



Information Breach Response Guide

WA health system entities are responsible for ensuring that misuse and inappropriate access, use, disclosure and/or loss of information held within the system are identified and future breaches mitigated. It is the responsibility of WA health entities to ensure that contracts where information is exchanged includes the requirements of the Information Breach Policy.

WHAT IS A SUSPECTED OR KNOWN INFORMATION BREACH ?



An information breach occurs when information that an entity holds is subject to unauthorised access, use or disclosure or is lost, damaged or destroyed. **Follow steps 1-4 to respond .**

Email: RoyalSt.PSPInfoManagement@health.wa.gov.au if you have any queries.
Link into the **Information Breach Response Standard** for more details.



1

CONTAIN



In the event of a breach the person who discovers the breach must immediately take whatever measures possible to contain the breach, minimise damage, and prevent any potential harm.

The person who is responsible for containing the breach collects information about the breach, preserves evidence, and must record the details in the **Information Breach Notification Form 'Part 1 Information Breach Report'** and immediately notify their line manager and follow local policies and procedures.

2

ASSESS



An assessment of the breach must be undertaken by the relevant Manager, Information Custodian or applicable person assessing the breach must complete **'Part 2 Information Breach Assessment and Resolution'** section of the Information Breach Notification Form.

Potential breach of discipline/code of conduct? If yes, immediately contact the relevant WA health system entity's responsible area and comply with their instructions. This will be the Integrity Unit, Human Resource/Workforce Unit, or other responsible as per the local policies and procedures.

Cyber security breach? If yes, immediately contact **Health Support Services ICT help desk: 13 44 77** or email: infosec@health.wa.gov.au

To report a suspicious email/text or phone call, email: scam@health.wa.gov.au

3

NOTIFY



Subject to the circumstances of the information breach, there are various notifications and communications that must be undertaken where relevant.

- Information Asset Custodian
- Information Steward
- Breach of Discipline or Code of Conduct
- Communications Directorate and/or the relevant WA health system entity
- Human Research & Ethics Committee
- Legal and Legislative Services
- Inform affected individuals/patients/clients
- Department of Health – Information and Performance Governance
- Commonwealth Data
- Other agencies

4

REVIEW



In this final stage of the Information Breach Response, the assessor will:

- Review the assessment to ensure all applicable notifications have been made
- Determine if further actions or investigation are required
- Assess the risk
- Prevent Recurrence
- Forward Information Breach Notification form to : RoyalSt.PSPInfoManagement@health.wa.gov.au



Complete assessment within 30 calendar days