Australian Government
Aged Care Quality and Safety Commission

GOVERNING FOR reform IN AGED CARE

Information management

THE ASK:

Information management systems and processes are critical to the delivery of safe, high-quality consumer-centred care. They ensure that consumers and those involved in consumer care have access to consistent, reliable and up-to-date information. Information and data are some of the most valuable assets an organisation can hold. To have effective oversight over a provider, it is important that governing body members understand the aspects of an effective information management system.

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.

Covered in this topic guide

- What is information management, and why is it important?
- The regulatory environment – aged care requirements and privacy requirements.
- Key features of effective information management systems.
- Role of the governing body in information management.
- The importance of continuous improvement.

Where are we now?

There is a lot of data and lots and lots of information. [We need to] invest in management systems and governance processes. While things can look glossy and glamorous in the front, there needs to be the background processes behind the scenes to back it up.

GOVERNING BODY MEMBER

Key concepts

- **Information**, in the broadest sense, refers to the knowledge, facts and data that a provider interacts with. This information may be stored electronically, or in hard copy, depending on the processes you have in place.
- **Personal information** under the *Privacy Act 1988* refers to information or an opinion about an identified individual or an individual who is reasonably identifiable. Generally, the information contained in a consumer record is personal information and will attract protections and obligations under privacy legislation.
- **Protected information** under the *Aged Care Act 2024* includes (amongst other elements) personal information that is acquired for the purpose of providing care to a consumer or information that relates to the affairs of an approved provider. Protected information should only be accessed or used for permitted reasons.
- **Information management** broadly refers to the systems and processes in place for the collection, storage, distribution, and retention of information within an organisation.
- **Integrity of information** refers to the assurance that information has been created, amended, or deleted only by the intended person and that the information is correct and valid.
- **Confidentiality of information** refers to limiting access to information to authorised persons for approved purposes only.
- **Emerging technologies** may impact information management through the introduction of new tools for improved accuracy of data collection, timeliness of data access, third-party sharing, and data security.

Information management in aged care

Effective information management is particularly important for the aged care sector as it underpins the sector's ability to deliver safe and high-quality consumer-centred care. Information management systems and processes ensure appropriate members of the workforce have access to information that helps them in their roles, from a consumer's medical records to their financial records. It also makes sure consumers can access information about their care and services.

Having complete and accurate records is crucial to demonstrating the organisation is compliant with the strengthened Aged Care Quality Standards.

Governing bodies are responsible for the oversight of the information management systems and processes by ensuring the relevant controls and reporting processes are in place. Governing bodies in aged care must be particularly mindful of the impacts that the information management system may have on the quality and safety of care that is delivered to consumers. Information management can be one of the key tools that inform and support the ability to deliver change and innovation across the aged care sector.

Tips for information management

Older Australians at the centre

- Information that supports older people in making decisions should be relevant and accurate and provided in a timely manner. Information should be presented to older people in a clear, understandable form, which includes the use of translation and/or interpreter services.
- Providers should ensure that an older person understands their right to access, or correct their information, or withdraw their consent to share information. Such consent should be communicated with access to language services if required.
- The information of older people is confidential and managed appropriately, in line with their informed consent.

Obligations and accountabilities

- Maintain records about the Quality Care Advisory & the Consumer Advisory bodies, and the qualifications, skills and experience of staff members.
- Critical information relevant to the older person's care and services is communicated effectively with the older person, between workers and the family, carers, and health professionals involved in the older person's care.
- Clinical risks, changes and deterioration in an older person's health condition is communicated as appropriate.
- Understand the requirements under the *Aged Care Act 2024* and its subordinate legislation in relation to the requirements for providers to demonstrate effective information management systems.
- Understand obligations regarding the collection, use and disclosure of personal information under the *Privacy Act 1988* and ensure your information management systems comply with those obligations.

Knowledge, skills and experience

- Understand the features that make up effective information management systems and the importance of accurate record keeping.
- Ensure that information management processes and security risks are clearly articulated in policies and procedures and understood by all workers and contractors.

Leadership and culture

- Stay abreast of regulatory reforms and emerging technologies, which may result in changes needing to be made to information management or record keeping systems

and processes. Seek out opportunities for continuous improvement of information systems and processes.

- Foster a culture that encourages compliance with information standards and obligations, including reporting or escalation of any information security risks.

Reflecting on your practice

Think

Below are the top things you need to be thinking about:

- Is our information management system helping us to make better, more informed decisions?
- How is information being analysed and used to help support consumers make decisions about their own care and to improve consumer outcomes?
- What measures do we have in place to be confident about our information integrity and confidentiality?
- Are we providing information that consumers want in a format that is easy to use and understand?
- Are we leading by example when it comes to a culture of encouraging effective information management, reporting and data security?

Ask and say...

Below are the top questions you need to be asking:

- Does the provider have mechanisms to assess the degree of potential harm to the consumer or organisation if information is inadvertently shared, lost or compromised?
- How does the organisation report and monitor information security incidents, and are these reports regularly reviewed by the governing body?
- Is there an ongoing awareness and training program established around information management and obligations for all staff to protect sensitive and personal information?
- Do we know what and where our most critical systems are, and is the level of monitoring adequate?
- Do we regularly review and improve the effectiveness of our information management system

Do...

These are the top **actions and behaviours** of leaders:

- Establish quality management practices to regularly review and check consumer satisfaction, accuracy, currency and security of information.
- Establish, define and document roles of the governing body in overseeing information management and cyber incidents and responses.
- Ensure key issues and concerns around information security are communicated during governing body meetings and directions and in communication from management.
- Establish processes for keeping abreast of regulatory reforms and emerging trends around information management.

What is information management?

Information management broadly refers to the systems and processes in place for the collection, analysis, storage, distribution, and retention of information within an organisation. How information is communicated and managed can vary, but the agreed processes need to be efficient and fit the situation. Acknowledging that providers have differing natures, sizes and complexity, the core components of better practice information management include:

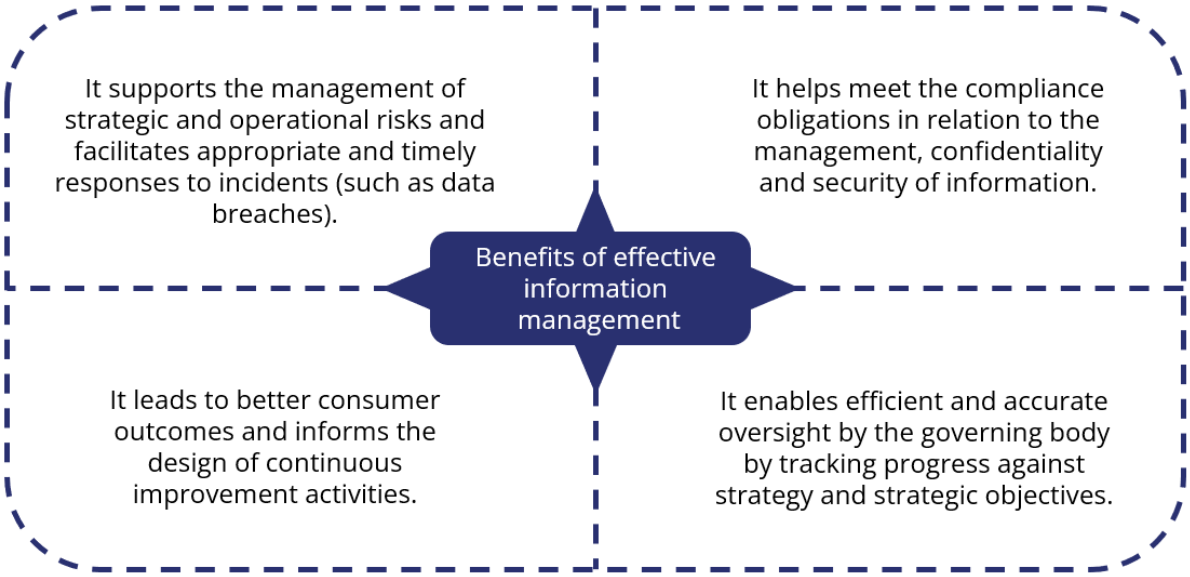
- understanding what types of information need to be collected
- reviewing and checking with consumers, workforce, and stakeholders that the information they require is available and easy to access
- understanding the regulatory environment that applies to how information needs to be managed
- implementing an effective information management system, including an information management policy
- fostering a culture that is inclusive and encourages record keeping and compliance with information management
- reviewing and auditing the information management system as part of ongoing compliance to ensure incidents and risks are appropriately managed and to identify opportunities for continuous improvement.

Why is information management important?

At its core, effective information management can lead to better, more informed decision making by consumers, care staff, the management team and the governing body. Accurate information that is communicated and accessible by the relevant people can lead to better consumer outcomes as well as increased consumer and community confidence and trust in the operation of the provider.

Accurate record keeping and information management play a key role in incident, risk and complaints management processes. Consumer records are used to demonstrate the care and services that were provided to consumers and can often be used as evidence in complaints or legal proceedings.

Some other benefits of effective information management include the following:



Collecting information

Information is collected and shared for a wide range of purposes within an aged care provider, including for the delivery of high-quality, safe care and for administrative purposes. This also includes information required to meet legislative requirements and mandatory reporting obligations (e.g. data required for the Serious Incident Response Scheme, the National Quality Indicator Program, financial reporting). Information can be collected from a variety of sources depending on the nature of the information, such as directly from consumers about their personal care preferences, by staff to document processes, or from healthcare professionals or third-party service providers. It is relevant for governing bodies to understand the types of information being collected, as different compliance requirements are likely to apply to different categories of information.

Providers should have adequate safeguards in place to ensure consumers have given informed consent for the collection and use of their information. Consent under the *Privacy Act 1988* must be given voluntarily and be specific, current and informed. The consumer must also have the capacity to understand and communicate that consent. Consumer consent and consumer records should be tailored to the specific language needs required to ensure that communications to consumers are in a language and form that they understand. Even where a consumer has agreed to have an advocate or representative, it is important that consumer consent is obtained and that the individual is able to exercise the authority to make decisions about their care and preferences (if they chose to and are able to do so).

Types of information

Providers collect large amounts of information that need to be effectively managed. This includes information about consumers, staff, and procedural or operational information. Governing bodies that review and draw insights from the information available are in a better position to oversee the information management systems. In doing so, they can ensure that they are effective in facilitating the delivery of care and services that are consumer-friendly and compliant with regulatory obligations.

- Consumer records, including personal information and general health information (which is considered sensitive information and afforded a higher level of protection).
- Information required for the delivery of care and services to the consumer, including assessments, care plans, prudential records, records relating to leave arrangements and representative contact details.

- Records of the qualifications, skills and experience of staff members.
- Employment records, including agreements, leave balances and worker qualifications.
- Worker screening clearances, including police certificate or NDIS worker screening.
- Volunteer records.
- Influenza and COVID-19 vaccination status records.

- Records required by the National Aged Care Mandatory Quality Indicator Program manual.
- Records of unspent home care amounts.
- Records about the governing body.
- Records about consumer, staff and volunteer vaccinations.
- Information regarding suppliers of services and equipment or other procurement activities.
- Financial records to produce financial reports.
- Reportable incidents and risk management.
- Records to demonstrate that a copy of the Statement of Rights has been provided and communicated to the consumer.

The regulatory environment

The nature and sensitivity of the information that is collected will attract different compliance obligations and regulatory protections. The governing body is responsible for the oversight of compliance with these regulatory requirements, where incidents of non-compliance can result in serious consequences not only for the consumer but also for the provider and for governing body members.

Navigating the regulatory environment can be complex. The nature of aged care services is that it overlaps and interplays with a range of other regulations. The two key regulatory categories that are important for governing bodies to consider when overseeing the information management system are:

- the *Aged Care Act 2024* in relation to what information aged care providers must collect
- the *Privacy Act 1988* in relation to what limitations and obligations apply when using or disclosing personal information.

Aged Care Act

With an emphasis upon person-centred care, and the protection of older people's rights and privacy, the *Aged Care Act 2024* (the Act) establishes clear obligations for registered aged care providers regarding information management, access, and record-keeping. These obligations include the type of information that must be collected, the use of that information and the retention period for certain information and records. Some key information management obligations in the Act include:

- Section 154 - that providers maintain and retain prescribed records in accordance with the Aged Care Rules 2025 (the Rules) whilst ensuring compliance with Section 168, which outlines strict requirements for safeguarding personal information.
- Section 155 - requires providers to provide and explain relevant records and information to individuals accessing or seeking aged care services, adhering to any prescribed requirements prescribed by the Rules.
- Section 156 – that providers ensure that supporters and independent aged care advocates have access to necessary information to assist individuals in making informed decisions about their care.

Certain information that is collected, accessed and maintained by providers is considered 'protected information'. The Act sets out that relevant information is protected information if:

- it is personal information
- it is information (including commercially sensitive information) that if disclosed, could reasonably be expected to initiate an action by an entity (other than the Commonwealth) for breach of a duty of confidence.

Protected information must be secured, safe guarded and only accessed in certain situations. Protected information includes information that is acquired for the purpose of providing care to a consumer and is either personal information, information related to the affairs of the provider, or information that relates to an applicant for a government grant. It is important for governing body members to be mindful that disclosure of protected information for purposes other than for which it was collected is an offence and can attract civil and criminal penalties.

Statement of Rights

The new *Aged Care Act 2024* (the Act) puts the rights of older people first and includes a Statement of Rights that describes what rights older people have when accessing Australian Government funded aged care services.

The Statement of Rights includes the right for an individual to have their personal privacy respected and their personal information protected. They also have the right to seek, and be provided with, records and information about their rights and the funded aged care services the individual accesses.

Under the Aged Care Rules 2025 (the Rules), a registered provider must provide an individual with:

- a copy of the Statement of Rights
- information about their rights in relation to the aged care service(s) they are accessing
- assistance to understand their rights under the Statement of Rights.

The provider must also retain records relating to the individual having been given the Statement of Rights. There is a requirement to keep and retain this information, with the Rules specifying that a registered provider must keep this record for 7 years from the date the record was made (outlined in Part 7 – Information and access).

Effective information management systems will contemplate these compliance requirements and build processes and systems to ensure that the relevant information is collected, stored, accessible and protected appropriately.

Aged Care Quality Standards

Having complete and accurate records is crucial to demonstrating the organisation is compliant with the strengthened Aged Care Quality Standards (Quality Standards). This will ensure a consumer receives safe and quality personal and clinical care. Information management systems reinforce the provision of safe care to consumers and are necessary for continuous improvement. A provider must demonstrate that it has information management systems in place that support the following Quality Standards:

- ***Standard 1 - The individual***
  Outcome 1.3 Choice, independence and quality of life: The provider must provide individuals with timely, accurate, tailored and sufficient information about their aged care services, in a way they understand.
  Outcome 1.4 Transparency and agreements: The provider must support individuals to understand information provided to them and to make informed decisions, including any agreement they will be required to enter, the terms relating to their rights and responsibilities, the care services to be provided and the associated fees, and the time to consider this information and seek advice.
- ***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 delivery of care services to individuals is communicated effectively to the individuals, between aged care workers delivering the services, with supporters of the individuals and other persons supporting the individuals and with health professionals involved in the individual's 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, supporters of individuals and other persons supporting individuals are involved. This will include communication and the sharing of information that is well documented and effectively managed for an appropriate transition and continuity of care.
- ***Standard 5 - Clinical care***
  Outcome 5.1 Clinical governance: The provider must work towards implementing a digital clinical information system that integrates clinical information into nationally agreed digital health and aged care records. The system should also support interoperability using established national Healthcare Identifiers, terminology and digital health standards and have processes for aged care workers and others to access information in compliance with legislative requirements.

- ***Standard 7 - The residential community***
  Outcome 7.2 Transitions: The provider must have processes in place for transitioning older people to and from hospitals, other care services and stays in the community including monitoring, documenting and communicating information about an older person's medical condition and their needs and preferences where responsibility for care is shared. The provider must ensure that supporters of individuals, health professionals or organisations are given timely, current and complete information about the individual as required.

Privacy Act 1988

The *Privacy Act 1988* sets out the requirements and reasonable steps an organisation must take to protect personal information. There are 13 Australian Privacy Principles (APPs) within the *Privacy Act 1988*, which all providers must meet in addition to any other state or territory privacy laws that apply.

Broadly, the APPs include requirements relating to:

- managing personal information in a way that is open and transparent
- maintaining anonymity and pseudonymity
- collecting and managing solicited and unsolicited personal information
- notification of the collection of personal information
- using and disclosing personal information collected (including for direct marketing purposes)
- ensuring quality of personal information (accurate, up to date and complete)
- using government identifiers
- maintaining the security of personal information (protection from misuse, interference, loss, unauthorised access, modification or disclosure)
- providing access to information and taking reasonable steps to correct any personal information it holds.

Many of the obligations relating to privacy require an organisation-wide approach. Compliant privacy practices should be reflected in the provider's policies and procedures and embedded into the information management systems of the provider.

Notifiable Data Breach Scheme

An important requirement of the *Privacy Act 1988* relates to data breach notifications. Specifically, when a data breach has occurred, a provider must notify the Office of the Australian Information Commissioner and any affected individuals if the data breach is likely to result in serious harm to the individual(s) and remedial action has not been able to prevent this likely risk of serious harm. Notifiable data breaches can not only result in damage to the individuals affected, such as staff or consumers, but can also cause significant reputational harm to providers and governing bodies.

Key features of effective information management systems

Effective information management systems set out clear processes to safeguard the protection and integrity of information across the entire information life cycle. This includes the following:

- **Protection & security** - protecting information requires an understanding of its value and an assessment of the risks. The security of information is one of the key pillars of an effective information management system, as the system should have safeguards in place to prevent misuse, unauthorised access, loss, or interference with information. This is becoming increasingly important with the increase in electronic data and the emergence of cyber-attacks and data theft.
- **Confidentiality** - confidentiality of information refers to limiting access to information to authorised persons for approved purposes only.
- **Integrity & accuracy** - integrity of information refers to the assurance that information has been created, amended, or deleted only by the intended authorised means and is correct and valid. To ensure the integrity and accuracy of information, the ability to edit records should also be restricted, with an audit trail in place.
- **Availability** - availability of information refers to allowing permitted persons to access information for authorised purposes at the time they need to do so. To remain compliant with relevant legislation, access to any personal or sensitive information about a consumer or staff member should be restricted and granted on an 'as need' basis.
- **Retention & disposal** - the information management system should support archives for long-term file storage and a file movement register to track any movement of records. The information management system should be periodically backed up to support file retention compliance. To ensure compliance obligations are met, the information management system should archive files and prevent any premature deletion and ensure information is disposed of once it is no longer needed (or required to be retained).
- **Fit for purpose & consumer-friendly** - the governing body should receive current data and analysis from the information management system that allows them to review its effectiveness in meeting consumer and compliance requirements and addressing risks in the organisation. This includes ensuring that information is accessible, inclusive, and easy to understand for consumers.

Information management policy

An information management policy can work together with other policies, or with information that may be contained in other policy documents (such as a privacy policy). Whichever way information is communicated, it is important that all staff are aware of their responsibilities and expectations regarding the provider's approach to information management.

Part of effective information management is to have a clear information management policy that outlines:

- roles and responsibilities for record keeping and information management, including responsibilities and processes to address complaints regarding information incidents
- the process for consumers to access their personal information
- procedures for record keeping, including which items are to be recorded and when/how
- procedures and compliance requirements for the retrieval and/or destruction of records
- expected actions where an information or data breach occurs, including any external reporting obligations
- consequences of policy non-compliance.

Role of the governing body

The governing body must ensure that there are systems to support organisation-wide governance within the provider's organisation (for example, the processes for the governing body's authority and decision making to be distributed throughout the organisation). Governing body members need to be able to 'connect the dots' to form bigger and clearer pictures, which provides an evidence base to inform ongoing sector reform activities and initiatives. It is important for governing bodies to be comfortable that the information used for data driven decision making is accurate and has integrity.

Fostering the right culture

A key role of the governing body is to foster a culture that prioritises accurate and up-to-date record keeping of all care and services provided to consumers. This includes ensuring that information and other communications are presented using inclusive, gender-neutral and accessible language and font. Ultimately, it is important the information management systems support improved consumer outcomes and seek to meet consumer expectations by facilitating accurate and timely access to resources, consumer records and care information. Governing bodies can encourage staff compliance with information management policies and procedures in the following ways:

- Ensure that governing body members and all staff receive sufficient training on the policies and procedures relating to information management and compliance. Regular training that sets out the key compliance obligations, as well as how to identify information management incidents and potential data breaches, can assist with increasing compliance.
- Embed compliance as a part of the organisational culture. This requires providing adequate support to staff to meet their information management obligations, which can include providing appropriate systems and tools, informing all staff that information management and good record keeping is a priority through regular communications, leading by example, encouraging an open and continuous improvement culture and ensuring breaches of the information management policy are thoroughly investigated.

The importance of continuous improvement

Monitoring and audit

Having good information management policies and systems in place alongside regular training is not enough to guarantee compliance.

The governing body should ensure regular audits of information management and record keeping systems and practices are undertaken, as well as an incident reporting process for any policy breaches or identified process gaps. This allows for the timely identification and analysis of gaps and issues and appropriate corrective action.

Audits of information management, and record keeping systems and practices may include:

- review of the organisation's compliance with the information management policy and regulatory requirements
- periodic review of records to identify any data quality issues, unauthorised changes or file damage
- monitoring and review of emerging cyber security threats, with timely staff communication and training on these.

Continuous improvement and looking ahead

As part of regular monitoring and review of the information management systems, effective governing bodies will seek to identify gaps and opportunities for improvement to efficiencies, accuracy or security of the information that the provider holds. This process of identifying gaps and improvements in developing improved information resources and systems should, where possible, include direct engagement and consultation with consumers. A continuous improvement approach that seeks to build and improve on existing systems ensures that providers are positioned to make informed decisions about their consumers as well as to be well prepared for change.

The aged care sector is one that is constantly subject to change, including environmental changes, regulatory changes, and emerging technologies. The importance of connectivity and digital health literacy (such as the integration of clinical information management systems with the My Health Record system) has emerged as enablers of improved accuracy and access to information. As a steward for the sustainability and progress of the provider's organisation, it is the responsibility of governing body members to stay abreast of regulatory reforms and emerging technologies, which may result in changes needing to be made to information management, or record keeping systems and processes.

Emerging technologies may also impact information management through the introduction of new tools for improved accuracy of data collection, timeliness of data access, third-party sharing and data security. Being aware of emerging trends, national digital health and aged care strategies and upcoming reforms will assist governing bodies to prepare for change and identify opportunities for growth and improvement of information management systems and processes. This includes providers working towards implementing a digital clinical information system.

Useful references and links

Aged Care Act 2024 | Australian Government Federal Register of Legislation

Strengthened Aged Care Quality Standards |Aged Care Quality and Safety Commission

Statement of Rights |Aged Care Quality and Safety Commission

Privacy Act 1988| Australian Government Federal Register of Legislation

Australian Privacy Principles quick reference | Office of the Australian Information

Notifiable data breaches | Office of the Australian Information Commission

Records Management AS ISO 15489 | The Standard for Information Documentation