Australian Government
Australian Digital Health Agency

CLOUD SERVICES

Considerations for healthcare organisations

A guide for
healthcare providers

This guide is for healthcare organisations to assist in assessing whether engaging a cloud service provider (CSP) is appropriate for identified business needs. It covers some of the benefits and implications of implementing cloud services but does not take the place of conducting other due diligence processes such as conducting risk assessments, obtaining legal advice and assessing the financial viability of the CSP.

The advice provided in this guide is general and is not intended to be a comprehensive guide for all the considerations involved in managing cloud services.

What are cloud services?

Instead of storing and managing your patient's healthcare information and business financial data on your own local server or personal computer, with cloud services you engage a cloud service provider and use a portion of their Information and Communications Technology (ICT) resources, software and services via the internet. Many organisations are reviewing this as an option for managing their ICT needs.

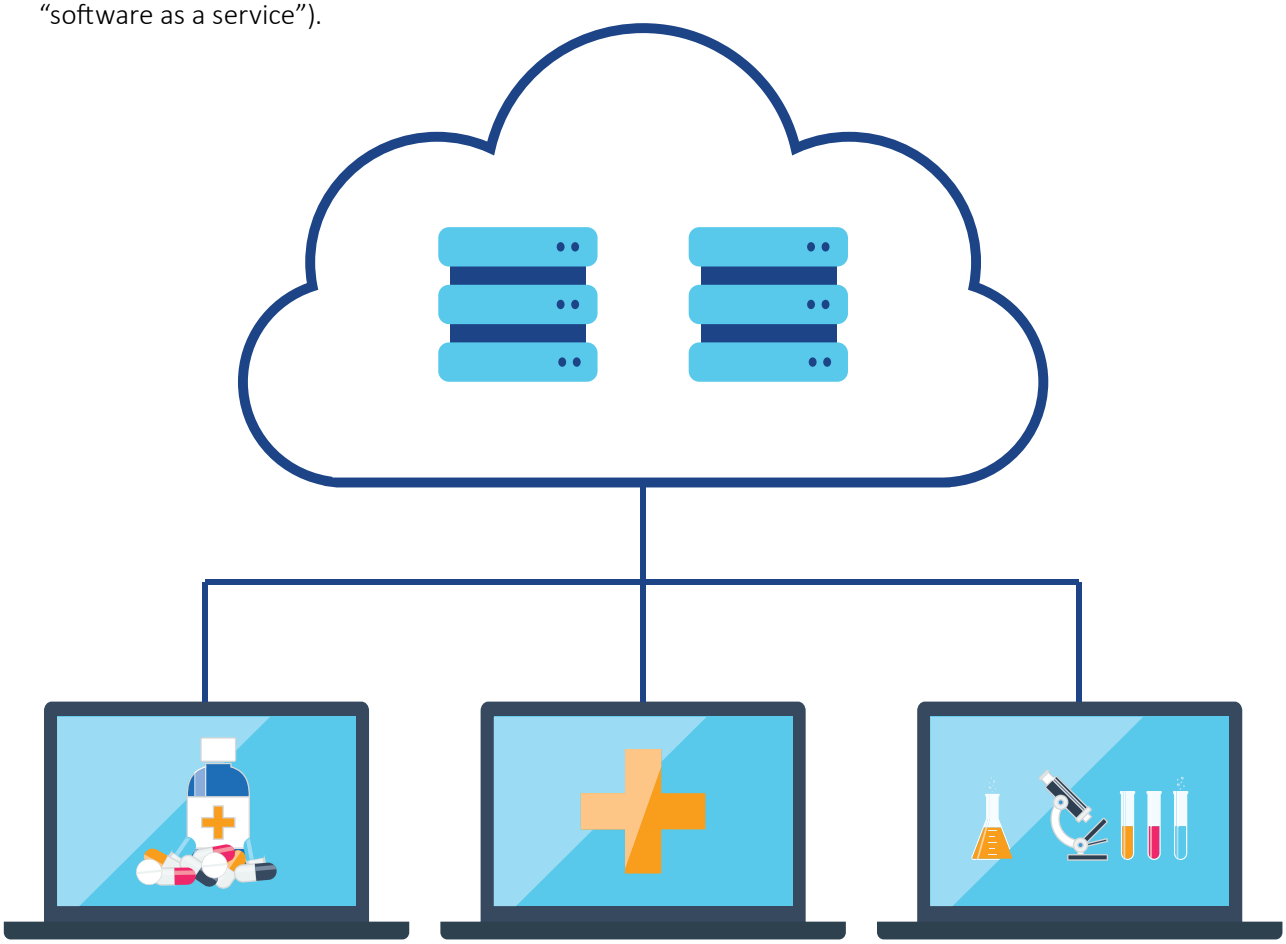
When considering cloud services, it is important to consider whether the cloud solution not only meets your business needs but also your security requirements and legal obligations.

"Like all ICT, using cloud computing is a question of taking advantage of the benefits while managing the potential risks."[1]

Cloud services for healthcare

Cloud services provide healthcare organisations the flexibility to outsource some or all ICT functions. Some healthcare organisations use cloud services with the aim of achieving operational efficiencies, accessing the latest technology with less capital cost, and the ability to quickly scale their business services to meet changing business demands.[2]

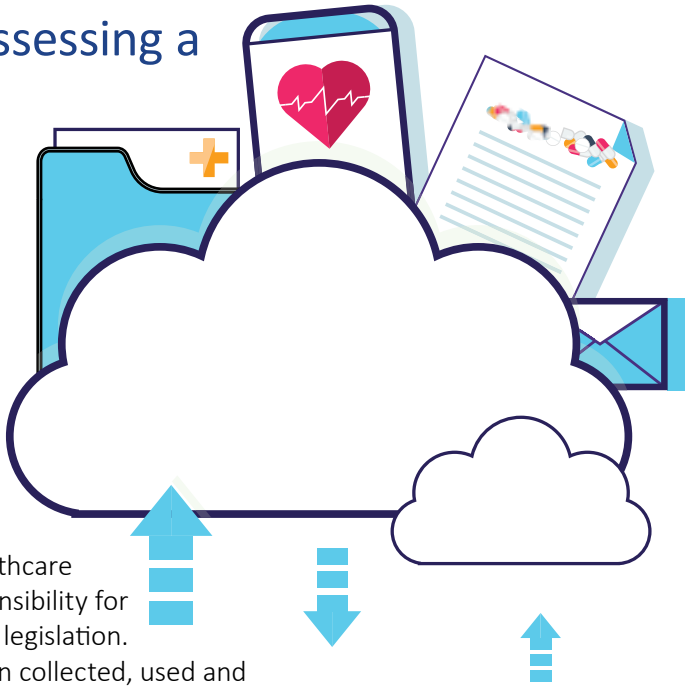
For example, cloud services are used by some healthcare organisations to access software provided by the Cloud Services Provider (CSP) to support their operations. A subscription arrangement is often used to provide healthcare organisations with access to medical practice software, financial software, or an online booking solution (this is generally referred to as "software as a service").



Alongside these projected benefits come potential issues and challenges. In addition to security and legislative requirements, an important consideration is to ensure visibility and seamless integration across an organisation's systems to support business availability and functionality.

Cloud solutions involve a **shared responsibility model** for ensuring appropriate security controls are in place. However, your organisation is ultimately accountable for making sure your information is managed securely in a manner that complies with all relevant legislation.

Factors to consider when assessing a Cloud Service Provider



Some of the main factors healthcare organisations should consider when researching and assessing a CSP include:

1. Shared responsibility model

Understand and clarify the responsibilities and accountabilities of your organisation and the CSP, then identify the services and security gaps which need to be addressed and managed.

Mitigating risks is a responsibility shared between parties, however, it is important for healthcare organisations to understand they retain the responsibility for protecting their data and complying with relevant legislation. This includes the security of the health information collected, used and stored and being accountable for any breaches of data.

Avoid the temptation to assume the CSP will automatically ensure their service meets all security and legal requirements. Make sure you frame any decisions within legal and security requirements and ensure they are supported with adequate contractual measures.

The following case study outlines the importance of understanding each party's responsibilities when utilising cloud services.

Case Study - Australian healthcare service data breach

In 2016, a company providing cloud services to a national healthcare service inadvertently exposed the details of 550,000 people online. A backup of a database containing personal information was accidently saved to a public-facing web server. The cloud service provider was found to be in breach of the *Privacy Act 1988* by disclosing personal information and failing to take reasonable steps to protect personal information.

The Office of the Australian Information Commissioner (OAIC) acknowledged the response by both parties to this incident was prompt and well managed. While the CSP was responsible for failing to protect personal information, the healthcare service was also found to be in breach of the Privacy Act, Australian Privacy Principle 11. This was due to not taking reasonable steps to ensure adequate security measures were taken by the CSP, and for having a data retention period that was longer than necessary. All affected individuals were contacted, information handling practices were improved, and information security was strengthened to mitigate against future breaches of this nature.

2. Legislative requirements

It is important to understand that healthcare organisations remain responsible for legislative obligations to protect all personal and health information that is collected, used and stored via a cloud service provider. This includes taking reasonable steps to ensure the CSP complies with applicable legislation.

- *Privacy Act 1988*
- State and territory privacy legislation
- My Health Record legislation.

For more information, read the Office of the Australian Information Commissioner's *Guide to Securing Personal Information*[3] and *Guide to Health Privacy*[4], available on the OAIC website.

3. Maintaining control of your healthcare information

One of the key issues that your organisation will face is maintaining control of personal health information, once it leaves your organisation's computer system and is transferred and stored with a CSP. There are two main considerations for maintaining your control of this information: data sovereignty and contractual arrangements.

Data sovereignty refers to the country in which data is stored and associated legal matters. It is important to know where the CSP is storing your organisation's data, as data stored in another country will be subject to the laws of that country.[5]

Australian healthcare providers are required to ensure Australian privacy laws are adhered to. This can be more challenging if data is stored in another country, particularly in cases where the country has fewer legal protections in place. Therefore, it is highly recommended healthcare providers ensure the CSP stores data in Australia as this will ensure consistency of legal protections, and will enable Australian authorities to provide assistance, if necessary.

Under the *Privacy Act 1988*, which applies to all private healthcare providers and Australian Government entities, there are certain conditions that apply in relation to overseas disclosure of information.

If you plan to engage a CSP that stores or processes data in another country, you will need to ensure the CSP complies with the Australian Privacy Principles, which are a key element of the Privacy Act. This includes ensuring reasonable steps are taken to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.[6] Work with the CSP to configure the solution to achieve an appropriate level of data protection. Check that the security configurations can be set to comply with all relevant legislation.

Contractual arrangements with a CSP should specify ownership rights, including that your data cannot be used by the CSP for their own purposes.

In addition, you will need to check what happens to your data when your contract with the CSP ends. It is important to ensure transferability provisions are in place for your data to make sure you receive a full copy of your data on contract termination. Then ensure the CSP permanently deletes any copies of your data (to be in compliance with data retention and disposal requirements).

If your CSP will be holding significant amounts of personal information on behalf of your organisation, you should seek legal advice.

4. Identification and management of your organisation's security risks

When implementing any ICT solution, including a cloud computing service, security risks need to be discussed and addressed. A good starting point can be a security risk management plan.

A security risk management plan will establish a framework for:

- assessing and identifying your organisation's most valuable assets (including information).
- identifying the security weaknesses (vulnerabilities) the CSP and your organisation may be susceptible to.
- mitigating the known threats (malicious or non-malicious) that may affect your organisation or the CSP.

The resultant security risk management plan should include the technical security controls that will assist in reducing or managing your healthcare organisations security risks when using a CSP.

In addition to technical security controls, you should also identify controls such as security governance, policies, contracts, physical security measures and well-trained staff who understand their role. These factors can each play an important part in mitigating your risk and protecting your data when a CSP is utilised.

5. Manage your CSP for business availability and functionality

Be aware of your dependency on a CSP in delivering your healthcare services. The more you rely on your CSP, the greater the attention required in managing risks associated with the CSP and related suppliers.

Your supply chain includes all organisations involved in the design, manufacture, supply, delivery, support and decommissioning of ICT hardware, software and services that are used within your organisation.[7] Risks associated with these organisations are known as your "supply chain risk".

Supply chain risk continues to increase as more companies look to outsource part or all of their business operations. Supply chain risk can include a range of issues, for example, the clinical software or security monitoring software your organisation uses may rely on other outsourced or sub-contracted services such as cloud services.

The interdependency of suppliers' services introduces additional risks including where the sub-contracted organisation's data is stored, a change in the supplier's ownership, or the cascading effect of a data breach due to unauthorised access (whether malicious or unintentional).

The priority is to ensure the continuity of your healthcare organisation's business operations when an incident occurs. This requires a clear understanding of how to respond and who is responsible for each of the required actions.[8]

Understand your CSP's method for managing backups of your data. If you need to recover from an incident, it is important that you have reliable backups available to enable data to be recovered.

To manage the risk of the CSP suffering a data breach or service failure, it is prudent for healthcare organisations to ensure a copy of their backed-up data can be restored in case of this type of situation.

Further guidance regarding good practices of backing up to protect your patient's information and your reputation can be found on the Australian Digital Health Agency's Cyber Security Centre webpage.

Regular reporting and reviews of the CSP gives healthcare organisations increased visibility to support understanding and managing cloud services to ensure business and security objectives are met. Be aware of contractual arrangements and understand what is, and is not, possible.

6. Consider the return on your investment

When reviewing CSP services, potential cost savings (on staffing and process efficiencies due to outsourcing) need to be balanced with the management of the CSP and the potential associated risks, including legislative and security risks.

Don't just select a CSP based on price, you need to understand the risk landscape and also identify what fees and charges will apply for additional services.

In addition, decision makers will need to understand the financial implications of moving from a capital expenditure model (upfront cost) for their own "on premises" ICT infrastructure to an operational expenditure model (ongoing cost) for outsourced ICT cloud services.

The following guidance materials can assist you with identifying what to ask a cloud service provider:

- Questions to ask about a cloud service.[9]
- Questions to ask your ICT vendors.[10]

What types of cloud services are available?

Organisations can consider using a combination of internal "on premise" ICT solutions and outsourced cloud services. When assessing the services of a CSP it is important to understand how your existing ICT environment and security controls will interact with the cloud service.

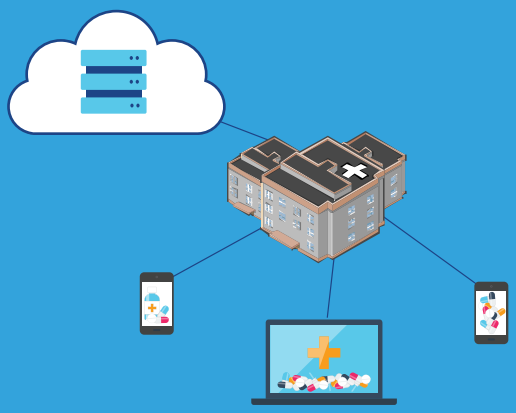
There are three main cloud services models which are offered and hosted by CSPs:[2]

1. **Infrastructure as a Service (IaaS)** – the CSP offers hardware services such as storage of data, and network bandwidth.
2. **Platform as a Service (PaaS)** – an organisation installs their own applications on the CSP's ICT infrastructure (the CSP may provide development services for building applications).
3. **Software as a Service (SaaS)** – the CSP provides the software for organisations to use. This may include, for example, desktop applications, mobile phone apps and medical device software.

There are four main cloud deployment models that healthcare organisations may use, as follows:[11]

Public Cloud

- services are accessed over a network that is open for use by any organisation
- offers a scalable data storage solution for managing short term projects or administration tasks
- commonly provided on a monthly subscription basis, which can make it more cost effective than other cloud models
- increased security risk due to need to maintain isolation between clientele

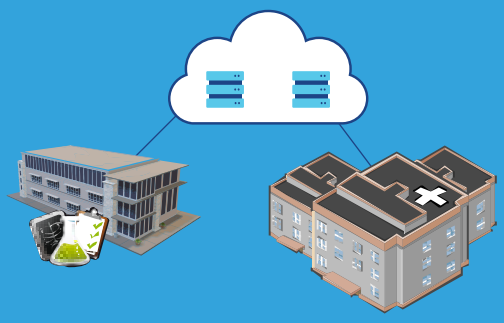


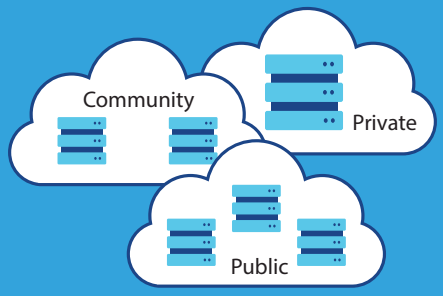
Private Cloud

- services are provided to a single organisation
- offers greater control over the data and managing obligations to protect personal and health information
- often more expensive than other cloud models
- reduced overall risk by avoiding infrastructure sharing

Community Cloud

- services are shared by organisations with common requirements
- often used for joint projects such as medical research studies
- costs are shared by the community of organisations using the service
- medium risk profile due to commonality of interests and risk profiles among clientele





Hybrid Cloud

- combination of private, public and community cloud services from different CSPs
- offers a way to diversify and manage the risks associated with having all services with one CSP
- provides more operational flexibility

Cloud services provide healthcare organisations with the flexibility to outsource some or all ICT functions. In addition to security and legislative requirements, an important consideration is to ensure visibility and seamless integration across an organisation's systems to support business availability and functionality.

Some cloud service providers will publish their own technical guidelines on how to securely use their service. However, healthcare organisations are advised to perform their own due diligence processes such as conducting risk assessments, obtaining legal advice and assessing the financial viability of a CSP before making any business decisions.

Further information

The Australian Digital Health Agency offers resources to assist healthcare providers to enhance their security practices.

Visit the Agency's website for additional guides and information on enhancing the security of your healthcare practice: https://www.digitalhealth.gov.au/healthcare-providers/cyber-security

For additional information or advice on whether a cloud service is suitable for your organisation you can consult the following resources:

Organisation	***Guidance materials***
Australian Cyber Security Centre (ACSC)	• Cloud Computing Security Considerations • Cloud Security Guidance • Cloud Computing Security for Cloud Service Providers • Cloud Computing Security for Tenants • Information Technology and Cloud Services • Cyber Supply Chain Risk Management
Department of Infrastructure, Transport, Regional Development and Communications	• Cloud computing and privacy – Small business factsheet • Questions to ask about a cloud service
Digital Transformation Agency (DTA)	• Secure Cloud Strategy • Managing cloud responsibilities
Office of the Australian Information Commissioner (OAIC)	• Data Breach Action Plan for health service providers • Guide to Securing Personal Information • Privacy for health service providers
Other	• US-CERT, The Basics of Cloud Computing • Cloud Security Alliance

References

1. Department of Infrastructure, Transport, Regional Development and Communications. *Cloud computing and privacy – Small business factsheet*. Available from: https://www.communications.gov.au/sites/g/files/net301/f/small-business-privacy-factsheet.pdf.

2. Australian Cyber Security Centre. *Cloud Computing Security Considerations*. Available from: https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-considerations.

3. Office of the Australian Information Commissioner. *Guide to securing personal information*. Available from: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/.

4. Office of the Australian Information Commissioner. *Guide to health privacy*. Available from: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-health-privacy/.

5. UNSW Cyberspace Law and Policy Centre. *Data Sovereignty and the Cloud: A Board and Executive Officer's Guide*. 2013. Available from: http://www.bakercyberlawcentre.org/data_sovereignty/CLOUD_DataSovReport_Full.pdf.

6. Office of the Australian Information Commissioner. *Chapter 11: APP 11 — Security of personal information*. Available from: https://www.oaic.gov.au/chapter-11-app-11-security-of-personal-information.

7. Australian Cyber Security Centre. *Information technology and cloud services*. Available from: https://www.cyber.gov.au/acsc/view-all-content/guidance/information-technology-and-cloud-services.

8. Office of the Australian Information Commissioner. *Data Breach Action Plan for health service providers*. Available from: https://www.oaic.gov.au/data-breach-action-plan-for-health-service-providers.

9. Department of Infrastructure, Transport, Regional Development and Communications. *Questions to ask about a cloud service*. Available from: https://www.communications.gov.au/sites/default/files/questionstoaskyourprovider.pdf.

10. Australian Digital Health Agency. *Selecting secure IT products and services*. Available from: https://www.digitalhealth.gov.au/healthcare-providers/cyber-security.

11. National Institute of Standards and Technology. *Definition of Cloud Computing*. Available from: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

Considerations prior to engaging a cloud service provider

A cloud services checklist for healthcare organisations

- Check that the cloud service provider meets your business objectives, security requirements and legal obligations.
- Choose a cloud deployment model which supports your organisation's risk profile.
- Check data sovereignty – where is your data stored with the cloud service provider?
- Confirm that the cloud service provider's contractual terms include service level agreements covering system availability, quality of service and your data ownership rights.
- Verify the cloud service provider's security posture and maturity. Are they certified to any ISO standards or utilise cyber security risk management frameworks?
- Request evidence of the cloud service provider's policies and procedures, including the security risk management plan, incident response plan, business continuity and disaster recovery plan.
- Is there visibility to monitor the currency and implementation of these plans and activities?
- Manage supply chain risk – identify your suppliers of software and services, their reliance and interdependency on other cloud services providers. Apply this checklist to all third parties in your supply chain.
- Maintain a backup of your organisation's data. This is in addition to the cloud service's backup copies.

Remember mitigating cloud services security risks requires a shared responsibility model

Review additional resources and references provided in this guide for further information

Publication date: October 2021 – second edition

Contact for enquiries

Telephone: 1300 901 001 or **email:** help@digitalhealth.gov.au

Acknowledgements

Council of Australian Governments
The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.

Australian Government

Australian Digital Health Agency

digitalhealth.gov.au