Government of **Western Australia**
Department of **Health**

Cloud Service Requirements

health.wa.gov.au

Cloud Service Requirements

1. Purpose

The *Cloud Service Requirements* supports the MP 0140/20 *Cloud Policy* and outlines the requirements to ensure the risks of storing and accessing WA health system information within cloud services are effectively assessed and managed.

1. **Infrastructure as a Service (IaaS)** provides servers, storage, and networking onto which customers install their own operating system and applications.
2. **Platform as a Service (PaaS)** provides fully maintained infrastructure and operating systems on which **applications** can be installed.
3. **Software as a Service (SaaS)** service provider hosted software applications made available over the **internet**. While configuration settings within the application can be managed by the customer, the supporting environment including backup and recovery, are the provider's responsibility.

Other cloud 'as a service' options are available. WA health system entities considering purchasing any cloud service should seek advice from the Health Support Services Security and Risk Management Team via email infosec@health.wa.gov.au

2. WA health system management of cloud

Cloud services have been categorised into three zones according to their respective risk profiles.

This three-zone model is intended to provide assistance in ascertaining how suitable a potential cloud service is and to mitigate common risks.

Where staff are uncertain about assessing the risks or suitability of a cloud service, advice can be sought from the Health Support Services Security & Risk Management Team via email: infosec@health.wa.gov.au

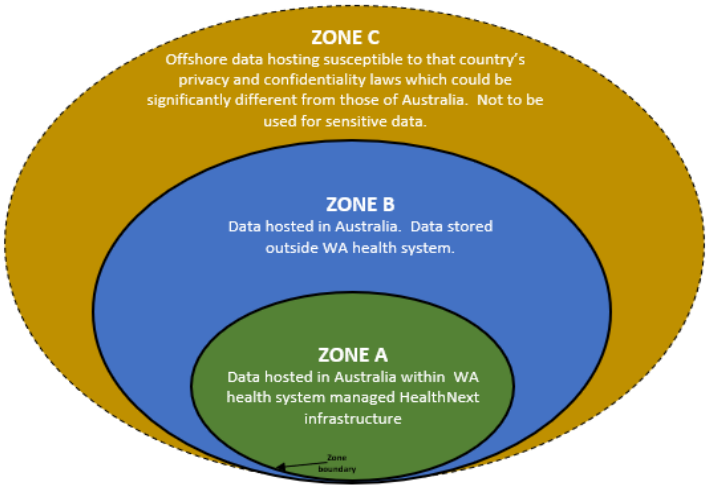

Diagram 1: WA health system's cloud zones

3. Cloud risk assessments

A risk assessment must be completed for each cloud service procured. Risk assessments must be provided to Health Support Services via infosec@health.wa.gov.au

The WA health system has undertaken provisional risk assessments of Zone A cloud services including establishing contractual arrangements to support the security and confidentiality of WA health system information. Zone A cloud services therefore require a short risk assessment only, as detailed in section 3.1.

Maintaining the privacy of personal information is a significant community expectation and legislative requirement. If personal information is stored in any cloud service, it must be managed in line with the *OD 0537/14 Information Classification Policy*.

Data Stewards must confirm a configuration baseline for each service in accordance with the relevant mandatory baseline needs detailed in the tables below.

Note: If information is intended to be stored or processed via any cloud zone covered under special legislative or protective controls (e.g. mental health, HIV, juvenile, etc), then the Data Steward must identify and satisfy those requirements in addition to the baseline requirements.

3.1 Cloud Zone A: HealthNext

Features:

- Utilises the WA health system managed services, support contracts and monitoring tools
- Offers pre-established processes to manage commissioning, billing, backups, and privacy.
- Provides a robust boundary for authentication, event monitoring, and information management.
- Contracts have been established to ensure that State and Commonwealth legislation applies.

If suitable cloud services can be arranged through the Zone A: HealthNext cloud, this service must be selected.

Baseline Requirements:

In addition to the Cloud Policy mandatory requirements, the following baseline requirements are the minimum attributes and processes to be implemented when deploying and using Zone A cloud services.

	Control	Baseline requirements
1.	**Classification of Information**	• Ensure the classification of the information to be stored and processed is clearly identified and communicated, to inform the risk assessment and control process in accordance with the OD 0537/14 *Information Classification Policy*. • The Classification will inform users of any special handling or control instructions e.g. The Classification may need to be included on login / processing screens and documentation.
2.	**Data Steward Approval**	• Ensure the Data Steward and Data Custodian of the information and system are identified and confirm there is full support for implementing the cloud service.

		• The Data Steward and Data Custodian will be the published contact for all queries relating to this service. • The Data Steward remains responsible for overall management and authorisations
3.	**Business Continuity Plans**	• Ensure business continuity plans are established to prevent/minimise service disruption, in the event of an internet outage, natural disaster or cyber-attack: - Vendor: will need backup and recovery plans - HSP and DOH: will need local business continuity plans. • Requirements for business continuity plans are outlined in OD 0595/15 *Business Continuity Management*. • Consult with the local site or application/information business continuity manager for details (if unsure request details from InfoSec@health.wa.gov.au).
4.	**Other Risks**	Ensure any other specific legislative requirements (e.g. mental health, HIV, juvenile etc.) and risks relevant to this information are addressed.

3.2 Cloud Zone B: Third party – Australian-Hosted

Features:

- Third party cloud services operating within Australian State, Territory or Commonwealth legal jurisdiction and/or where Australian Privacy Principles apply.
- Zone B cloud service providers may have standard contract terms which are not negotiable. Users need to exercise care and seek advice to ensure any clauses do not potentially or inadvertently compromise information security.
- Security, backup and business continuity processes may be managed by the external vendor. Controls must be clearly documented to ensure that information is backed up, secure and not accessible by unauthorised users.
- Vendor technical support staff will have full access to information hosted on their servers. Controls must be clearly documented to ensure that vendor access is managed via a suitable confidentiality agreement.
- Australian vendors may use a combination of Australian and offshore information storage. Contract documentation should provide details of these arrangements. Where information may be split between Australian and offshore data centres, the cloud service should be considered a Zone C – Offshore hosted cloud and the risk assessment detailed in section 3.3 applies.

Baseline Requirement:

The baseline requirements for Zone B include all requirements for Zone A and the following:

	Control	Baseline requirements
5.	**Evaluation due diligence**	Outline the reasons why Zone A is not suitable. The Data Steward needs to be satisfied that an assessment of Zone A services has been completed and it has been found not to be suitable.

	Control	Baseline requirements

6.	**Privacy**	Ensure privacy obligations can be met for the term of the contractual arrangement. These obligations include:
		• understanding how privacy of patients and staff could be jeopardised by the information being stored within the cloud service
		• obtaining assurance from the cloud service provider on the security and accessibility of information including:
		  ○ where it will be stored/backed-up
		  ○ who will have access to the information and how will this access be controlled
		  ○ how security will be managed within the cloud service
		  ○ whether the WA health system needs to relinquish control of the information.
		• obtaining confirmation from the cloud service provider regarding their compliance with Australian Privacy Principles, including how privacy breaches and any cross-border disclosure of personal information requests would be addressed
		• confirming that all information disclosure requirements, as outlined in MP 0015/16 *Information Access, Use and Disclosure Policy* and MP 0010/16 *Patient Confidentiality Policy* will be implemented.

7.	**Information breach notifications**	• Ensure that there is a clearly documented information breach management and notification process, including:
		  ○ who will receive notifications and when
		  ○ listing of any external parties to the contract who need to be notified
		  ○ how the vendor will respond if information is lost or accessed in the event of an accidental or malicious incident by an internal or external attack.

8.	**Security Standards**	• Ensure security standards comply with MP 0067/17 *Information Security Policy.* • Assess what security measures are available including the suitability of password complexity rules and use of two-factor authentication, for example, biometrics, SMS verification or authenticator application, wherever possible.

9.	**Identity management**	• Assess whether there are any risks posed by the types of user accounts to be registered with the vendor. For example:
		  ○ what login identities and passwords will be used
		  ○ who will have management responsibility

	Control	Baseline requirements
		○ what WA health system details will be registered with the cloud service provider (and how can these be minimised) • Any external registration must never re-use the WA health system's passwords.
10.	**Intended users**	• Understand who the intended users of the cloud service are (internal to the WA health system or public) • Assess any risks or issues posed via users accessing the service, for example, will the system be accessed by the public and how will access be managed. • Understand how access will be disabled when no longer required, for example, staff movement or departures.
11.	**Administrative access**	• Understand who will have full administrative access to the cloud service and the stored information. • If full control does not remain with the WA health system, ensure protection measures for stored information & information being transmitted are included (i.e. encryption).
12.	**Information ownership & retrieval**	Ensure that contract documentation: • stipulates the WA health system retains ownership of all information and/or intellectual capital (IP) - the vendor is not permitted to extract subsets or metadata for their own purposes, for example, marketing or service analysis • details what happens to the WA health system information if the cloud service provider is purchased by another company or the contract is terminated • clearly defines cloud service ownership and partnerships used to deliver the service, for example trusted third parties. • If the vendor is not independent, i.e. owned by a parent company, the contract documentation should also ensure that the WA health system entity's information cannot be accessed by the parent entity.
13.	**Compliance with WA health system retention, destruction and disposal policies**	• The WA health system's record retention requirements are as specified in the following schedules: ○ MP 0002/16 *Patient Information Retention and Disposal Schedule* ○ Retention and Disposal Schedule for Administrative and Functional Records

	Control	Baseline requirements
		• The cloud service provider should return information to the WA health system on request, and at the conclusion of the contract, in a usable format. • Information which may need to be used as evidence should be proven as authentic, reliable, and not altered or tampered with in any way.
14.	**Service Level Agreement (SLA)**	If a Service Level Agreement can be established for this arrangement, it must address the following: • Where, when, and how fast the service needs to be consumed • Acceptable service downtime arrangements for patch or maintenance activities.
15.	**Certification**	Information Security Registered Assessors Program (IRAP) or Service Organisation Control 2 (SOC 2) certification is considered highly desirable.
16.	**Penetration Test**	An independent penetration test of the proposed cloud service is considered highly desirable. It will provide information on whether there is any security: • vulnerabilities that an attacker could exploit, and/or • weaknesses that need to be addressed.
17.	**Costs**	• Ensure a total cost of operation comparison has been undertaken. • Verify the full tenure of the proposed cloud service – is there a contract/minimum term? • Verify the full financial costs of the proposed service during its lifetime – how will these be met, and by whom • Verify cloud service capacity to meet the required needs.

3.3 Cloud Zone C: Third party – Offshore-hosted

Features:

- Cloud services which are fully or partially managed or run on infrastructure outside of Australia, for example, overseas hosting or management where WA health system's information is in use, in transit or at rest, administration resourcing, or information back-up storage.
- Offshore information hosting is susceptible to that country's privacy and confidentiality laws which could be significantly different from those of Australia. In the event of an incident there may be no practical intervention possible from the WA health system, or any Australian legal or government entity.
- Not to be used for sensitive information.

Baseline Requirements:

The baseline requirements for Zone C include all requirements for Zone A, B and the following:

	Control	Baseline requirements
18.	The geographic location(s)	• Ensure the classification of the information is suitable for being offshore. • Ensure the country or countries in which the information will be stored are identified. • Ensure the contractual and legislative environment does not contravene the WA health system legal obligations for information protection, performance management, contract termination, contract management.
19.	Executive approval	Prior to the final deployment of any service into Zone C, written approval must be granted by the Data Steward (as per the Delegation Schedule – Health Information) and recorded in the Cloud Services Register.

This document can be made available in alternative formats on request for a person with disability.