Information Breach Response – Checklist

Responding to an information breach or suspected breach involves taking into consideration 4 key stages.

1. **Contain** the breach to minimise the damage and prevent harm
2. **Assess** the details of the incident
3. **Notify** relevant bodies/persons
4. **Review** the incident, assess the risks and prevent recurrence

Below is a checklist of the steps within each of the stages in order to formulate a comprehensive response when completing the Information Breach Notification Form. For more details around each of the key stages, refer to the Information Breach Response Standard, Section 5.0 Information Breach Response.

Email queries to: RoyalSt.PSPInfoManagement@health.wa.gov.au

	1 CONTAIN *Contain the breach to minimise the damage and prevent harm*	✓
1	**Take measures to contain the breach, minimise damage and prevent any potential harm.** • Limit distribution of affected information. • Suspend activity that led to the breach. • Revoke or change access codes and/or passwords. • Remove/relocate the information asset.	
2	**Complete Information Breach Notification Form. The completion of the form is a mandated requirement in the policy and must be commenced at the time of discovery of an actual or suspected information breach.** • The person who is responsible for containing the breach, preserves evidence and records the details in *Part 1 Information Breach Report* of the form. • They must immediately notify their line manager and follow local policies and procedures.	
	2 ASSESS *Assess the details of the incident*	✓
3	**An assessment of the breach must be undertaken by an appropriate assessor/s. The purpose is to determine the extent of damage and harm caused.** • The appropriate assessor will depend on circumstances. This could be the Information Custodian, a Manager or other person deemed appropriate and impartial. • The assessor completes *Part 2 Information Breach Assessment and Resolution.* • In cases of a suspected breach of discipline or code of conduct, advice must be sought from the relevant WA health system entities responsible area prior to proceeding to interview any employees. This	

	will be the Integrity Unit, Human Resources/Workforce Unit, or other responsible area as defined in local policies and/or procedures. • It is important to follow local policies and procedures.	
4	**Details of the breach** • The type and sensitivity of information involved e.g. health or personal information or a combination of types of information.	
5	**Source of the breach** • The source of the breach must be fully investigated to determine the root cause and/or causal factors that contributed to the incident. • Did the breach occur due to malicious intent, through inadvertent oversight/human error.	
6	**Impact assessment – the impact of the breach depends on the nature and extent of the breach.** • The extent of the breach. • Was there harm to individuals (or to a WA health system entity). • Financial and reputational loss.	
	3 NOTIFY *Notify relevant bodies / persons where applicable*	✓
7	**Information Asset Custodian** • To identify the relevant custodian refer to the instrument of delegation and the WA health system Information Register.	
8	**Information Steward** • provide strategic guidance and executive-level support where the information breach involves an information asset under their stewardship.	
9	**Information Sponsor** • The sponsor is allocated functions to assist the Steward in the operation of managing Information Assets.	
10	**Breach of Discipline or Code of Conduct** • Information breaches involving an employee member, which may be a breach of discipline or the Code of Conduct, must be reported to the relevant WA health system entity.	
11	**Information Systems Security** • The Health Support Services (HSS) Security and Risk Management Unit is to be notified of cyber security breaches and can be contacted on infosec@health.wa.gov.au • To report a suspicious email/text or phone call, email scam@health.wa.gov.au • The HSS ICT Help Desk can be contacted on 13 44 77.	
12	**Affected Individuals** • Consideration needs to be given on whether notification is provided to any affected individuals. The assessor in conjunction with relevant stakeholders, must assess who should be notified, when and how the notification should occur, who should make the notification and what information should be included.	
13	**Communications Directorate and/or the relevant WA health system entity communication area**	

	• To assist in communicating the details of the information breach within or external to the WA health health system, including the media and external stakeholders.	
14	**Human Research & Ethics Committee** • If the information breach pertains to a research project that was approved by a WA health system Human Research Ethics Committee and Research Governance Office.	
15	**Legal and Legislative Services** • For legal advice, or the General Counsel (where applicable) for entity specific legal advice.	
16	**Other agencies or organisations affected by the breach** • Parties under the terms of an agreement, Memorandum of Understanding or contract must be notified.	
17	**Department of Health – Information & Performance Governance** • The Information Breach Notification Form is sent to the Department of Health – Information and Performance Governance (IPG) unit. RoyalSt.PSPInfoManagement@health.wa.gov.au.	
18	**Commonwealth Data** • There may be information held within the WA health system that is collected under the Commonwealth Legislation. Any breach involving Commonwealth data must be reported in accordance with the relevant legislative requirements.	
	4 REVIEW *Review the incident, assess the risks and prevent recurrence*	✓
19	**Ensure that all applicable notifications have been made. Determine if further actions or investigation is required** • Assess the Risk. • Prevent Recurrence.	
20	**Risk Assessment** • Entities are responsible for ensuring that risks to their organisations are identified and managed. • Assessor must consider all the information gathered during the assessment stage and refer to the Risk Assessment Tables for the WA health system.	
21	**Prevent Recurrence** • An essential and final stage of the Information Breach response is to mitigate the risk of a recurrence. • At a minimum relevant amendments to policies, processes and procedures must be made where necessary.	
22	**Expected Response time** • Reasonable steps should be taken within the first 24hours to contain the breach. • The assessment and Information Breach Notification Form should be completed within 30 calendar days of identification of the breach. • Information Breach Notification Form to be emailed to the RoyalSt.PSPInfoManagement@health.wa.gov.au	