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

Information Breach Process Guide

health.wa.gov.au

Owner:	Department of Health, Western Australia
Contact:	Anthony Jones
Approved by:	Angela Kelly
Approval Date:	5 May 2020
Current Version:	1.0
Links to:	Information Management Policy Framework

VERSION	DATE	AUTHOR	COMMENTS
1.0	5 May 2020	Anthony Jones	Approved by the Assistant Director General, Purchasing and System Performance.

Contents

Acronyms

CE	Chief Executive
DG	Director General
HSP	Health Service Provider
WA	Western Australia

1 Purpose

The Information Breach Process Guide is a supporting document in the *Information Breach Policy*. The purpose of the guide is to assist stakeholders to comply with the mandated requirements in the *Information Breach Policy*. The guide is not mandatory.

For ease of reference and to assist stakeholders understand the mandatory and non-mandatory requirements, this Guide refers to the appropriate sections in the *Health Services Act 2016* and other relevant policies.

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 imperative that information is valued, available, shared, governed, trustworthy, secure and protected to support the vision of the WA health system. It is also imperative that information is not misused and inappropriately accessed, used, disclosure and/or lost.

Information breaches can cause significant harm to the individuals whose information is compromised. Further, information breaches can negatively impact an entity's reputation. A quick response can reduce the likelihood of affected individuals suffering harm. It can also lessen the impact of an ongoing breach of an information asset, or the financial or reputational damage to the entity that results from the breach. An Information Breach Policy Education Module has been developed to support the *Information Breach Policy*.

3 Information

Information may be, but is not limited to:

- information assets across the WA health system (refer to the WA health system Information Register and the Instrument of Delegation – Health Information which is issued in accordance with section 24 of the *Health Services Act 2016*)
- patient health and personal information
- business/ corporate information
- email and other correspondence
- digital files and systems, printed materials, video or sound recordings
- biological samples, physical samples or images
- statistics and graphs
- reports and briefing notes.

4 Types of 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. 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.

There are many different types of information breaches. Common information breaches typically related to:

- Information security

- Health information
- Corporate, financial or workforce information
- Environmental or physical.

4.1 Information security breach

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

An information security breach occurs when an individual or an application illegitimately enters a private, confidential or unauthorised information technology perimeter. An information 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 external intrusion. The method of intrusion needs to be identified to stop further access and mitigate damage to servers.

Some causes of an information security breach are:
- databases containing personal information being illegally accessed by individuals outside of the agency or organisation
- abuse of privileges in a network environment
- unauthorised changes to network profiles or access control lists.

4.2 Health information breach

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.

Health information, under section 213 in the *Health Services Act 2016*, is defined 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.

Personal information has the meaning given in the *Freedom of Information Act 1992* in the Glossary clause 1 which is 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.

A breach of health information is considered to be an incident whereby information has potentially been viewed, shared, stolen, removed, destroyed or used by an individual unauthorised to do so.

A health information breach occurs when there is unauthorised access, use or disclosure of health information, whether intentional or unintentional. Some causes of a health information breach are:
- improper handling of classified information

- an agency or organisation inadvertently providing health information to the wrong person, for example, sending details out to the wrong address
- an individual deceiving staff into improperly releasing the health information of another person
- lost or stolen laptops, removable storage devices or paper records containing health information
- 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
- unauthorised access to records or electronic databases
- unauthorised disclosure of information that has the potential to cause an adverse event
- any unforeseen event that has or may affect the ethical acceptability of the use of the personal health information provided.

4.3 Corporate, financial or medical workforce information breach

Corporate, financial or workforce information breach occurs when there is unauthorised access, use or disclosure of information, whether intentional or unintentional. Some causes of corporate, financial or medical workforce information breach are:

- unauthorised access to human resource systems
- improper handling of staff bank account details or payslip details
- a person inadvertently disclosing staff contact details such as mobile phone number or home address
- unauthorised publishing of budget related information
- unauthorised disclosure of staff professional development documentation or assessment results.

4.4 Environmental breach

An environmental breach or physical breach may occur 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. Some causes of environmental information breaches could include:

- fire
- storms and floods
- biological agents and chemical spills
- power outages.

5 Information Breach Notification Form

The Information Breach Notification Form is a related document in the *Information Breach Policy*. The completion of the form is a mandated requirement in the Policy and should be submitted to the staff member's line manager, the relevant Integrity Unit, and/or the Information Custodian. The form should be completed by staff in all instances of an information breach or suspected information breach.

The Information Breach Form comprises four parts including:

- Part 1: Reporter Details
- Part 2: Information Breach Details
- Part 3: Assessor Details
- Part 4: Assessment Details

Parts 1 and 2 are to be completed immediately, by the person who discovers or suspects the breach. Part 1 of the form captures the details of the staff member reporting the breach incident and Part 2 the information breach details. Key information breach details captured in Part 2 include:

- the date, time, duration and location of the breach
- information classification of the breached information (refer to the *Information Classification Policy*)
- how the breach was discovered or why it is suspected
- description of the breach
- the suspected or known cause of the breach.

Parts 3 and 4 of the form needs to be completed by the individual undertaking the assessment of the breach. This individual could be the custodian or the manager or any other individual deemed appropriate. If the manager is the suspected cause of the breach, the information custodian or another individual should undertake the assessment. Part 3 of the form captures the assessor details and Part 4 the assessment details.

A key part of the assessment is the completion of a breach assessment summary and actions taken. Key information that should be considered as part of the assessment in Part 4 includes:

- details of who is affected by the information breach and the estimated number of individuals affected
- a description of the immediate actions taken to contain the breach
- details of anyone notified of the incident and, how and when they were notified. This should include if impacted individuals have been notified (when appropriate).
- whether any evidence has been preserved
- if any further investigation is considered necessary
- if any steps have been taken to prevent the information breach from occurring again
- an impact severity rating assessment (refer to Appendix 1 for further details). Note that severity rating in Appendix 1 is not mandated and WA health system entities may use severity ratings that are established and fit for purpose for their specific entity.

6 Information breach response

Information breaches should be dealt with on a case-by-case basis by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action. Information security methods should be commensurate with the sensitivity of the information and any disciplinary action commensurate with the seriousness of the breach. There are four key steps to consider when responding to a breach or suspected breach. These steps[a] include:

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

The key focus of the information breach response is to minimise the impact and prevent future incidents. An example of an Information Breach Resolution Process is provided in Appendix 2.

[a] Based on the Office of the Australian Information Commissioner's 2018 Data Breach Response Plan.

6.1 Contain the information breach

In the event of a breach the person who discovers the breach should immediately initiate a process of containment by taking whatever steps possible to immediately contain the breach. For example:

- stop the unauthorised practice
- recover any records
- shut down the system that was breached. If it is not practical to shut down the system, then revoke or change the account privileges or block access from the unauthorised person.

It is important that the individual who discovers the breach collects information about the breach promptly and captures the appropriate details so that it can be included in Parts 1 and 2 of the Information Breach Notification Form. This information will also assist the individual to undertake the initial Information Breach Impact Severity Rating Assessment. The assessment is recorded in Part 4 of the Information Breach Notification Form.

The relevant Integrity Unit, and the Information Custodian and/or the appropriate assessor should also be notified immediately of the breach. The person who discovered the breach should also provide the completed Parts 1 and 2 of the Information Breach Notification Form to these stakeholders.

6.2 Assess the information breach

An assessment of the breach needs to be undertaken by an appropriate assessor. The appropriate assessor will depend on the circumstances and the type of breach. In the first instance the staff member's line manager should be considered as an assessor. This may not, however, be appropriate if the line manager does not have the subject matter expertise to undertake the breach assessment or is not an impartial stakeholder. Typically, the appropriate assessor would be the Information Custodian, a Manager and/or a subject matter expert.

It is the assessor's role to undertake an assessment of the breach. A part of the breach assessment is the review and evaluation of risks to individuals and the WA health system. To determine the severity of the information breach the assessor should use the Information Breach Impact Severity Rating in Appendix 1.

The assessor needs to determine the risk of harm to the affected individuals and determine the risk of harm to the WA health system. Some examples of possible harm to the WA health system include:

- the loss of public trust in the agency or particular program
- the loss of assets, for example, stolen computers or storage devices
- financial exposure, for example, if bank account details are compromised
- regulatory penalties or legal liability to any third party.

After completing the Information Breach Incident Notification Form it is important for the assessor to determine if further investigation into the information breach is required and the appropriate documentation that will be required when applicable.

Further actions may include interviews (or further interviews) with staff involved and/or affected, or the request of further investigation by appropriate Health Support Service (HSS) staff into system failures or ICT security issues.

To assess the risks, the following factors should be considered:

- the type of information involved e.g. Medicare numbers, health information, phone numbers and who are affected by the breach
- the context of the affected information and breach e.g. how was the information used
- the cause and extent of the breach e.g. what was the source of the breach? Is there a risk of further exposure of the information? Is this a recurring problem of the system?
- the risk of serious harm to the affected individuals and the risk of other harms e.g. what harm occurred as a result of the breach, such as, financial loss or threat to physical health.

6.3 Take action to remediate any risks of further harm

The assessor should consider the particular circumstances of each breach and determine, using the Information Breach Impact Severity Ratings the level of notification required (refer to Appendix 1).

Consideration also needs to be given on whether notification is provided to any affected individuals. In some cases, if there is a high level risk of serious harm to individuals, it may be appropriate to notify them immediately.

The assessor, in conjunction with the other relevant stakeholders, should assess:

- whether or not to notify individuals and if so:
    - when and how the notification should occur
    - who should make the notification
    - who should be notified
- what information should be included in the notification
- who else should be notified such as:
    - the police/law enforcement
    - the Corruption and Crime Commission (CCC)
    - other agencies or organisations affected by the breach
    - parties under the terms of an agreement, Memorandum of Understanding (MOU) or contract.

If there has been an intentional or suspected information breach by a staff member in the WA health system, the Director General and the Health Service Provider Chief Executives have a statutory obligation to report all incidents of suspected misconduct to the CCC. It is important that staff should report incidents of suspected misconduct as soon as practicable to the Information Custodian, the relevant integrity unit or appropriate authority.

6.4 Review the incident and take preventative actions

It is important that the cause of the breach has been fully investigated and the outcomes and recommendations are provided to the appropriate authorities.

At a minimum, amendments to policies, processes and procedures should be made where necessary and staff training should be undertaken where deemed appropriate. A debriefing session should be held with relevant staff to assess the response to the breach and to ensure any necessary recommendations are allocated and actioned appropriately.

The significance of the breach should be reviewed as to whether it was an isolated event or a recurring breach.

A prevention plan could include:

- a security audit of both physical and technical security

- a review of employee selection and training practices
- a review of policies, processes and procedures to reflect the lessons learned from the investigation
- staff training in responding to information breaches effectively.

The competed Information Breach Notification Form is required to be emailed to the Information Governance and Performance Unit (via: RoyalSt.PSPInfoManagement@health.wa.gov.au). The form will be retained and included into an Information Breach Notification Registry.

6.5 Expected response time

The specific activities and the expected response times will vary, depending on the incident type and the severity rating of the incident.

The response time needs to be managed to ensure the information breach contained and managed appropriately and within reasonable time frames.

7 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 manage the prevention, containment, remediation and investigation of information breaches.

7.1 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, stakeholders should refer to the relevant Department of Health Instrument of Delegation (WA Health employees only) or the relevant Health Service Provider Authorisation and Delegations.

An example is section 217 of the *Health Services Act 2016.* This section allows the Health Service Provider CEO to disclose health information to a person who has sufficient interest in the treatment, care, health, safety or wellbeing of the patient without the requirement for consent subject to compliance with regulation 4 of the *Health Services (Information) Regulations 2017.* In this instance, to identify the delegated authority for section 217 of the Act, stakeholders should refer to the relevant Health Service Provider Authorisations and Delegation Schedule.

7.2 Information custodians

Under section 24 of the *Health Services Act 2016*, the Department CEO may delegate any of their functions including information management functions and powers. These delegations may be to Health Service Providers or staff members within the Department of Health and are documented and authorised through the Instrument of Delegation – Health Information. The Instrument of Delegation lists the approved Delegated Officer and the legislative powers they have been delegated against the WA health system information asset(s) in the WA health system Information Register. The register lists all information assets in the Instrument of Delegation – Health Information. The register includes the information asset name, description and officer with the delegated responsibility for the collection. To identify the relevant custodian,

stakeholders should refer to the Instrument of Delegation – Health Information and the WA health system Information Register.

8 Other relevant policies

Once an information breach has been investigated, any related documentation should 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*.

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

The *Code of Conduct Policy* 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 position. An employee accessing, using or disclosing confidential and/or sensitive information should ensure it is protected from misuse, interference, loss, unauthorised access or modification.

The *Code of Conduct Policy* identifies the fundamental values, and translates these values into principles that guide conduct in the workplace. It defines the standards of ethical and professional conduct and outlines the behaviours expected across the WA health system. Mandatory policies related to conduct, ethics and integrity include:

- MP 0124/19 *Code of Conduct Policy*
- 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)

In addition to the mandated requirements in the *Information Breach Policy*, it is important that any potential misconduct is also reported in accordance with the *Code of Conduct Policy*. This would include an information breach that relates to a breach in the code of conduct.

Compliance with the *Code of Conduct Policy* includes ensuring that information remains secure while in transit. Refer to the *Information Security Policy* found within the *Information Communications Technology Policy Framework* and the *Information Storage and Disposal Policy* in the *Information Management Policy Framework* for more information.

9 Definitions

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

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.
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.

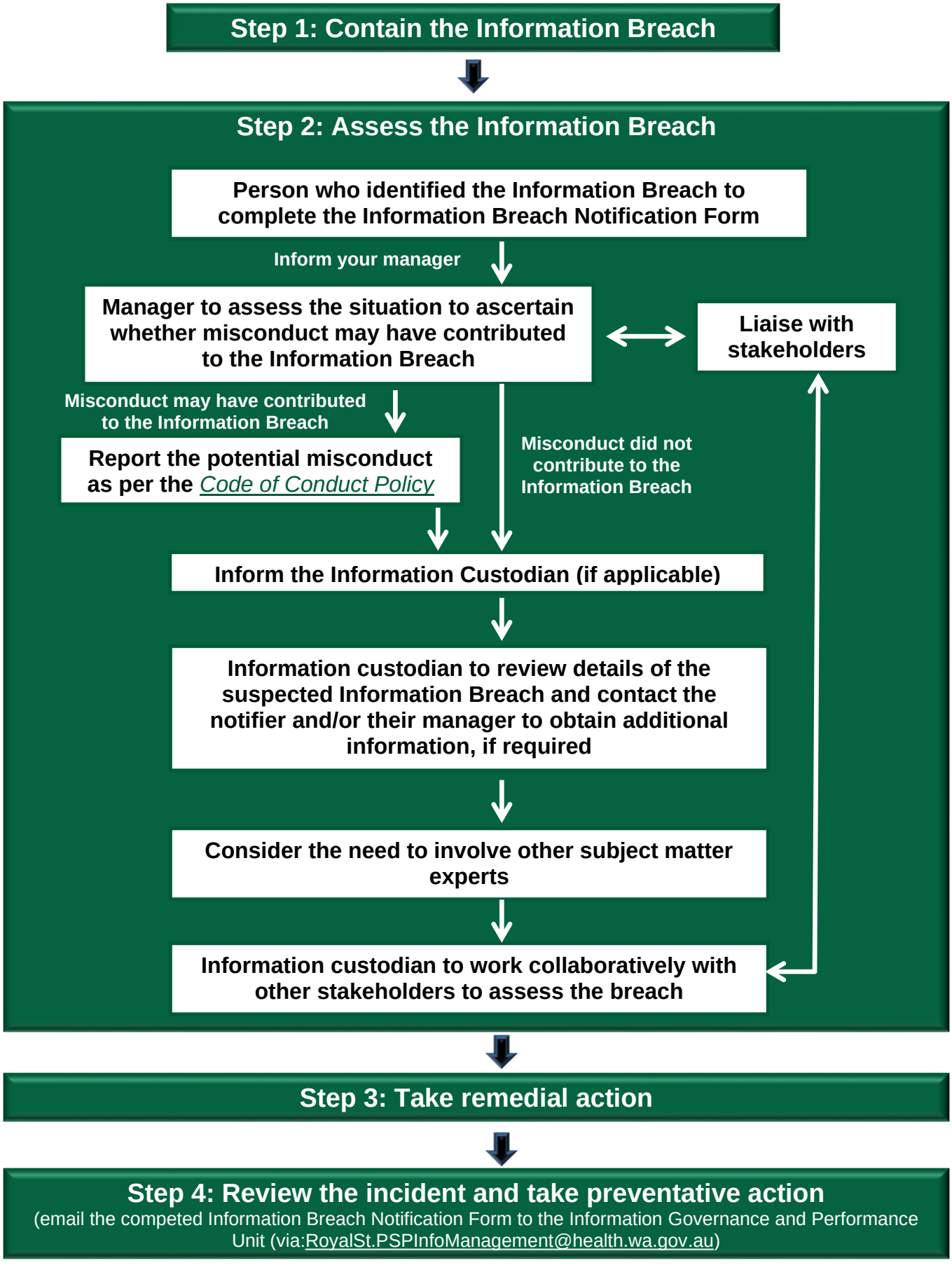
Term	Description
disclosure	A person discloses information if they cause the information to appear, allow the information to be seen, make the information known, reveal the information or lay the information open to view.
health information	Has the meaning given in the *Health Services Act 2016* in section 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, 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.

Appendix 1: Information Breach Impact Severity Ratings

INFORMATION BREACH IMPACT SEVERITY RATINGS					
Impact Type	**Severity** **Lowest** ← → **Highest**				
Impact Severity	**1. NEGLIGIBLE**	**2. LOW**	**3. MEDIUM**	**4. HIGH**	**5. VERY HIGH**
Risk to individual safety due to unauthorised access or disclosure of classified information	No injury/minimal risk to personal safety	Single injury/low risk to personal safety of client/employee	Multiple injuries/moderate risk to safety of client/employee	Death/disabling injury/high risk to safety of client/employee	Multiple deaths or disabling injuries/very high risk to safety of client/employee
Distress caused to any party or damage to any party's standing or reputation	Negligible, no public concern – only routine internal reporting	Minor distress, minor damage – visible limited/localised media interest, internal reporting	Substantial short term distress – restricted negative publicity from local media, internal inquiry	Substantial long term distress – main stream media report, internal inquiry	Substantial long term distress to multiple parties – broad public concern and media coverage, Parliamentary inquiry or Royal Commission
Non-compliance – unauthorised release of information classified as protected or confidential, to a third party	Minor compliance issues – no or negligible impact, offence punishable by small fine	Short to medium term action required – minor impact, offense punishable by moderate fine	Immediate action needed to achieve compliance – measurable impact, offense punishable by major fine	Shutdown of service for non-compliance – significant impact, offence punishable by imprisonment	Shutdown of multiple services for non-compliance – major consequences to a person or agency
Threat to WA Health's capacity to deliver services due to Information Security breach	No or negligible threat to, or disruption of business or systems or service delivery	Minimal threat to, or disruption of localised business or systems or service delivery	Moderate threat to or cessation of a service for a week, and subsequent disruption	Multiple essential/critical services impaired, or disrupted over a month	Cessation of multiple essential/critical services for several months

INFORMATION BREACH IMPACT SEVERITY RATINGS (Continued)					
Impact Type	**Severity** **Lowest** ← → **Highest**				
Impact Severity	**1. NEGLIGIBLE**	**2. LOW**	**3. MEDIUM**	**4. HIGH**	**5. VERY HIGH**
Impact on Government finances, economic or commercial interests	No or negligible impact – consequences resolved by routine operations	Minor impact on finances, economic or commercial interests	Moderate impact – disadvantage caused to the government in commercial or policy negotiations	Substantial – damage to finances, economic or commercial interests	Substantial – damage to finances, economic or commercial interests
Impact on development or operation of major government policy	No or negligible impact – consequences resolved by routine operations	Minor – impact on efficiency or effectiveness, managed internally	Impede effective development or operation – significant review or changes required	Seriously impede development or operation – project or program may not survive	Substantially impede operation or development
Reporting Recommendation	Submit report to Information Custodian	Submit report to Information Custodian and Information Steward	Submit report to Information Custodian, Information Steward and if appropriate Health Service Provider Chief Executive and the Director General	Submit report to Information Custodian, Information Steward, Director General and the Minister for Health	Submit report to Information Custodian, Information Steward, Director General and the Minister for Health

Appendix 2: Information Breach Resolution Process Example



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