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

Information Breach Response Standard

health.wa.gov.au

Owner:	Department of Health, Western Australia - Information and Performance Governance
Contact:	Anthony Jones
Approved by:	Giulia Clifford
Approval Date:	08/05/2023
Current Version:	3.0
Links to:	Information Management Policy Framework

VERSION	DATE	AUTHOR	COMMENTS
3.0	8 May 2023	Kathleen Alloway & Wendy Ugarte	Approved by the Assistant Director General, Purchasing and System Performance.

Contents

Acronyms

CE	Chief Executive
DG	Director General
WA	Western Australia
IMGAG	Information Management Governance Advisory Group
EDRMS (TRIM)	Electronic Document Records Management System
HSS	Health Support Services
IPG	Information and Performance Governance

1 Purpose

The Information Breach Response Standard is a related document in the *Information Breach Policy*. The purpose of the standard is to mandate the minimum requirements to manage and respond to an information breach.

2 Introduction

Information in the WA health system is collected, accessed, stored, used and disclosed to support the realisation of WA health system's vision to have a sustainable health system that delivers safe, high quality health care to all Western Australians. It is therefore imperative that information is valued, available, shared, governed, trustworthy, secure and protected.

An information breach refers to an incident in which personal or confidential information, or non-personal information that could be sensitive or commercial is compromised. The information may be 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.

Information breaches can be caused or exacerbated by a variety of factors, involve different types of information, and give rise to a range of actual or potential harms to the individuals and WA health entities whose information is compromised.

As such, there is no single way of responding to an information breach. Each breach will need to be dealt with on a case-by-case basis, with an understanding of the risks posed by a breach and the actions that would be most effective in reducing or removing these risks.

A quick and effective response can reduce the likelihood of affected individuals suffering harm, lessen the impact of an ongoing breach of an information asset, or financial or reputational damage to the organisation.

3 Information

The term ‘information’ generally refers to records, data or information 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 document.

WA health entity information assets are listed in the WA health system Information Register.

An information asset is a collection of information that is recognised as having value for the purpose of enabling the WA health entities to perform its clinical and business functions, which include supporting processes, information flows, reporting and analytics.

An information breach may involve more than one type of information asset or other information record. Information may be, but is not limited to:

- patient or employee health and personal information
- business and corporate information
- digital information and records in:
    - office applications – for example, word-processed documents, spreadsheets, presentations and desktop-published documents
    - online and web-based environments such as intranets, internets and public websites
    - clinical and patient administration information systems
    - business information systems such as databases, geospatial data systems, human resources systems, financial systems, client management systems, and electronic document and records management systems (EDRMS/TRIM)
    - digital communication systems such as SMS (short messaging services), MMS (multimedia messaging services), voicemail, instant messaging, paging messaging, video conferencing and teleconferencing.
- data from external organisations. For example, other government agencies, St John’s Ambulance, Private Hospital patient activity data.
- printed materials – for example, documents, reports and briefing notes
- email and other correspondence
- images, video or sound recordings
- biological or physical samples.

4 Information Breach Categories

There can be many different types of information breaches. Common information breaches typically relate to:

- information systems security
- health or personal information
- corporate, financial or workforce information
- environmental or physical.

4.1 Information systems security breach

An information system security breach is any incident that results in unauthorised access of information, applications, services, networks and/or devices through bypassing their underlying security mechanisms.

An information systems security breach must be assessed with reference to *MP 0067/12 Information Security Policy*.

An information system security breach occurs when an individual or an application illegitimately enters a private, confidential or unauthorised information technology perimeter.

An information system security breach may also be caused by any software attempts to subvert the confidentiality, integrity or availability of a system. This may be the result of an external intrusion which must be identified to stop further access and mitigate damage.

Some causes of an information system security breach are:

- information systems being illegally accessed by individuals outside of the agency or organisation
- cyber threats and malware
- unauthorised use of computer network authorised access
- unauthorised changes to computer network access profiles or access control lists
- inadequate data storage, transfer and disposal.

For information systems security breaches, Health Support Services (HSS) need to be notified immediately in accordance with section 5.3.6 of this document.

4.2 Health or Personal information breach

4.2.1 Health Services Act 2016

A clear understanding of the meaning of health information and personal information is vital for stakeholders to be able to recognise if health information has been breached.

4.2.1.1 Health Information

Health information, under section 213 of the *Health Services Act 2016*, is defined as

- personal information, whether collected before, on or after the *Health Services Amendment Act 2023* (section 78) comes into operation, that is information or an opinion about:
    - the health (at any time) of an individual; or
    - a disability (at any time) of an individual; or
    - an individual's expressed wishes about the future provision of health services to the individual; or
- a health service provided, or to be provided to an individual; or
- other personal information collected to provide, or in providing, a health service.

4.2.1.2 Personal Information

The definition of personal information in the *Health Services Act 2016* has the meaning given in the *Freedom of Information Act 1992* which is:
Information or an opinion, whether true of not, and whether recorded in a material form or not, about an individual, whether living or dead:

- whose identity is apparent or can reasonably be ascertained from the information or opinion; or
- who can be identified by reference to an identification number or other identifying, such as a fingerprint, retina print or body sample.

4.2.1.3 Examples of health and personal information breach

Some examples of a health/personal information breach are:

- authorised system users accessing information for unauthorised reasons, such as employees looking up patient information in medical records, computer applications or other databases for personal reasons
- inadvertent disclosure of information due to 'human error', for example a message, email or letter sent to the wrong person or address
- an individual deceiving an employee into releasing the information
- lost or stolen laptops, removable storage devices or paper records
- disclosure of information, as a result of inadequate identity verification procedures
- computer hardware, hard drive and other storage media being disposed without the contents first being erased
- unauthorised publishing of classified information to an uncontrolled environment e.g., internet or social media.

4.2.2 My Health Records Act 2012

My Health Records Act 2012 (MHR Act) health information may be collected, used and disclosed from a healthcare recipient's My Health Record for the purposes of providing healthcare to the recipient, subject to any access controls set by the recipient (or if none are set, default access controls). There are other limited circumstances in which health information may be collected used or disclosed from a My Health Record. Criminal and civil penalties apply if a person collects, uses or discloses information from a My Health Record without authorisation.

4.2.2.1 My Health Records Data Breach

A My Health Records Data Breach occurs if an entity such as the system operator a registered healthcare provider organisation, a registered repository operator, a registered contracted service provider, or any other party becomes aware that:

- a person has or may have contravened the MHR Act in a manner involving an unauthorised collection, use or disclosure of health information included in a healthcare recipient's My Health Record; or
- an event has, or may have, occurred (whether or not involving a contravention of the MHR Act) that compromised, the security or integrity of the My Health Record System; or
- circumstances have, or may have, arisen (whether or not involving a contravention of the MHR Act) that has compromised or may have compromised, the security integrity of the My Health Record system; and
- the contravention, event or circumstances directly involved, may have involved or may involve the entity.

4.2.2.2 Notifying the System Operator

In the event of a data breach involving the MHR Act, the Australian Digital Health Agency, as the system operator must be notified. Notification is done via the link Data breaches Australian Digital Health Agency.

4.2.2.3 Notifying the Office of the Australian Information Commissioner

Suspected data breaches must be assessed using the Office of the Australian Commissioner (OAIC) guide Assessing a suspected data breach to identify eligible data breaches where:

- information was collected under Commonwealth legislation; or
- information within the WA health system is received from an Australian Privacy Principle entity.

Identified eligible breaches must be notified and submitted to the OAIC by completing the online Notifiable Data Breach Form in accordance with the Commissioner's Data Breach Preparation and Response Guide.

4.3 Corporate, financial or workforce information breach

Some examples of a corporate, financial or workforce information breach are:

- unauthorised access or use of documents in an electronic document and records management systems (EDRMS/TRIM)
- unauthorised access to or disclosure of bank account or payslip details
- a person disclosing employee contact details such as mobile phone number or home address
- unauthorised publishing of budget related information
- unauthorised disclosure of employee professional development documentation or assessment results.

4.4 Environmental or physical breach

An environmental or physical breach may occur from an uncontrollable/unexpected event or when information management facilities that record and produce confidential and sensitive information (including patient information) are not located in a safe, secure environment that provides appropriate operating conditions. For example:

- location not adequately secure
- visibility of information
- fire
- weather events
- water damage due to plant failure
- biological agents and chemical spills
- power outages
- inadequate decommissioning of site
- inadequate transportation method
- lost medical records.

5 Information Breach Response

Information breaches should be dealt with on a case-by-case basis by undertaking an assessment of the risks involved and deciding on the appropriate course of action.

The key focus of the information breach response is to minimise the impact and prevent future incidents. There are four key stages[a] to follow when responding to a breach or suspected breach. These include:

1. Contain the breach to minimise 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.

5.1 Contain the information breach

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 or further compromise of the information. For example:

- limit distribution of the affected information
- prevent any further compromise of the information:
  - suspend the activity that led to the breach
  - shut down the system that has been breached
  - revoke or change access codes
  - reset passwords
  - remove/relocate the information asset
  - recover the information.

Containing the information breach may require engagement with several areas. It is important to contact the HSS on 13 44 77 prior to commencing an investigation into data or systems

[a] Based on the Office of the Australian Information Commissioner's 2019 Data Breach Response Plan.

misuse. In cases of a suspected breach of discipline or the Code of Conduct, advice must be sought from the relevant WA health entity's responsible area prior to commencing an investigation.

5.1.1 Information Breach Notification Form

The person who discovers the breach must collect information about the breach, preserve any evidence, and record the details in the Information Breach Notification Form 'Part 1 Information Breach Report'. They must immediately notify their line manager and follow local policies and procedures. The Information Custodian, Assessor and other relevant bodies/persons must be informed as outlined in Section 5.3 Notify.

The Information Breach Notification Form must be commenced at the time of discovery of an actual or suspected information breach. Documenting the details of the data breach on the Information Breach Notification Form will facilitate the assessment, review and development of preventative actions.

Annexure A – Information Breach Notification Form provides guidance on completing each section of the form. The form aligns with the four stages of the Information Breach Response.

5.2 Assess the information breach

An assessment of the breach must be undertaken by an appropriate assessor. Multiple assessors can be involved, depending on the circumstances and the type of breach. An assessor may be the Information Custodian, a manager or other person deemed appropriate and impartial.

The assessor/s must complete the Information Breach Notification Form Part 2 Information Breach Assessment and Resolution'. This section records the details of the assessment, review and risk management of the breach response.

In cases of a suspected breach of discipline or code of conduct breach, advice must be sought from the relevant WA health entity's responsible area prior to interviewing any employees. This will be the Integrity Unit, Human Resource/Workforce Unit, or other responsible area as defined in local policies and/or procedures.

The assessor is required to:

- undertake an assessment of the information breach to determine the extent of the damage and harm caused
- determine if breach of discipline or code of conduct breach may have contributed to the information breach and must undertake the relevant reporting in accordance with MP 0124/19 Code of Conduct Policy
- determine other notification and communication requirements as outlined in Section 5.3 Notify
- assess the risk and initiate actions to prevent recurrence
- 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.

The assessment stage is a broad scope evaluation to assess the circumstances of the breach and remediate the risk of harm.

5.2.1 Details of the breach

The assessment must consider:

- The type and sensitivity of information involved. E.g., health or personal information, or a combination of types of information.
- Who is affected by the breach? E.g., employees, patients, general public, other agency or third party.
- The extent of the breach, who and how many are affected. A large volume of data may still present a risk to some specific individuals. A small volume of data may enable easy identification of individuals/entities.
- The mode of the breach. E.g., leakage, loss, unauthorised use.
- When, where, how and by whom the data breach was discovered.
- Who obtained the information and are they likely to cause harm? Unintentional receipt of information may result in less harm compared to unauthorised obtaining of specific personal information intended for malicious purposes.
- How was or could the information be used to cause harm.
- Requirement for communication strategies to manage public/media interest.
- Was the information protected by security or technology measures? Consider; access restrictions that were bypassed, user activity identification logs, and data encryption that could be overcome.
- How long has the information been accessible? The length of time between occurrence and discovery may increase the potential for misuse and increase the risk of harm.
- Is there a risk of further access, use or disclosure, including via media or online?
- Is this a recurring system/process problem?

5.2.2 The 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 or negligence?
- If it was human error, what were the underlying circumstances or reason for the human error?
- Was it due to a system failure or procedural breach?
- Was it a one-off incident or does it expose an ongoing risk?

5.2.3 Impact assessment

The impact of the breach depends on the nature and extent of the breach, who is affected by the breach, and the type of information that has been compromised. The assessor needs to determine the extent of the breach and potential current, and future harm to affected individuals, and the WA health entity.

Extent

- Quantify how much data/number of records were breached?
- How long did the breach go undetected?
- How long has the information been accessible and has it been recovered?

Harm to individuals

- Identity theft
- Threats to personal safety
- Damage to reputation or relationships
- Loss of business or employment opportunities
- Workplace or social bullying or marginalisation
- Financial loss or other interests.

Harm to WA health entity

- Impact on the entity's capacity to provide services
- Loss of reputation and public trust in the agency or program
- Financial loss
- Publishing of sensitive business information
- Loss of assets, for example, stolen computers or storage devices
- Regulatory penalties or legal liability to any third party.

5.3 Notify

Subject to the circumstances of the information breach, there are various notifications and communications that must be undertaken. The following positions and groups must be taken into account for notification:

5.3.1 Information Asset Custodian

The information asset custodian is responsible for the management of a data collection or information, as outlined in the Information Management Governance Model. The custodian must have an oversight of breaches related to their information asset to ensure their risk and mitigation strategies are continually reviewed and updated. To identify the relevant custodian, refer to the WA health system Information Register. The register includes the information asset name, description and officer with the delegated responsibility for the information asset.

5.3.2 Information Steward

The information steward provides strategic guidance and executive level support where the information breach involves an information asset under their stewardship.

The steward's role regarding information breaches is to:

- ensure that the information breach policy is supported and implemented
- support the participation to the information management communications and education programs relating to information breaches
- review and manage all risks and issues that arise as a result of an information breach
- escalate information breaches to the Information Management Governance Advisory Group as required.

5.3.3 Information Sponsor

The information sponsor is allocated functions to assist the steward in managing the information assets.

The sponsor's role regarding information breaches is to:

- support the steward in implementing the information breach policy, processes and procedures
- support the custodians on the management of information management practices including access, use and disclosure issues resulting from information breaches
- support information sharing that promotes the access, use and disclosure of information when it is permitted or required by law to resolve information breaches
- review and manage all risks and issues that arise as a result of information breaches
- escalate information breach issues to the steward as required.

5.3.4 Breach of Discipline or Code of Conduct

The Code of Conduct outlines the standards of behaviour expected of employees. It requires that employees maintain the confidentiality of any personal or other information that becomes available to them in the course of their employment and to only use the information in connection with their role.

An employee accessing, using or disclosing confidential and/or sensitive information must ensure it is protected from misuse, interference, loss, unauthorised access or modification.

Information breaches involving an employee, which may be a breach of discipline or the Code of Conduct, must be reported to the relevant WA health entity's responsible area. This will be the Integrity Unit, Human Resource/Workforce Unit, or other responsible area as defined in local policies and/or procedures.

The relevant WA health entity's responsible area will ensure the Director General and Health Service Chief Executives statutory obligations to notify oversight agencies of suspected misconduct are met. Additionally, the relevant WA health entity's responsible area will undertake the reporting to the police or law enforcement agencies.

Compliance with *MP 0124/19 Code of Conduct Policy* includes ensuring information remains secure while in transit and is retained and disposed of in accordance with MP 0067/17 Information Security Policy in the Information Communications Technology Policy Framework and the relevant policies in the Information Management Policy Framework.

Mandatory policies related to conduct and integrity include:

- MP 0124/19 Code of Conduct Policy (applicable to all WA health entities)
- MP 0127/20 *Discipline Policy* (applicable to Health Service Providers only)
- MP 0125/19 *Notifiable and Reportable Conduct Policy* (applicable to Health Service Providers only)
- Department of Health Discipline Policy (applicable to Department of Health employees).

5.3.5 State Records

When information managed in accordance with the *State Records Act 2000* is breached then the State Records Office must be notified at sro@sro.wa.gov.au. The State Records Office will in turn notify the State Records Commission. The Commission will determine if the information breach and related actions require further investigations.

5.3.6 Health Support Services

The HSS Security and Risk Management Unit is responsible for managing cyber security and strengthening cyber resilience of WA health entities. HSS must be notified immediately regarding information systems security breaches via the following:

- To report information system breaches, the HSS Security and Risk Management team can be contacted via infosec@health.wa.gov.au
- To report a suspicious email/text or phone call, email scam@health.wa.gov.au. Refer to section 4.1 Information systems security
- The HSS ICT Help Desk can be contacted on 13 44 77.

HSS, in undertaking their IT support functions, is also required to notify the relevant WA health entity of any suspected information breaches and assist when applicable.

Additional information and resources regarding the information and systems security breaches can be found on the Security & Risk Management Services share point page.

5.3.7 Affected individuals

Consideration also needs to be given on whether notification is provided to any affected individuals. In some cases, if there is a high risk of serious harm to individuals, it may be appropriate to notify them immediately. The assessor, in conjunction with the other relevant stakeholders, must assess whether to notify individuals and if so:

- who should be notified?
- when and how the notification should occur?
- who should make the notification?
- what information should be included in the notification?

Circumstances where it may be appropriate to delay notification include where notification would compromise an investigation into the cause of the breach and when it is suspected there may have been a breach of discipline or code of conduct.

5.3.8 Internal and External Communications

The Department of Health Communications Unit or the relevant WA health entity communication units will assist in communicating details of the information breach within or external to the WA health system. This includes the media and external stakeholders. The aim of the communication is to limit the extent of harm to the affected individuals and key stakeholders. Clear communication to the staff and public will also demonstrate accountability and transparency and reduce the impact of the information breach. Communication examples include:

- Global messages
- WA health entity wide emails

- Media releases
- Personalised emails.

5.3.9 Human Research & Ethics Committee

If the information breach pertains to a research project that was approved by a WA health entity Human Research Ethics Committee and Research Governance Office, the applicable committee must be notified and included in the assessment and resolution process.

5.3.10 Legal and Legislative Services

For legal advice contact Legal and Legislative Services via Legal.services@health.wa.gov.au, or the relevant General Counsel (where applicable).

5.3.11 Other agencies or organisations affected by the breach

Parties under the terms of an agreement, memorandum of understanding (MOU) or contract must be notified if there is a breach of their information or data by a WA health entity. Information breaches involving external organisations data will carry additional reporting requirements, for example the Office of the Australian Information Commissioner.

5.3.12 Department of Health - Information & Performance Governance

The Information Breach Notification Form is sent to the Department of Health, Information and Performance Governance (IPG) Unit who maintain a central register of information breaches. This Unit can also be consulted for advice. Any information breaches that the assessor deems serious must be notified immediately to IPG for policy and compliance advice via RoyalSt.PSPInfoManagement@health.wa.gov.au.

IPG reports information breaches to the Information Management Governance Advisory Group (IMGAG). IMGAG reviews the breaches to ensure lessons learnt are identified and actions taken to reduce the likelihood of future breaches.

5.3.13 Commonwealth data

There may be information held by WA health entities that is collected under Commonwealth legislation. Any breach involving Commonwealth data must be reported in accordance with the relevant legislative requirements. For example, an information breach may trigger legislative reporting obligations to the Commonwealth Privacy Commissioner.

Critical ICT infrastructure breaches are required to be reported to the Australian Signals Directorate (ASD). These types of IT security breaches should immediately be reported to HSS in accordance with section 5.3.6 to ensure the ASD are notified.

5.4 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 investigations are required including:
  - implementing processes to assist individuals who have been affected by the breach

- conducting interviews, or further interviews, with employees involved and/or affected (note that in cases of a suspected breach of disciplined or Code of Conduct, advice must be sought from the relevant WA health entities responsible area prior to undertaking any interviews)
- conducting further investigation by appropriate HSS employee into system failures or ICT security issues
- informing applicable persons/bodies of the outcomes and recommendations of the assessment
- reviewing communication strategies to manage ongoing public/media interest.

- assess the risk
- prevent recurrence.

5.4.1 Risk Assessment

Health Service Providers and the Department of Health are responsible for ensuring that risks to their organisation are identified and managed effectively and in accordance with the requirements of the MP 0006/16 Risk Management Policy. The future likelihood of harm occurring and anticipated consequences for individuals and the WA health system must be verified.

The assessor must consider all the information gathered during the assessment stage and refer to the Risk Assessment Tables for the WA health system to determine the level of risk. The following factors must be considered:

- the type of information involved
- the context of the affected information and breach
- how did the breach occur? E.g., source/cause
- effectiveness of the controls in mitigating the information breach e.g. policy, procedures, restricted access, monitoring, security
- the extent of the breach e.g. how many/how long?
- is there a risk of further exposure of the information?
- the risk of serious harm to the affected individuals and the risk of other harms e.g. what harm occurred or may occur in the future as a result of the breach
- what is the likelihood of recurrence?

As a result of the risk assessment it may be necessary to register the risk as directed by local risk management policy and processes.

5.4.2 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 and employee training must be undertaken where deemed appropriate.

If appropriate, a debrief must be held with relevant employees to assess the response to the breach and to ensure any necessary recommendations are allocated and actioned appropriately.

A treatment/prevention action plan could include:

- a security audit of both physical and technical security
- a review of employee induction and mandatory training requirements
- a review and revision of policies, processes and procedures to address the lessons learned from the investigation
- education and training:
  - responsibilities under the MP 0124/19 Code of Conduct Policy
  - how to respond to information breaches effectively
  - information management.

At the completion of the information breach response the completed Information Breach Notification Form must be emailed to the Information and Performance Governance Unit (via: RoyalSt.PSPInfoManagement@health.wa.gov.au). The form will be retained, and details recorded in the WA health system Information Breach Notification Registry.

5.5 Expected response time

Ideally, reasonable steps should be taken to complete the assessment within 30 calendar days of identification of the breach. It is acknowledged that the expected response times will vary, depending on the type and extent of the breach. However, the response time needs to be managed to ensure the information breach is effectively contained and managed appropriately, and within reasonable time frames.

6 Roles and Responsibilities

The roles and responsibilities of key stakeholders in the information breach process is subject to the circumstances of each information breach. For any information breach process undertaken it is expected that stakeholders will work collaboratively when required to appropriately respond to and manage the breach.

6.1 Delegated authorities

The Department CEO or a Health Service Provider may delegate any of their statutory functions in accordance with the *Health Services Act 2016* and any other written laws. This includes the delegations of information management functions and powers. To identify the relevant delegated authority, please refer to the relevant Instrument of Authorisations and Delegations for the WA health entity.

6.2 Information Asset Custodians

The Information Asset Custodian has a number of responsibilities as outlined in the Information Management Governance Model. One such responsibility focuses on risk management – where the custodian must maintain a work plan for the asset highlighting risk and mitigation strategies.

Information assets from across the WA health system are collectively listed in the WA health system information register. This register includes the information asset name, description and the relevant steward and custodian.

6.3 Department of Health

The Department of Health's Information and Policy Governance Unit are responsible for the Information Management Policy Framework. The framework specifies the information management requirements that all Health Service Providers and Department of Health

divisions must comply with to ensure effective and consistent management of health, personal and business information across the WA health system. Functions include:

- providing advice on management of an information breach
- reviewing breach notifications to ensure all response and notification requirements are completed
- providing feedback/request further information on reported information breaches
- maintaining the Information Breach Register
- tabling all information breaches at the WA Health Information Management Governance Advisory Group (IMGAG)
- conducting an annual review of reported breaches and tabling the review report at IMGAG and provided to key stakeholders to review and facilitate the sharing of lessons learnt
- providing education and training resources.

7 Record Keeping

Adequate documentation must be kept in accordance with WA health entity's record keeping plans. The documentation must record all decisions made so that decisions are transparent and capable of review, including the rationale for the decision that reflects the assessment of the level of risk and seriousness of the matter.

Once an information breach response is completed any related documentation must be kept by the assessor and any appropriate stakeholders in accordance with the General Disposal Authority produced by the Western Australian State Records Office: General Disposal Authority for State Government Information GDA 2013-017 and the relevant WA health entity's record keeping plan.

The Department of Health's Information and Performance Governance Unit ensures that all Information Breach Notifications are stored and managed on the Electronic Document Records Management System (TRIM).

Any information breach documentation relating to the investigation must also be maintained in accordance with the relevant policies in the Information Management Policy Framework.

8 Definitions

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

Term	Description
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.
Australian Privacy Principle Entity	Has the meaning given in section 6 of the *Privacy Act 1988* as an agency or organisation (note that agency and organisation are defined in section 6(1) of the Act.

Term	Description
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.
Information Breach	An information breach refers to an incident in which personal or confidential information, or non-personal information that could be sensitive or commercial is compromised. The Information may be subject to unauthorised access, use or disclosure, or is lost, damaged or destroyed.
Information Custodian	The person(s) responsible for the day-to-day management of a data collection or information. An Information Asset Custodian is a subset of Information Custodians.
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.
System Operator	Has the meaning given by section 14 of the *Medical Record Act 2012* as the Secretary of the Department; or if a body established by a law of the Commonwealth is prescribed by the regulations to be the System Operator—that body.
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.

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