to the Secretary to support the certification of fraud control arrangements for the annual report. This is a requirement of section 17AG of the PGPA Rule 2014, which requires accountable authorities to certify in their Annual Report that these requirements have been met.

Quarterly reporting to senior governance committees: reporting on key fraud control initiatives, progress of investigations, investigations outcomes, and current and emerging strategic fraud and corruption control risks are reported quarterly to the EC and ARC. Reporting on security and workforce integrity risks, including those for fraud control, professional conduct, and anti-corruption are reported quarterly to the SWIAC.

Annual reporting to the Australian Institute of Criminology (AIC): the Commonwealth Fraud Control Policy requires the collection of data on fraud within the department and to report this information annually to the AIC.

Annual reporting to the Commonwealth Ombudsman: the department is required to submit an annual workbook and survey to the Commonwealth Ombudsman on Public Interest Disclosures.

Assurance framework: to provide confidence to Government that the department’s outcomes are being achieved, all business areas must identify areas of assurance need, conduct assurance activities, implement any recommendations identified, and communicate this with the department’s Executive. The Assurance Framework provides guidance on how to do this.

Live assurance: mapping activities are used to identify higher risk priority areas and provide ‘real-time’ risk and controls advisory services to directly support program areas and the department. Key risks are mapped, including fraud and corruption risks and the highest priority measures are identified to undertake a 'risk snapshot’. Areas requiring immediate ‘real time’ and ongoing risk, fraud, corruption, and assurance advice are identified for targeted deep dives. Key risks, key control gaps and opportunities are highlighted to strengthen mitigation strategies and/or assist the department to capture the decision-making and approval processes where controls may have been removed.

Other reviews: quality assurance reviews of departmental investigations in accordance with the AGIS or the department’s compliance with the Fraud Rule may be the subject of audit by the Australian National Audit Office.

Further information

Queries about the Department of Health and Aged Care Fraud and Corruption Control Plan can be forwarded to fraudprevention@health.gov.au.

Key legislation and instruments

APS Values and Code of Conduct

Australian Government Investigations Standards

Commonwealth Fraud Control Framework 2017

Criminal Code Act 1995

Public Governance, Performance and Accountability Act 2013

Public Interest Disclosure Act 2013

Public Service Act 1999

Departmental policies and links

Accountability Authority Instructions

Assurance Framework

Conflict of Interest Policy

Fraud Control Toolkit

Gifts and benefits

Grants Toolkit

Health Integrity and Security Framework

ICT Acceptable Use Policy

Notification of Significant Events – in Procurement (Department of Finance)

Personnel Security Policy

Public Interest Disclosure Framework

Probity Principles – in Procurement

Procurement Advice

health.gov.au

All information in this publication is correct as of 19 April 2023