Government of Western Australia
Department of Health

Policy Frameworks
MP 0135/20
Effective from: 28 April 2021

Information Breach Policy

1. Purpose

The purpose of the *Information Breach Policy* is to ensure that misuse and inappropriate access, use, disclosure and/or loss of information held within WA health system entities is investigated and solutions are identified and implemented to mitigate future breaches.

An information breach occurs when information that an entity holds is subject to unauthorised access, use or disclosure, or is lost, damaged or destroyed. An information breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems[1].

Examples of information breaches include:

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
- unauthorised access to personal information by an employee
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person
- disclosure of information to a scammer, as a result of inadequate identity verification procedures.

This Policy applies to all information generated, collected, accessed, used, managed, stored and disclosed by the WA health system entities including, but not limited to, information collected under the *Health Services Act 2016*, *Health (Miscellaneous Provisions) Act 1911, Mental Health Act 2014*, *Private Hospital and Health Services Act 1927, Public Health Act 2016, Public Sector Management Act 1994* or any other written law.

This Policy is a mandatory requirement under the *Information Management Policy Framework* pursuant to section 26(2)(k) of the *Health Services Act 2016*.

This Policy is a mandatory requirement for the Department of Health pursuant to section 29 of the *Public Sector Management Act 1994*.

2. Applicability

This Policy is applicable to all WA health system entities, as defined in this Policy.

To the extent that the requirements contained within this Policy are applicable to the services purchased from contracted health entities, WA health system entities are responsible for

[1] This definition has been adapted from the Office of the Australian Information Commissioner's Data breach Preparation and Response Guide available from https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response

ensuring these requirements are accurately reflected in the relevant contract and managed accordingly.

3. Policy requirements

WA health system entities are required to have local policies, processes and/or procedures to manage the prevention, containment, remediation and investigation of information breaches.

When an information breach becomes known, WA health system entities must take all reasonable actions required to minimise the damage of the information breach, including taking action to:

1. contain the information breach
2. assess the impact of the information breach to determine the extent of the damage and harm caused
3. remediate any risk of further harm
4. review the incident and take preventative actions.

WA health system entities are required to determine the appropriate roles and responsibilities to address the circumstances of the breach.

3.1 Contain the information breach

WA health system entity employees are required to:

- take action to contain any known or suspected information breach including taking immediate action that is reasonably practical to:
    - limit any further access, loss or damage
    - limit distribution of the affected information
    - prevent any further compromise of the information
- immediately notify the relevant WA health system entity Integrity Unit when a breach has occurred.

Health Support Services, in undertaking their IT support functions, is also required to:

- immediately notify the relevant WA health system entity and provide assistance when applicable.

3.2 Assess the impact of the information breach

WA health system entity employees are required to:

- complete the Information Breach Notification Form
- notify their line manager or the WA health system entity delegated authority of the identified breach
- notify the information custodian (if applicable)
- provide any information required to assist the investigation.

The line manager and/or the WA health system entity delegated authority are required to:

- undertake an assessment of the information breach to determine the extent of the damage and harm caused
- determine if misconduct may have contributed to the information breach
- report any potential misconduct as per the *Code of Conduct Policy*

- liaise with the information custodian (if applicable) or other stakeholders as required (refer to 'other stakeholders' listed in the information custodian requirements below)
- provide the Information Breach Notification Form assessment findings to the information custodian (if applicable)
- ensure the assessment is completed expeditiously within a reasonably practicable timeframe.
- prepare an explanation if the assessment is not conducted expeditiously and provide it to an investigator, auditor and/or the System Manger as requested.

The information custodian (if applicable) is required to:

- review the Information Breach Notification Form assessment findings provided by the line manager and/or the WA health system entity delegated authority
- undertake an additional assessment of the information breach to determine the extent of the damage and harm caused
- liaise with other stakeholders as required. This may include, but is not restricted to:
    - Health Support Services – to establish the cause and impact of an information breach that involves ICT systems. For example, reviewing system security, audit logs, authentication processes.
    - Information Steward – to provide strategic guidance and Executive-Level support where the information breach involves an information asset under their stewardship.
    - Information and Performance Governance – for information breach policy and compliance advice.
    - WA health system entities Integrity Unit – for integrity advice and assistance on local issues and investigations.
    - System-wide Integrity Services (SWIS) – for integrity advice and assistance for Department of Health and system wide issues.
    - Legal and Legislative Services – for legal advice, or the General Counsels (where applicable) – for Health Service Provider specific legal advice.
    - Communications Directorate and/or the relevant WA health system entity communication areas – to assist in communicating details of the information breach within or external to the WA health system, including the media and external stakeholders.
    - Human Research Ethics Committees/Governance Office – if the breach pertains to a research project that was approved by a WA health system Human Research Ethics Committee and Research Governance Office, the breach must be reported to the relevant committee and office that approved the research project.
    - External agencies – including, but not limited to, the Corruption and Crime Commission, the police or law enforcement bodies.

3.3 Take actions to remediate any risk of further harm

WA health system entity employees and information custodians (if applicable) are required to:

- undertake all reasonable actions to reduce potential further harm from the information breach
- notify individuals who have been adversely impacted (when appropriate).

3.4 Review the incident and take preventative actions

WA health system entity employees are required to:

- identify and implement solutions within their remit to address the cause of the information breach and prevent future breaches from occurring
- ensure any implemented solutions do not prevent the collection, use and/or disclosure of information that is permitted or required by law
- notify the appropriate area if the identified solution is not within the employee's remit or area of expertise.

WA health system entities and information custodians (if applicable) are required to:

- review the incident and take appropriate preventative actions such as:
    - a security review including a root cause analysis of the information breach
    - a prevention plan to prevent similar incidents in future
    - audits to ensure the prevention plan is implemented
    - a review of policies and procedures and changes to reflect the lessons learned from the review
    - change employee selection and training practices
    - a review of service delivery partners that were involved in the breach.
- establish and/or amend any local policies, processes and/or procedures to prevent future breaches from occurring
- ensure any preventative actions do not prevent the collection, use and/or disclosure of information that is permitted or required by law
- email the competed Information Breach Notification Form to the Information Governance and Performance Unit (via:RoyalSt.PSPInfoManagement@health.wa.gov.au)

4. Compliance monitoring

Health Service Providers are responsible for complying with this Policy.

The System Manager, through the Purchasing and System Performance Division, Department of Health, may carry out compliance audits to ascertain the level of Health Service Provider compliance with this Policy and may provide updates to Information Stewards, Chief Executives of Health Service Providers, the Director General and other relevant persons regarding the findings of compliance monitoring activities.

The Department of Health (Information and Performance Governance Unit), as a Department of State, is responsible for monitoring and reporting Department of Health compliance with this Policy to Executive.

5. Related documents

The following documents are mandatory pursuant to this Policy:

- Information Breach Notification Form

6. Supporting information

The following information is not mandatory but informs and/or supports the implementation of this Policy:

- Information Breach Process Guide

7. Definitions

The following definition(s) are relevant to this Policy.

Term	Definition
access	Refers to the right or opportunity to use or view information. An individual enacts this access when they use, view or enter the environment in which this information is held.
data	The term 'data' generally refers to unprocessed numbers, facts or statistics, while the term 'information' refers to data that has been processed in such a way as to be meaningful to the person who receives it. The terms 'data' and 'information' are often used interchangeably and should be taken to mean both data and information.
disclosure	A person discloses information if they cause the information to appear, allow the information to be seen, make the information known, reveal the information or lay the information open to view.
Health information	Has the meaning given in the *Health Services Act 2016* in section 213 as: (a) information, or an opinion, that is also personal information, about: (i) the health (at any time) of an individual; or (ii) a disability (at any time) of an individual; or (iii) an individual's expressed wishes about the future provision of health services to the individual; or (iv) a health service provided, or to be provided, to an individual; or (b) other personal information collected to provide, or in providing, a health service.
information	The terms 'information' generally refers to data that has been processed in such a way as to be meaningful to the person who receives it. Information can be personal or non-personal in nature. The terms 'data' and 'information' are often used interchangeably and should be taken to mean both data and information in this Policy.
information breach	Refers to an incident, in which personal or confidential information, or non-personal information that could be sensitive or commercial, is compromised, disclosed, copied, transmitted, accessed, removed, destroyed,

Term	Definition
	stolen or used by unauthorised individuals, whether accidentally or intentionally.
information custodian	The person(s) responsible for the day-to-day management of a data collection or information.
non-personal information	Information from which a person's identity is not apparent, and cannot be reasonably ascertained. Whether information is truly non-personal will depend on the context, including the nature of the information, the number of people to whom it could potentially relate and the amount of information proposed to be disclosed. Although a series of individual pieces of information may not, on their own, enable the identity of an individual to be ascertained, identification may occur when all the pieces of information are combined together.
personal information	Has the meaning given in the *Freedom of Information Act 1992* in the Glossary clause 1: Means information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual, whether living or dead — (a) whose identity is apparent or can reasonably be ascertained from the information or opinion; or (b) who can be identified by reference to an identification number or other identifying particular such as a fingerprint, retina print or body sample.
use	A person 'uses' information if they: employ the information for some purpose, put the information into service, turn the information to account, avail themselves of the information or apply the information for their own purposes.
WA health system	Pursuant to section 19(1) of the *Health Services Act 2016*, means the Department of Health, Health Service Providers and to the extent that Contracted Health Entities provide health services to the State, the Contracted Health Entities.
WA health system entities	• All Health Service Providers as established by an order made under section 32(1)(b) of the *Health Services Act 2016*; • The Department of Health as an administrative division of the State of Western Australia pursuant to section 35 of the *Public Sector Management Act 1994*. Note: Contracted health entities are not considered WA health system entities.

8. Policy contact

Enquiries relating to this Policy may be directed to:

Title: Assistant Director General

Directorate: Purchasing and System Performance Division

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

9. Document control

Version	Published date	Effective from	Review date	Effective to	Amendment (s)
MP0135/20	6 May 2020	6 May 2020	May 2023	4 August 2020	Original version
MP0135/20 v.1.1	4 August 2020	4 August 2020	May 2023	28 April 2021	Minor amendment details summarised below:
Minor amendment to *Information Breach Notification Form* to: • Section 2 Information Classification to align with OD 0537/14 *Information Classification Policy* sensitivity and risk classifications • Amend wording in Section 4 from 'Cause and estimated cost of the information breach (if known)' to 'Cause and estimated impact of the information breach (if known)' • Address formatting inconsistencies					
MP0135/20 v.1.2	28 April 2021	28 April 2021	May 2023	Current	Minor amendment to *Information Breach Notification Form*

10. Approval

Approval by	Nicole O'Keefe, Assistant Director General, Strategy and Governance Division, Department of Health
Approval date	5 May 2020

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