Technology & Cyber Security

THE ASK:

The effective use of technology in aged care can lead to better consumer outcomes and helps to support the delivery of safe and high quality care. Governing bodies and executives that consider technology to be an enabler of growth and that implement processes to support the safe use of emerging technology can help position the provider to respond and adapt to change.

Covered in this Topic Guide

- Technology as an enabler
- Data and elements of cyber security
- Role of the governing body

Where are we now?

> *In order for our [organisation] to grow, the big thing that was needed was information, communications and technology capability to make it happen and to use technology as a tool to improve systems and governance.*
>
> GOVERNING BODY MEMBER

Key concepts

The following high-level definitions are provided to assist in interpreting some of the key concepts discussed in this Topic Guide:

- A **cyber incident** occurs when computer information systems, infrastructures, computer networks or individual computers are compromised by unauthorised access. A cyber incident can include data breaches and cyber attacks such as malicious software, ransomware, phishing messages or hacking.
- **Cyber security** refers to the protection of systems, networks and programs from digital interference, theft or damage.
- **Digital literacy** refers to the ability to understand, communicate and use information on digital platforms.

Tips for effectively embracing technology and ensuring cyber security

Older Australians at the Centre

- View technology as an enabler to better deliver care and services to consumers.
- Support change and transition to new ways of working that improve efficiency and consumer outcomes.

Obligations and Accountabilities

- Ensure the governing body is receiving the right reports and information needed to effectively manage cyber security risks.

Knowledge, Skills and Experience

- Encourage a culture that values digital literacy and supports the workforce by providing training and learning opportunities to better prepare them for changes in technology.

Leadership and Culture

- Foster a culture that encourages awareness and compliance with cyber security obligations, including detecting and reporting any cyber incidents.

Reflecting on your practice

Think...

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

- Do the governing body and executives view technology as an enabler to better consumer outcomes or as an outcome itself?
- Are we comfortable that we are adequately prepared to be able to adapt to change in the way that we do things?
- Can any of our systems and processes be more efficient with the use of a digital solution?

Ask and say...

Below are the top **questions you need to be asking**:

- How do the governing body and executives support opportunities to trial new practices, products and emerging technologies?
- Where we have adopted a digital solution, how do we ensure that the data we have is secured and monitored appropriately?
- Have our staff been adequately trained on cyber security and cyber incident response activities? Does management have the necessary confidence to lead such activities?
- Does our crisis management framework or information management framework contemplate cyber security incidents and attacks?

Do...

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

- Establish processes for staying informed about emerging technologies that present opportunities to improve service delivery processes.
- Stay up to date on known cyber attacks and information security incidents and take steps to ensure that staff understand their obligations in detecting and reporting any suspicious activity.
- Establish, define and document roles of the governing body in overseeing technology development and cyber incidents and responses.
- Encourage staff at all levels of the provider (including the governing body and executives) to increase their digital literacy skills by facilitating training and learning opportunities.

Technology in aged care

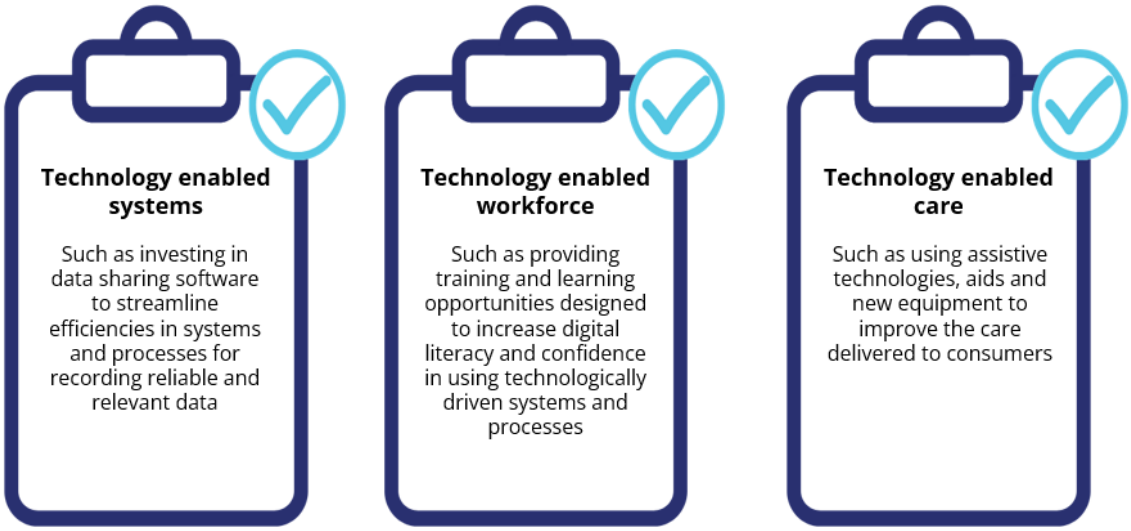
Technology in aged care can refer to digital care such as telehealth services, technology-enabled organisational systems, communications technology, as well as monitoring and surveillance technologies. Technology and innovation in aged care can play a key role in supporting the delivery of safe, high quality care and improving consumer outcomes. It is playing an increasingly larger role in supporting the organisational governance of aged care providers. Standard 8 of the Aged Care Quality Standards requires that the governing body is accountable for the delivery of safe and quality care and services. It is expected that the governing body implements systems to assess, monitor and drive continuous improvement across the provider, which includes processes for information management and incident and risk management.

Technology also plays a critical role in the ability of providers to collect, store and use data and information. From a consumer perspective, data allows individuals to find relevant information to support their access to care services and to ensure that consumer preferences are recorded and communicated. From a workforce perspective, data allows workers to access the right data in a timely manner to support quality care and make informed decisions. From a governing body perspective, data is a key element in understanding provider-level performance measures. Technology ultimately should be viewed as the enabler of providers continuing to meet their obligations under the Aged Care Quality Standards to deliver safe, high quality consumer-centred care.

Technology as an enabler for better care

The use of technology in the aged care sector has the potential to change the way providers deliver services and improve consumer outcomes. Governing bodies that view technology as an enabler of improvement and change are better positioned to be able to respond to change, identify opportunities for improvement and continue to deliver high quality care. An example of this was seen in the aged care sector's response to the COVID-19 pandemic. The scale and speed of the COVID-19 pandemic presented significant challenges in delivering safe, consumer-centred care to consumers. However, one of the outcomes of the COVID-19 outbreak was the acceleration of innovation and adoption of different technology by staff, consumers, care professionals and families. For example, the increased use of telehealth services, remote monitoring and technology-based communication options allowed consumers to stay connected with family, friends and representatives.

Ultimately, technology assists providers with the goal of providing safe, high quality care to consumers in a consistent and sustainable manner. Aged care providers can therefore use technology as an enabler in several ways, including improving systems and processes in the workforce and the consumer experience.



Technology as an enabler can:

- improve the effectiveness of administration and paperwork by providing smoother and more efficient automated processes
- provide more connected and personalised care and deeper consumer insights
- provide quicker access to data and allows providers to manage data on the go
- allow staff to provide more convenient and regular interactions with consumers and their families and friends
- improve the precision and accuracy of records
- improve compliance with regulatory requirements, such as mandatory reporting of serious incidents to the Commission using an effective incident management system
- provide opportunities to further enhance consumer well-being and personal choice.

Technology can facilitate the development of more efficient and effective processes. Ultimately, this enables care staff to dedicate more time to care activities and consumer engagement, which leads to better care outcomes.

Data and cyber security

While the use of technology does not necessarily refer to the digitisation of information or records, the increase in the use of data and digital information is commonly linked with the use of digital technological solutions. Technology as an enabler provides ways for this information to be stored contemporaneously, in a single source and, where appropriate, shared with the staff, consumers, regulators and other stakeholders to help inform decision making about the delivery of care and services.

Examples of where digital platforms have supported better consumer outcomes include:

- digital consumer records, including care and clinical records that can enable informed and up-to-date decision making by clinical care staff
- digital information management systems that record consumer preferences to facilitate communication and consumer-directed care
- electronic medication management systems to assist with reducing the number of medication management-related incidents
- digital consumer engagement and communication tools that allow up-to-date consumer information to be easily accessible by family and friends.

The decision to implement digital technology systems should be guided by a clear vision of how the technology will improve or enhance the delivery of care and services to consumers.

The importance of cyber security

As the technological maturity of a provider increases, so must its preparedness for cyber- and data-related incidents. Governing bodies should be mindful of the increased risks associated with the increased use of technology and must put in place reasonable steps to ensure the security of any data that is collected and stored.

Cyber security refers to the protection of systems, networks and programs from digital interference, theft or damage. With the increase in digital solutions and data driven decision making, there has also been an increase in the prevalence of cyber attacks and data breaches.

Cyber security measures are particularly important in aged care because:

- a cyber attack may impact the delivery of clinical care to consumers, which can have implications on a consumer's health and well-being
- aged care providers heavily rely on sensitive health information, which attracts obligations under the Privacy Act 1988, a breach of which can have significant impacts on the consumer, governing body and the provider more broadly.

Cyber risks are not simply an information and technology issue but can present provider-wide risks. While technical specialists in information technology and cyber security should be consulted and engaged, it is important the governing bodies do not solely rely on these

specialists. That is, the governing body should understand the risks involved and put measures in place to ensure the safety of any digital information that the provider holds and embed good cyber security, information management and data protection measures in the provider's systems and processes. Governing bodies who take a proactive approach to cyber security and who maintain ongoing awareness of their security obligations are more effective in anticipating and responding to data risks or incidents.

The interaction with other agencies

It is important to note that the increase in the use of data and digital records can bring with it additional security requirements and interactions with agencies such as the Australian Digital Health Agency (with respect to My Health Record) and the Office of the Australian Information Commission (with respect to personal information).

Elements of cyber security

Cyber security activities will vary from provider to provider depending on the size, complexity and nature of services provided. However, effective cyber security should include processes for prevention, detection, response and recovery of cyber security incidents.

Prevention

Prevention of cyber incidents requires systems and processes to be put in place that safeguards the collection, storage and use of data that is collected. This can include cyber security measures from passwords to investing in information and technology security infrastructure.

While investment in IT infrastructure and tools are essential for basic security and must be integrated into the technology architecture, they are not the markers of a holistic and robust cyber security strategy and policy. Good security starts with developing a holistic and robust cyber defence capability, which includes consideration of people, culture, processes, risk and technology, which all play a key role in the prevention of cyber incidents.

Detection

There is a common misconception that effective cyber security requires absolute prevention of all cyber incidents. Certain cyber incidents may be unavoidable, and despite reasonable steps being taken by the governing body, it may not always be possible to prevent these incidents from occurring. It is, therefore, important that the governing body has systems and processes in place to monitor and detect possible cyber incidents, such as data breaches or cyber attacks.

Response

Following detection, it is equally important that the provider has processes to respond appropriately to a cyber incident. It is important that consumers, staff and service providers (such as third-party software providers) are trained and aware of how to respond to a cyber incident to ensure that any harm to individuals is appropriately and quickly minimised and any reporting or compliance obligations are satisfied. This can be integrated into the provider's broader crisis management policy, data breach response plan or information management systems.

Recovery and review

The cyber incident must be contained and managed before returning to normal operations. Once the incident has been isolated and appropriately managed, it is important to review and evaluate:

- whether the relevant data has been recovered and data integrity restored
- whether the risk mitigation activities have been effective in managing the incident.

Role of the governing body and executives

Adopting new technology

The adoption of new technology and cyber security can often be viewed as the responsibility of specialist professionals. However, the governing body is responsible for ensuring that there are appropriate technology and systems in place to support organisation-wide governance within the provider. The governing body is also responsible for ensuring that technology and data are being used safely, efficiently and effectively to deliver services to consumers.

Governing bodies and executives play a key role as leaders and as the drivers of change within the aged care sector by adopting innovative practices, investing in information and technology infrastructure and supporting new practices, products and technologies that could lead to improvements in the way providers deliver care and services.

It is the governing body's responsibility to ensure that the activities of the provider align with the strategic objectives set by the governing body. It is important to ask, 'What are we trying to achieve as an organisation? What technology is going to help us achieve those goals, and what are the cyber threats to those objectives that we need to consider?'

The governing body and executives should have sufficient oversight over activities, such as technology procurement, asset protection, and response to cyber incidents, to ensure that these activities help ultimately meet the provider's strategic objectives.

Oversight of cyber security practices

With respect to the oversight of cyber security risks, governing bodies should seek to ensure that:

- their role in overseeing cyber security and cyber incident responses are clearly defined and documented
- they are aware of trends in cyber security risks and emerging issues in order to effectively and proactively manage those risks
- cyber security matters are routinely considered before implementing or adopting the use of new technology
- they seek out opportunities for continuous improvement of information systems and processes
- accountabilities and reporting lines for cyber security management are clearly defined and well understood
- there is regular provider-wide cyber risk training and communication
- they are addressing the strategic issues regarding the use of technology and cyber security, and staff at all levels are receiving clear, consistent and relevant messages from the executive and management team
- the key issues and concerns around cyber security are clearly communicated in governing body meetings and directions and in communication from management
- they are receiving the right reports and information needed to effectively manage cyber security risks
- the provider is transparent in informing stakeholders about cyber risk and security concerns.

Training and workforce capability

It is important that staff are provided training in any new technology, as well as regular training on cyber security and data processes.

Technology training

Establishing regular ongoing training can help to increase the digital literacy and technological capability of the workforce. The onset and uplift in video conference capabilities present an opportunity for governing bodies to consider increased investment in online learning opportunities for staff to access learning and development opportunities and, therefore, increase the digital maturity of the workforce.

Cyber Security training

It is also important that governing body members and all staff receive sufficient training on the policies and procedures relating to cyber security and compliance. The nature of cyber incidents will continue to evolve as the role of technology and digital data continues to increase in the delivery of care. As such, it is important that regular training that sets out the key compliance obligations, as well as how to identify and respond to cyber incidents, is undertaken.

Roles and responsibilities

Governing bodies should work with the senior executive team to ensure that roles, responsibilities, delegations and risk appetites (in relation to things like technology procurement, responses to a cyber attack and data-related risks) are aligned.

A key element of good governance is clearly setting out roles and responsibilities with respect to response to risks. It is common for organisations to assign senior responsibility for cyber risk to the Chief Information Officer (CIO) (or equivalent head of information management and technology) or the Chief Security Officer (CSO)/Chief Information Security Officer (CISO). In some smaller organisations, the Chief Financial Officer (CFO) or the Chief Executive Officer (CEO) or equivalent organisational head may be assigned this responsibility.

Clear-cut accountability is essential for effective cyber risk management, and whilst a senior officer is assigned responsibility for the day-to-day management, final accountability for cyber security remains with the governing body.

Technology and risk management

Improving technological maturity within an organisation requires a balance between investment, implementation, and current operations. The safe use of technology and digital solutions should be embedded in the provider's policies and procedures. It is one of the key responsibilities of the governing body to ensure risks in relation to the implementation of technology and cyber security are managed appropriately.

It is therefore important for governing bodies to have technology and cyber security on their meeting agenda and for this to be included in any risk assessments undertaken for the provider.

Encouraging a culture of digital literacy and change

A key role of the governing body is to foster a culture that encourages change and innovation. The use of technology and practices that support cyber security are more than a single policy document or compliance requirement. Rather, it is an approach to continuous improvement, information management and delivery care that seeks out opportunities to adapt and improve how services can be delivered in the aged care sector.

The implementation of technology can often require changes to existing processes or procedures. It is a key role of the governing body to consider what change management processes are in place in order to ensure that new technologies are implemented in a structured, systematic way that supports a culture of preparedness and willingness for change. Effective change management processes can play a critical role in ensuring that the implementation of new technology creates meaningful and sustainable improvements that do not disrupt the care being provided to consumers.

Embedding the use of technology as a part of the organisational culture facilitates a provider's digital maturity, which will assist a provider in preparing and adapting to changes in the aged care environment. This requires providing adequate support to staff, regular communications about risks to cyber security and, ultimately, encouraging a culture of continuous improvement and learning to improve the quality of services delivered to consumers.

Technology, innovation and continuous improvement

Undoubtedly digital technology will play an increasingly larger role in advancing innovation in aged care and improving the delivery of care and services. As consumer expectations start to include the use of technology and innovative solutions for how care is delivered, it is important that providers seek to use technology where appropriate to continuously improve. Governing bodies who are able to develop insightful strategic plans that see technology as an enabler to better service delivery are able to better take advantage of emerging opportunities and technologies. As a steward for the sustainability and progress of the provider, it is the responsibility of governing body members to look ahead and have an awareness of emerging technologies to continuously improve and innovate the way care and services are delivered to consumers. Emerging technologies may impact information management through the introduction of new tools for improved accuracy of data collection, ease of communication, timeliness of data access, third-party sharing and data security. Being aware of emerging trends will assist governing bodies in not only preparing for change but also in identifying opportunities for continuous improvement of information management systems and processes.

Useful references and links

Aged Care Act 1997

Quality of Care Principles 2014

Aged Care Quality and Safety Commission Rules 2018

Quality Standards | Aged Care Quality and Safety Commission

Australian Privacy Principles quick reference | Office of the Australian Information Commission

Notifiable data breaches | Office of the Australian Information Commission