Australian Government
Aged Care Quality and Safety Commission

GOVERNING FOR reform IN AGED CARE

Information management

The flipbook guides have been designed as supplementary supports for the learning modules. The guides include key messages and insights for your continued reflection.

Disclaimer: The new Aged Care Act 2024 (the Act) starts on 1 November 2025. The Act replaces existing aged care legislation. The Aged Care Rules (the Rules) are expected to be finalised before the Act starts. The Rules give more information about how the new Act will work. This resource is in draft. We will update it when both the Act and the Rules come into force.

Need to know: Information management

In the aged care sector, information has a myriad of important uses. It can provide key insights to determine strategic decision making, inform risk management approaches, and best practice delivery of safe and high-quality care, and ensure providers are meeting their obligations and accountabilities.

It is the role of governing bodies and executives to be acutely aware of, how, why and what information is collected, stored and utilised.

A provider's governance systems are critical to the delivery of safe, quality, effective and person-centred care for every older person, and continuous care and service improvements.

Effective information management can ensure providers:

- ensure critical information is effectively communicated in a timely way
- meet their compliance obligations in relation to the management of information
- make the most informed decisions about individual people
- ensure oversight by the governing body and executive is effective and efficient
- use the information gathered to inform the design and continuous improvement of the provider's care and services
- track progress against strategy and strategic objectives
- manage strategic and operational risks and controls.

Poor information management can result in:

- decision-making that compromises the older people's safety and quality of care due to out-of-date, inaccurate or incomplete data inputs
- loss or theft of sensitive information about older people or providers
- breach of confidentiality requirements, privacy rights and other regulations.

To achieve best practice, information management providers must ensure they have effective systems and structures in place in all aspects of information management to ensure that information used is accurate and reliable, complete, consistent and accessible in a timely manner.

Information management obligations & accountabilities

Read about the obligations listed below on the following pages to learn more about each.

The collection and management of information in an aged care setting is linked to several legislative and other regulatory requirements.

A list of relevant acts has been provided. It is advised that governing bodies and executives take the time to review their obligations and accountabilities thoroughly.

01 *Aged Care Act 2024*

02 *Aged Care Rules 2025*

03 Statement of Rights

04 *Privacy Act 1988*

05 Strengthened Aged Care Quality Standards

Information management obligations & accountabilities

01 *Aged Care Act 2024*:

- provider obligations for record retention enabling transparent and effective delivery of care and services
- the type of information that must be collected, the allowable use of that information and the retention period for certain information and records
- that records must be kept in accordance with the Aged Care Rules 2025
- definitions of protected information and the penalties resulting from misuse of information.

02 *Aged Care Rules 2025*

- maintain records that document the delivery of care and services, staff qualifications and training, incident reports and financial statements
- implement robust data protection measures to safeguard personal and sensitive information
- develop and sustain information sharing protocols
- compliance related reporting of specific information including incidents, changes in responsible persons, audits, financial reporting
- record retention and disposal timeframes

03 **Statement of Rights:**

Providers must give older people information about their rights in relation to the aged care service(s) they are accessing, give them a copy of the Statement of Rights, and help older people understand their rights under the Statement.

Providers must also retain records relating to the older person having been given the Statement of Rights.

04 *Privacy Act 1988*:

Broadly speaking, there are 13 Australian Privacy Principles within the Act, which all providers must meet.

To learn more about these principles please take the time to review the *Privacy Act 1988.*

Information management obligations & accountabilities

05 **Strengthened Aged Care Quality Standards:**

Having complete and accurate records is crucial to demonstrating the organisation is compliant with all the strengthened Aged Care Quality Standards and ensuring an older person receives safe and high-quality personal and clinical care, for example:

Standard 2 - The organisation
Outcome 2.7 Information management: The provider must ensure that information recorded about an individual is accurate and current, is able to be accessed and understood by the individual, supporters of the individual, aged care workers and health professionals involved in the individual's care. The provider must ensure that the information of individuals is kept confidential and managed appropriately, in line with their informed consent. The provider must implement an information management system and ensure that the system is maintained and is regularly reviewed for effectiveness.

Standard 3 - Care and services
Outcome 3.3 Communicating for safety and quality: The provider must ensure that critical information relevant to the of delivery care services to individuals is communicated effectively to the individuals and those who support them or deliver their care. The provider must implement a system for communicating structured information about individuals and their care to ensure that critical information is effectively communicated in a timely way to aged care workers, supporters of the individual, other persons supporting the individuals and health professionals involved in the individual's care.

Outcome 3.4 Coordination of care and services: The provider must ensure that individuals receive quality care services that are planned and coordinated, including where multiple health providers and registered providers are involved. The information required to manage this care needs to be effectively documented, shared and communicated with individuals, their supporters, and care and service providers to maintain continuity of care and ensure an appropriate transition of care.

The role of the governing body in information management

As a provider's information management practices can affect an entire organisation, it is essential that governing body members understand their role in supporting best practice information management.

After reviewing the information management online module, please take a moment to reflect on the questions on the following page about:

Information management systems and processes

Training and guidance

Fostering the right culture

Maintain oversight and reporting responsibilities

Auditing of information management and record keeping systems:

The role of the governing body in information management

Information management systems and processes:

What initial steps can our governing body take to ensure our providers information management systems and processes are sufficient to support decision making, compliance and person-centred care?

Training and guidance:

What could our governing body do to ensure that the training staff receives on information management is aligned to our strategic priorities and compliance?

Fostering the right culture:

How can we as a governing body shape a culture that prioritises record keeping and information management compliance?

Maintain oversight and reporting responsibilities:

What steps could our governing body or management take to improve our current oversight of incidents and risks, supporting ongoing reporting requirements?

Auditing of information management and record keeping systems:

What steps can we take to ensure our governing body regularly audits our information management processes and what can we implement to ensure this information is presented effectively at a governing body level to support our strategic decision making?

Best practice information management

Whilst the different nature and size of a provider may affect how information is managed, the core components of best practice information management are the same. Governing bodies and executives need to be aware of these components and regularly assess their organisation's capability to deliver each component.

Best practice information management (continued)

Information policy:

- Regularly assesses information management policy effectiveness and alignment to organisational requirements and are informed by contemporary, evidence–based practices.
- Information management policy clearly articulates:
  - roles and responsibilities for record keeping and information management
  - procedures for record keeping, including which items are to be recorded and when/how
  - procedures for disposal and/or destruction of records (such as security bins, disposal schedules, etc.)
  - compliance requirements for relevant legislation and standards
  - expected actions where an information or data breach occurs, including any external reporting obligations
  - consequences of policy non-compliance
  - how older people can access information about themselves held by the provider
  - details on protection of client information.

Best practice information management (continued)

Protecting information:

Governing bodies and executives, management and workforce are aware of the following fundamentals of information protection as well as their individual roles and responsibilities:

- Confidentiality - information is managed in an information management system and is only able to be accessed by authorised persons for approved purposes
- Integrity - there is assurance that information has been created, amended or deleted in line with authorised means and is correct and valid (as outlined in the information policy)
- Availability - authorised persons can access information reliably and when required. This includes older people being aware of how they can access or correct their own information or withdraw their consent to share information.

Best practice information management (continued)

Information management system:

It is essential that providers have an effective information management system that enforces restrictions on the access, retention and disposal of records as per the provider's information management policy.

- Access - a provider's Information Management System (IMS) should restrict access to personal or sensitive information to an 'as needs' basis. In addition, when information is shared with older people, it should be provided in ways to meet the needs of those who may have cognitive, sensory, literary or language barriers.
- Feedback - seek feedback from workers and other users of the IMS, to understand if there are challenges or barriers in accessing or operating the system and address these issues.
- Retention - the IMS should:
  - support the archiving of critical information
  - have clear labelling and naming conventions in place to improve accessibility
  - periodically be backed-up to support file retention compliance
  - support requirements as outlined in a provider's information management policy.
- Disposal - information should be stored and disposed of in alignment with any legislative compliance obligations.

Best practice information management (continued)

Confidentiality and data protection:

- Governing bodies and executives should be assured that:
  - access to sensitive or personal information is restricted to the appropriate staff and older people
  - use of multi-factor identification for data access is in place
  - there is a disaster recovery plan in place for any loss or destruction of records, which has been tested
  - software approaching end of life has a replacement found
  - anti-virus and firewall software is in place
  - there are strong password requirements with regular password changes
  - information is backed up every 4 months
  - regular penetration testing is occurring to identify any data breach vulnerabilities.

Additional resources

- Aged Care Act 2024
- Aged Care Rules 2025
- Statement of Rights
- Strengthened Aged Care Quality Standards
- Privacy Act 1988
- Cybersecurity Governance Resources
- Australian Privacy Principles: quick reference
- Australian Cybersecurity Centre
- Notifiable data breaches
- Data Governance Foundations for Boards
- Cyber Security Governance Principles
- **Governing Through a Cyber Crisis:** Cyber Incident Response and Recovery for Australian Directors
- Aged care provider reporting

Australian Government
Aged Care Quality and Safety Commission

GOVERNING FOR reform IN AGED CARE

Contact us:

www.agedcarequality.gov.au

1800 951 822

info@agedcarequality.gov.au