



Australian Government
Australian Digital Health Agency

CLOUD SERVICES

Considerations for healthcare organisations



*A guide for
healthcare providers*



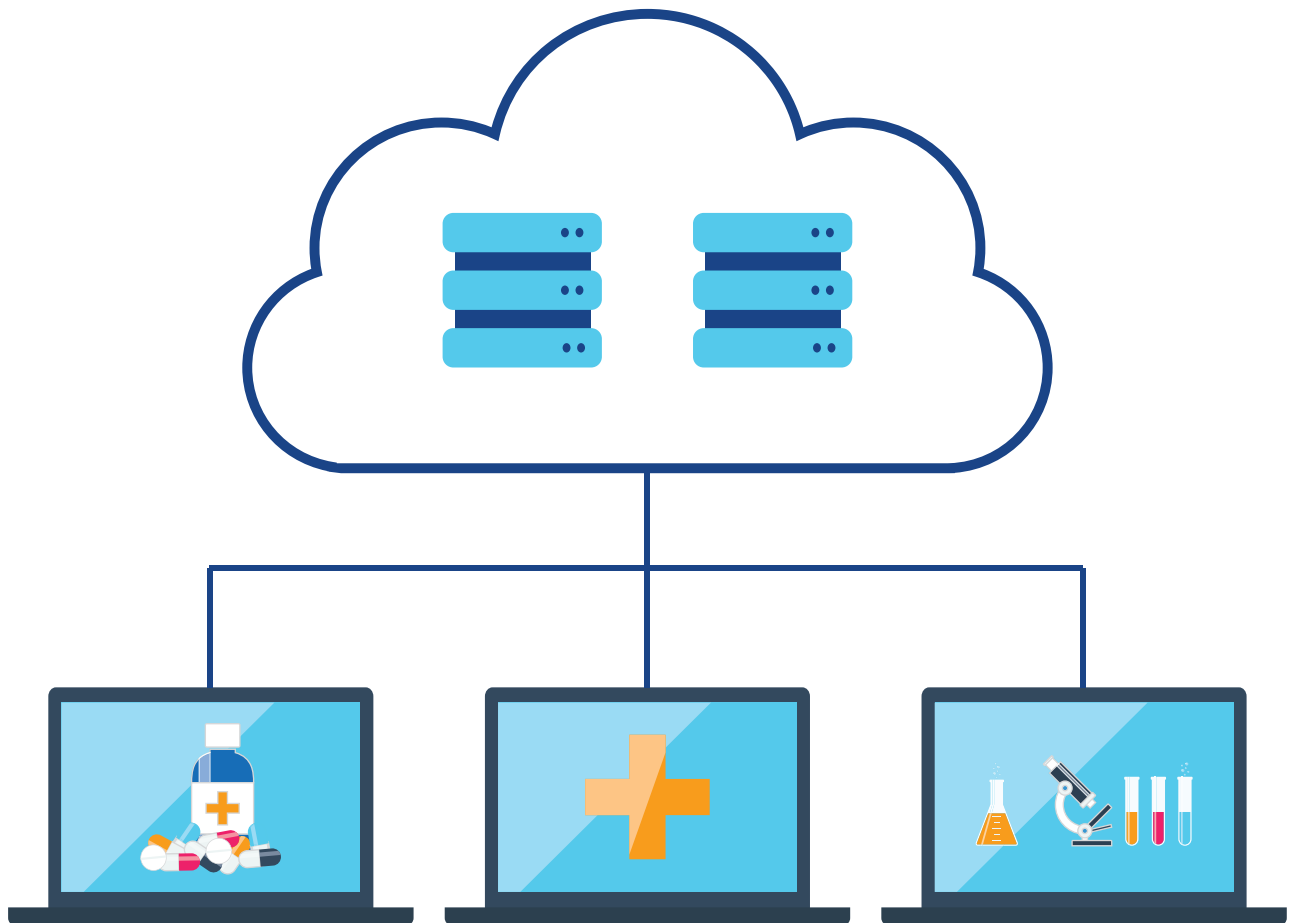
This guide is for healthcare organisations to assist in assessing whether engaging a cloud service provider (CSP) is appropriate for identified business needs. It covers some of the benefits and implications of implementing cloud services but does not take the place of conducting other due diligence 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.

Cloud services for healthcare

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. 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.

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



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 IT resources, software and services via the internet.

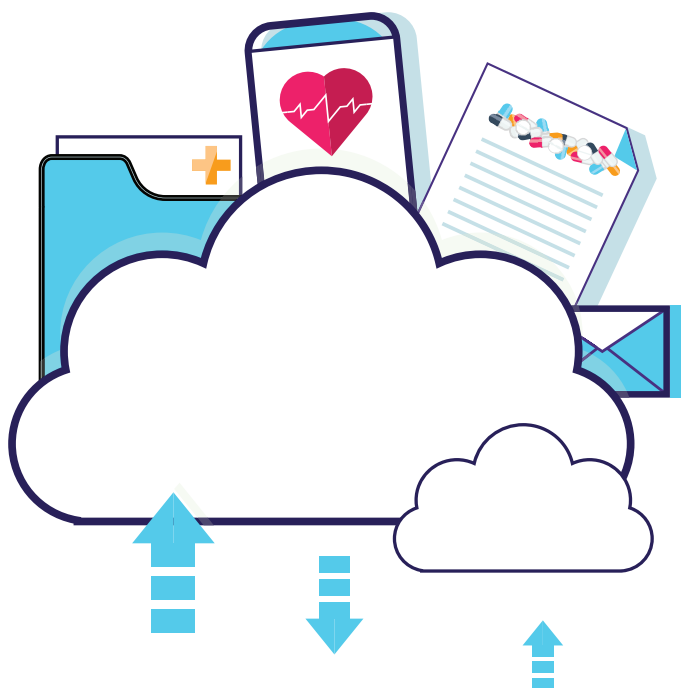
“Cloud computing is the practice of using servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.”²

For example, cloud services are used by some healthcare organisations to access software provided by the 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’).

Factors to consider when assessing a Cloud Service Provider

Some healthcare organisations use cloud services with the aim of achieving operational efficiencies, accessing the latest technology with less capital cost, and having the ability to quickly scale their business services to meet changing business demands.³ Alongside these likely benefits come potential issues and challenges.

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. 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. Healthcare organisations are ultimately responsible for ensuring the security of the health information they collect, use and store. Healthcare organisations are also accountable for any breaches of data.

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 accidentally saved to a public-facing web server. The CSP 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 to this incident by both parties 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](#) and [Guide to Health Privacy](#), 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.⁴

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.⁵ For more information on security considerations that may be relevant see the OAIC's [Guide to Securing Personal Information](#).

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

“Cloud service providers can become an integral part of business processes. Choosing providers who will be reliable, long-term partners is critical, as is ensuring that they implement adequate cyber security.”⁶

Take care to ensure your CSP **contractual arrangements** 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).

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

When implementing any IT 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. This requires a strong partnership and clear understanding between you, your CSP and your healthcare recipients.

Your supply chain includes all organisations involved in the design, manufacture, supply, delivery, support and decommissioning of IT 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 risk of change in ownership of the CSP, or the CSP suffering 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 and 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' IT infrastructure to an operational expenditure model (ongoing cost) for outsourced IT 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 IT vendors.](#)¹⁰

What types of Cloud services are available?

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

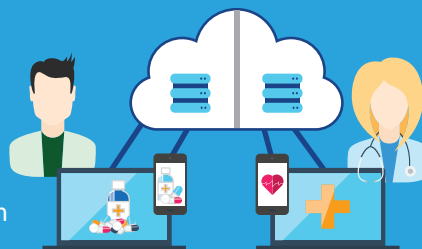
There are three main cloud services models which are offered and hosted by CSPs:¹¹

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 IT 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, including:¹²

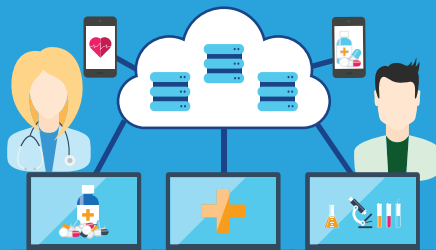
Public Cloud

- 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



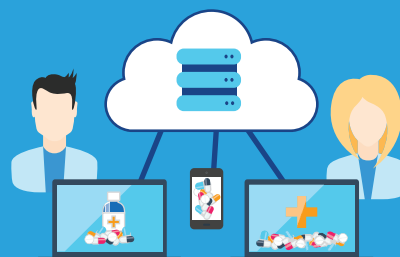
Private Cloud

- 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



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



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 the flexibility to outsource some or all IT 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 ensure they conduct 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: www.digitalhealth.gov.au/about-the-agency/digital-health-cyber-security-centre

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

Organisation	Guidance materials
Australian Cyber Security Centre (ACSC)	<ul style="list-style-type: none"> • Cloud Computing Security Considerations • Cloud Computing Security • Cloud Computing Security for Cloud Service Providers • Cloud Computing Security for Tenants • Cyber Supply Chain Risk Management Guidance
Department of Communications and the Arts	<ul style="list-style-type: none"> • Cloud computing and privacy – Small business factsheet • Questions to ask about a cloud service
Digital Transformation Agency (DTA)	<ul style="list-style-type: none"> • Secure Cloud Strategy • Managing cloud responsibilities
Office of the Australia Information Commissioner (OAIC)	<ul style="list-style-type: none"> • Data Breach Action Plan for health service providers • Guide to Securing Personal Information • Privacy for health service providers
Other	<ul style="list-style-type: none"> • The Basics of Cloud Computing • Cloud Security Guidance

References

1. Department of Communications and Arts: Cloud computing and privacy – Small business factsheet:
<https://www.communications.gov.au/sites/g/files/net301/f/small-business-privacy-factsheet.pdf>
2. Australian Cyber Security Centre (ACSC): Cloud computing security
<https://www.cyber.gov.au/advice/cloud-computing-security>
3. ACSC Cloud Computing Security Considerations:
<https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-considerations>
4. ACSC Cloud Computing Security
<https://www.cyber.gov.au/advice/cloud-computing-security>
5. Office of the Australian Information Commissioner
<https://www.oaic.gov.au/chapter-11-app-11-security-of-personal-information>
6. ACSC Cloud Computing Security
<https://www.cyber.gov.au/advice/cloud-computing-security>
7. ACSC Executive companion and Practitioners guide: Cyber Supply Chain Risk Management Guidance
<https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management-practitioner-guide>
8. Australian Government: Data Breach Action Plan for health service providers
<https://www.oaic.gov.au/data-breach-action-plan-for-health-service-providers>
9. Department of Communications: Questions to ask about a cloud service
<https://www.communications.gov.au/sites/default/files/questionstoaskyourprovider.pdf>
10. Australian Digital Health Agency: Questions to ask your IT vendor
<https://www.digitalhealth.gov.au/about-the-agency/digital-health-cyber-security-centre/toolkit-for-selecting-secure-it-products-and-services>
11. ACSC Cloud Computing Security Considerations:
<https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-considerations>
12. National Institute of Standards and Technology, Definition of Cloud Computing:
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

Publication date: April 2020

Contact for enquiries

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

Disclaimer

The Australian Digital Health Agency (“the Agency”) makes the information and other material (“Information”) in this document available in good faith but without any representation or warranty as to its accuracy or completeness. The Agency cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document control

This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

Copyright © 2020 Australian Digital Health Agency

This document contains information which is protected by copyright. All Rights Reserved. No part of this work may be reproduced or used in any form or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without the permission of the Australian Digital Health Agency. All copies of this document must include the copyright and other information contained on this page.

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