healthOS

SECURITY POLICY

Security Incident and Data Breach Response

What counts as an incident, how it is contained and investigated, and who is told and when, including data breach notification.

Edition November 2026 · Public edition · Security: security@healthos.net.au

Contents

What counts as an incident 2

Roles 3

Severity 3

Detection: where the signal comes from 4

Response 4

1. Record and assess 4
2. Contain 4
3. Preserve evidence 5
4. Investigate and eradicate 5
5. Recover 5
6. Review 5

Data breach assessment and notification 5

Testing the plan 6

What counts as an incident

A security incident is any event that has compromised, or may have compromised, the confidentiality, integrity or availability of information HealthOS holds or of a system it connects to. In particular:

- personal or health information read, changed, sent or lost without authority, including one tenant's data reaching another tenant;
- a credential, signing secret or encryption key exposed or suspected exposed;
- an account used by someone other than its owner;
- malicious code, or an unauthorised change, in a deployed image, the repository or the infrastructure;
- a vulnerability reported to `security@healthos.net.au` (the contact in `website/.well-known/security.txt`) that is being exploited or is trivially exploitable;
- a fault in HealthOS that sends wrong or unauthorised requests to a government system (Services Australia, the My Health Record system, the NDIA APIs).

A suspected incident is handled as an incident until it is shown not to be one. Anybody who suspects one reports it; nobody is expected to be sure first.

Roles

ROLE	WHO	DOES
Incident lead	Aaron Le Saux	Runs the response, decides severity, keeps the incident record
Deputy	None appointed (risk R-014). The sealed emergency access pack described in the continuity policy, section 7, is the interim measure	Acts when the lead is unreachable
Privacy officer	Aaron Le Saux	Runs the data breach assessment, makes the notifications
Engineering	Whoever the lead calls in	Contains, investigates, fixes
Executive approver	Aaron Le Saux	Approves external statements and notifications

One person may hold more than one role. The lead and the executive approver are never the same person for a Severity 1 incident. Until there is a second person they are: the decision and its reason are recorded at the time, and the independent security adviser reviews them afterwards.

How to report one: email security@healthos.net.au. Out of hours, phone the incident lead's mobile; the number is kept in SharePoint: HealthOS ISMS > Contacts and given to customers in their onboarding pack, not published here.

Severity

SEVERITY	MEANING	LEAD ENGAGED WITHIN	EXAMPLES
1	Confirmed or likely unauthorised access to personal or health information, a compromised production key or secret, or a compromised production system	1 hour, any hour	Cross-tenant read confirmed; `JWT_SECRET` or `FIELD_ENCRYPTION_KEY` exposed; a PRODA device key exposed
2	A real weakness with no evidence yet of access, or an incident confined to one account	4 hours	An exploitable vulnerability report; one staff account taken over; sustained probing that reached data it should not
3	An attempt that the controls refused, or a weakness that needs unusual access to use	Next business day	A burst of refused cross-tenant requests; a scanner finding rated Medium

Severity is set by the lead and may only be lowered with a written reason.

Detection: where the signal comes from

These exist in the system today and are where an investigation starts.

SOURCE	WHAT IT SHOWS
Azure Monitor alerts (`infra/modules/security-alerts.bicep`)	One source probing (more than 20 refusals in 10 minutes) and distributed probing; emailed to `securityAlertEmails`
`platform.security_events` **and** `GET /api/v1/admin/security-events`	Every refused cross-tenant or token-misuse attempt, with source address, user and route — see security-events.md
`audit_access_log`	Every read of a clinical record: who, which person, from where, with flags for unusual access
`audit_log`	Every change to a record, with old and new values
`credential_access_log`, `integration_auth_failure_log`	Each use of a stored credential, and each failed authentication to a government service
Container Apps console logs (Log Analytics)	Application logs, with tokens and identifiers redacted (`utils/logging/redaction.ts`)
CI security scans (`security-scan.yml`, `security-static.yml`, `secret-scan.yml`**)**	Vulnerable images, risky code patterns, secrets in commits
`security@healthos.net.au`	Reports from customers and researchers

All the audit tables above are append-only: an UPDATE or DELETE raises. An investigation can rely on them not having been edited through the application's database role.

Response

1. Record and assess

The lead opens an incident record at once: time reported, who reported it, what is known, severity. Every later action and decision is added with its time. The record is kept in SharePoint: HealthOS ISMS > Incident register, outside the systems that may be affected.

2. Contain

Stop the harm before understanding it fully. The usual moves, each of which this system supports:

- **Exposed secret or key:** rotate it using key-rotation.md. Rotating a signing secret signs every user out, which also ends any stolen session.
- **Compromised account:** disable the account and revoke its sessions; for a privileged infrastructure account, remove its role assignments.
- **Bad release:** redeploy the previous image. Images are tagged and deployed by commit SHA, so the previous one is known exactly.
- **Compromised government credential:** disable the PRODA device or NASH certificate with its issuer, and switch the affected organisation's integration off.

- **Active attack on one route:** block the source at the edge, or withdraw the route.

Do not delete anything, and do not restart or rebuild a compromised component before its logs and state have been preserved.

3. Preserve evidence

Export the relevant rows of the audit tables and the Log Analytics results for the window, and record the image SHAs that were running. Log Analytics retention is 90 days (`infra/modules/container-apps-env.bicep`): export before it lapses.

4. Investigate and eradicate

Establish what happened, what was reached, whose information it was, and for how long. Fix the cause in the development environment and release it the normal way (secure-development.md); an emergency fix still goes through review, by a second person, before it deploys.

5. Recover

Restore service and data (infra/BACKUP-AND-RECOVERY.md has the restore procedure), confirm the fix on the deployed stack, and watch the detection sources above for recurrence for at least 14 days.

6. Review

Within 10 business days of closing a Severity 1 or 2 incident, the lead writes a review: timeline, cause, what worked, what did not, and the actions that follow, each with an owner and a date. The review is about the system and the process, not about who made a mistake.

Data breach assessment and notification

The privacy officer starts this as soon as an incident may involve personal information; it runs beside the response, not after it.

Assessment. Decide whether the incident is an eligible data breach: unauthorised access to, disclosure of, or loss of personal information that is likely to result in serious harm to any individual, where remedial action has not removed that likelihood. The assessment is completed as fast as practicable and in no case later than **30 days** after becoming aware (Privacy Act s 26WH). The reasoning is written into the incident record whichever way it goes.

Who is told, and when.

WHO	WHEN	BY WHOM
The affected customer organisation	Without delay once their data is known or suspected to be involved, and in no case later than 72 hours. HealthOS usually holds this data on the customer's behalf, and the customer has its own obligations to meet	Privacy officer

WHO	WHEN	BY WHOM
The Office of the Australian Information Commissioner	As soon as practicable after concluding there is an eligible data breach, using the OAIC's notification form. Where the customer is the entity that holds the information, agree with them who lodges it; it must be lodged once	Privacy officer, with the executive approver
Affected individuals	As soon as practicable after the OAIC statement, directly where possible	The customer organisation, or HealthOS by agreement
The NDIA (Digital Partnership Office)	**Immediately** on becoming aware of a breach or possible breach of the Privacy Act or the NDIS Act in connection with the NDIA APIs, by HealthOS, its people or an end user (Terms cl. 4.3). Also promptly for any event that has or may have compromised the security or integrity of the API or the NDIA's systems or data (cl. 5.2(b))	Incident lead
Services Australia, the Australian Digital Health Agency	As their agreements and conformance terms require, where their services or identifiers are involved	Incident lead
The Australian Cyber Security Centre	Optional report through cyber.gov.au for a Severity 1 incident	Incident lead

For the NDIA, "possible" matters: the obligation starts at suspicion, before the assessment is finished. HealthOS then follows any reasonable direction from the NDIA and gives the help it asks for (cl. 4.3, 5.3), including API access logs (cl. 3.5 requires at least three months to be producible).

The contact list for each of these bodies is kept in SharePoint: HealthOS ISMS > Contacts and checked when this policy is reviewed.

Testing the plan

Once a year the lead runs a tabletop exercise on a scenario from the severity table, with everyone who holds a role, and records what was learned. A plan that has never been walked through is assumed not to work.

healthOS

Questions about security

Email **security@healthos.net.au**. To report a vulnerability, see https://healthos.net.au/trust/#disclosure.

© 2026 HealthOS Pty Ltd · ABN 81 697 460 889. This is the public edition. The web edition is at https://healthos.net.au/trust/policy-incident-response.html.