Data Breach Response Policy
TITLE: DATA BREACH RESPONSE POLICY

1. BACKGROUND

The term ‘data’ generally refers to unprocessed information, 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. For the purposes of this document, the terms ‘data’ and ‘information’ have been used interchangeably and should be taken to mean both data and information.

WA Health creates, collects and maintains a vast amount of data, much of which is confidential personal health information. The data collected is used for direct patient care, planning, management and monitoring of health services. It is also used to meet funding and performance reporting obligations and health related research.

Information in WA Health is held in many forms such as medical records, reports, personnel records, paper files, and computerised databases and documents. It may be transmitted in many ways including by hand, by courier, or electronically using shared communications lines. Information may be transmitted through systems controlled by WA Health or systems controlled by external parties. The principles underlying the need for information security applies to all information irrespective of the media on which it is held.

A data breach is 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.

In the event that WA Health experiences a data breach, or suspects that a data breach has occurred, it is important that procedures are in place to enable WA Health to contain, assess and respond in a timely manner. This will help minimise potential damage to individuals and the organisation.

2. SCOPE

This policy applies to all persons employed in WA Health (including contractors, students, volunteers and agency personnel) incorporating the following entities:

- Department of Health
- Metropolitan Health Service
- WA Country Health Service.

This policy also applies to external organisations and their personnel who have been granted access to WA Health Information and Communication Technology (ICT) infrastructure, services and data.

The scope of the policy includes WA Health data held in any format or medium (paper-based or electronic) that has been assigned a classification of protected (internal use) or
confidential. The policy does not apply to information that has been classified as Public (refer to Information Classification Policy OD 0537/14).

The policy covers all record level and aggregate level data collections within WA Health, including those provided for by statute. It includes collections of patient, corporate, financial and workforce information. For the purpose of this policy, a data collection includes both operational data collections and data repositories.

Depending on the type and extent of the data breach, management of public relations may be required, including coordinating the timing, content and method of public announcements and similar activities. These activities are outside the scope of this policy, which is limited to the immediate internal responses of business units.

3. POLICY

This policy sets out mandatory procedures that staff must apply in the event that WA Health experiences a data breach or suspects that a data breach has occurred.

WA Health policies that should be read in conjunction with this policy are:
- Information Security Policy (OD 0389/12)
- Information Access and Disclosure Policy (OD 0539/14)
- Information Classification Policy (OD 0537/14)
- Practice Code for the Use of Personal Health Information (IC 0177/14).

4. TYPES OF DATA BREACHES

A data breach is an incident, in which information is compromised, disclosed, copied, transmitted, accessed, removed, destroyed, stolen or used by unauthorised individuals, whether accidentally or intentionally.

4.1 Information Security Breach

An information security breach is any incident that results in unauthorised access of data, 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 and 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 Personal Health Information Breach

A breach of personal 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 personal health information breach occurs when there is unauthorised access or disclosure of WA Health information, whether intentional or unintentional. Some causes of a personal health information breach are:

- improper handling of classified WA Health information
- an agency or organisation inadvertently providing personal information to the wrong person, for example, sending details out to the wrong address
- an individual deceiving WA Health into improperly releasing the personal information of another person
- lost or stolen laptops, removable storage devices or paper records containing personal 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 by WA Health.

4.3 Corporate, Financial or Medical Workforce Information Breach

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

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

5. FORMS FOR REPORTING A DATA BREACH

5.1 Data Breach Incident Reporting Form

A Data Breach Incident Reporting Form (Appendix A) should be completed by WA Health staff in all instances of a data breach or suspected data breach.

The form is comprised of two parts, Part A and B. Part A is to be completed immediately, by the person who discovers or suspects the breach. The following details must be recorded:

- the date, time, duration and location of the breach
- how the breach was discovered or is suspected
- description of the incident and the type of data involved in the breach
- the cause and extent of the breach
- other staff members that either witnessed the event or were notified at the time of the incident
- an initial breach impact severity rating.

The Data Custodian must complete Part B of the Data Breach Incident Reporting Form by providing the following details:

- details of who is affected by the data breach and the estimated number of individuals affected
- a description of the immediate actions taken to contain the breach
- details of anyone else notified of the incident and, if so, how and when they were notified
- whether any evidence has been preserved
- if any further investigation is considered necessary
- if any steps have been taken to prevent the data breach from occurring again.

5.2 Data Breach Impact Severity Ratings Form

The Data Breach Impact Severity Ratings Form (Appendix B) provides a standardised approach for assessing the severity of a data breach and outlines the reporting requirements for data breach notification. Staff are required to make an initial assessment using the Data Breach Impact Severity Ratings Form and to notify relevant staff of the breach in accordance with this form.

The impact severity rating of a data breach can range from negligible to very high. A rating should be considered against each of the categories below:

- risk to individuals’ safety
- distress caused to any party or damage to any party’s standing or reputation
- unauthorised release of personally or commercially sensitive data to third parties
- threat to WA Health or third party systems, or capacity to deliver services
- financial loss to WA Health or liability to a third party
- impact on Government finances, economic/commercial interests
- impact on development or operation of government policy.
6. DATA BREACH RESPONSE

Data breaches must 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. Data security methods must 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.

**STEP 1: Contain the breach and make a preliminary assessment**

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.

The person who discovers the breach must collect information about the breach promptly and the details must be recorded in Part A of the WA Health Data Breach Incident Reporting Form (Appendix A).

They must also make an initial assessment using the Data Breach Impact Severity Ratings Form (Appendix B). The assessment is to be recorded on Part A of the WA Health Data Breach Incident Reporting Form.

The Data Custodian must be notified immediately of the breach and be provided with the Data Breach Incident Reporting Form with Part A completed.

**STEP 2: Evaluate the risk for individuals associated with the breach**

The Data Custodian is responsible for undertaking a risk assessment and evaluating the risks to individuals associated with the breach as well as the risks for WA Health. In undertaking a risk assessment the Data Custodian should use the Data Breach Impact Severity Ratings Form (Appendix B) to determine the impact severity of the data breach.

The Data Custodian will need to determine the risk of harm to the affected individuals and determine the risk of harm to WA Health. Some examples of possible harm to WA Health 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 Data Breach Incident Reporting Form the Data Custodian must decide whether further investigation into the data breach is required and document how this will be undertaken, where applicable.

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

To assess the risks, the following factors should be considered:
- the type of personal 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.

**STEP 3: Consider breach notification**

The Data Custodian must consider the particular circumstances of each breach and determine, using the Data Breach Impact Severity Ratings Form ([Appendix B](#)), the level of notification within WA Health.

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 Data Custodian, in conjunction with the Data Steward, should assess:
- whether or not to notify individuals and if so when and how the notification should occur, who should make the notification, and 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.

The Data Custodian is responsible for preparing a briefing note and a report for consideration, to the required person(s), as stipulated in the Data Breach Severity Ratings Form. The report should provide a recommendation of either no further action necessary or provide details to any further action(s) and the reasoning for the recommendations.

If there has been an intentional or suspected data breach by a member of WA Health staff, the Director General has a statutory obligation to report all incidents of suspected misconduct to the CCC. All staff should report incidents of suspected misconduct as soon as practicable to the Data Custodian. These instances must also be escalated, as
appropriate to the Data Steward, WA Health’s Corporate Governance Directorate, the Director General and the CCC.

**STEP 4:** Review the incident and take action to prevent future breaches

The Data Custodian must ensure that the cause of the breach has been fully investigated and that the Data Steward and the Director General have been briefed on outcomes and recommendations, as appropriate.

At a minimum, amendments to policies 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 should include:

- a security audit of both physical and technical security
- a review of employee selection and training practices
- a review of policies and procedures to reflect the lessons learned from the investigation
- staff training in responding to data breaches effectively.

7. **EXPECTED RESPONSE TIMING FOR TYPES OF DATA BREACHES**

The Data Breach Response Steps as set out in this policy should be followed in all instances of a data breach. The specific activities and the expected response timing of these steps will vary, depending on the incident type and the severity rating of the incident.

The WA Health Potential Causes and Expected Responses for Data Breaches Guideline (Guideline) ([Attachment C](#)) provides staff with a guide for managing data breaches that correspond with the four types outlined in Section 4.

The Guideline provides examples according to the type of data breach, as well as their potential cause, and suggests an appropriate response and timeframe for managing the data breach.

These Guidelines may be used to provide Data Custodians with assistance to develop their own response timings that will relate directly to their data collection.

8. **DATA RETENTION**

Once a data breach has been investigated, any related documentation must be kept by the Data Custodian and maintained 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 electronic records relating to the investigation should also be maintained in accordance with WA Health policies relating to the management and long term preservation of electronic
Data Breach documentation should be classified as confidential and access must be managed in accordance with the Access and Disclosure Policy (OD 0539/14).

9. DEFINITIONS

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregate Level Data</td>
<td>is summed and/or categorised data that is analysed and placed in a format that precludes further analysis (for example: in tables or graphs) to prevent the chance of revealing an individual’s identity (individual records cannot be reconstructed).</td>
</tr>
<tr>
<td>Confidential Information</td>
<td>access and disclosure of this information must be controlled and will only be given to persons in order to perform their duties (need-to-know) or through legislation.</td>
</tr>
<tr>
<td>Data Breach</td>
<td>is 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.</td>
</tr>
<tr>
<td>Data Collection</td>
<td>is a systematic gathering of data for a particular purpose from various sources, including manual entry into an application system, questionnaires, interviews, observation, existing records and electronic devices. This includes both operational data collections and data repositories.</td>
</tr>
<tr>
<td>Data Custodian</td>
<td>is a person(s) responsible for the day-to-day management of data from a business perspective. The Data Custodian aims to improve the accuracy, usability and accessibility of data within the data collection.</td>
</tr>
<tr>
<td>Data Repository</td>
<td>includes data that is collected from various sources, including operational data collections for the primary purpose of monitoring, evaluation, reporting and research. Examples of data repositories include data held within the Hospital Morbidity Data Collection, Finance Data Warehouse and the Emergency Department Data Collection.</td>
</tr>
<tr>
<td>Data Steward</td>
<td>is a delegated person responsible for setting the overall strategic direction of a specific data collection. They ensure the collection is developed, maintained and utilised in accordance with the strategic goals of WA Health. The Data Steward is also responsible for authorising access, use and disclosure of data from the data collection for clearly defined purposes that comply with WA Health’s statutory obligations.</td>
</tr>
<tr>
<td>Internal Protected Information</td>
<td>is information readily available to WA Health employees. Information may be accessed or disclosed to third parties.</td>
</tr>
<tr>
<td><strong>Logon Number</strong></td>
<td>is a unique alphanumeric string allocated by the system administrator and used to identify a computer system user. The logon number is used in conjunction with a secure password to gain access to a computer system.</td>
</tr>
<tr>
<td><strong>Personal Data</strong></td>
<td>information or an opinion whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.</td>
</tr>
<tr>
<td><strong>Personal Health Information</strong></td>
<td>pertains to all health information where the identity of a person is apparent or can reasonably be ascertained from the information itself. Information is also personal information if it is reasonably possible for the person receiving the information to identify the individual by using other information that they already hold.</td>
</tr>
<tr>
<td><strong>Public Information</strong></td>
<td>is information approved as suitable for public dissemination or deemed public by legislation or routine disclosure.</td>
</tr>
<tr>
<td><strong>Record Level Data</strong></td>
<td>is data at the level of an individual person. Record-level data need not directly identify the data subject, but is more vulnerable to re-identification than aggregate data.</td>
</tr>
<tr>
<td><strong>Risk Assessment</strong></td>
<td>is the identification, evaluation and estimation of the levels of risks involved in a situation.</td>
</tr>
<tr>
<td><strong>WA Health Information</strong></td>
<td>refers to anything spoken, overheard, written, stored electronically, copied, transmitted or held intellectually concerning WA Health’s general business, information systems, employees, business partners, patients or customers.</td>
</tr>
<tr>
<td><strong>WA Health</strong></td>
<td>incorporates the legal entities of the Metropolitan Health Service, WA Country Health Service, Department of Health and the administrative entities of Child and Adolescent Health Service, North Metropolitan Health Service and the South Metropolitan Health Service.</td>
</tr>
</tbody>
</table>

10. **ROLES AND RESPONSIBILITIES**

10.1 **Data Steward**

Data Stewards are accountable for data breaches relating to their data collection.

Data Stewards are responsible for ensuring that the Director General has been sufficiently briefed in relation to data breaches with a medium, high or very high impact severity rating. The Data Steward has the authority to determine that further investigation or action in relation to a data breach is required.

10.2 **Data Custodian**

Data Custodians are responsible for the security of the data and adherence to standards. Once the Data Custodian has either discovered or been informed of a data breach or
suspected data breach, it is the responsibility of the Data Custodian to assess the severity of the incident and decide on any immediate action to be taken in consultation with the Data Steward.

The Data Custodian must complete the relevant sections of the WA Health Data Breach Incident Reporting Form (Appendix A).

Once a data breach has been finalised, the Data Custodian is responsible for maintaining all data breach documentation in accordance with record keeping practices.

10.3 WA Health Staff

It is the responsibility of all WA Health personnel to ensure that data breaches are reported to the Data Custodian and the Data Breach Incident Reporting Form (Appendix A) is completed and signed before submitting the form to the Data Custodian.

11. COMPLIANCE

Compliance with this Operational Directive is mandatory. Those who fail to comply with this policy may face disciplinary action and, in serious cases, termination of their employment or engagement. Moreover, users who breach confidentiality and security may be subject to disciplinary action and other remedies available through legislative provision such as the Public Sector Management Act 1994 and Criminal Code Act 1913. Unauthorised access, use, disclosure and destruction of confidential information is misconduct pursuant to the WA Health Code of Conduct and suspected cases may be reported to the Corruption and Crime Commission (refer to WA Health Misconduct and Discipline Policy OD 0323/11).

12. EVALUATION

In order to ensure currency and ongoing relevance to WA Health, this policy will be reviewed every 3 years by the Information Development and Management Branch (IDM) within the Resourcing and Performance Division.

13. RELATED DOCUMENTS

Acceptable Use Policy – Information and Communications Technology (OD 0468/13)
Data Stewardship and Custodianship Policy (OD 0487/14)
General Disposal Authority for State Government Information GDA 2013-017
Information Access and Disclosure Policy (OD 0539/14)
Information and Communication Technology (ICT) Physical and Environmental Security Policy (OD 0506/14)
Information Security Policy (OD 0389/12)
Information Use Policy (OD 0390/12)
Patient Confidentiality (IC 0164/13)
Policy on Use of Official Information and Public Comment (OD 0327/11)
Updated ICT Risk Management Policy (OD 0480/13)
14. RELEVANT LEGISLATION

Children and Community Services Act 2004
Commonwealth Privacy Act 1988 (Australian Privacy Principles)
Coroners Act 1996
Criminal Code Act 1913
Electronic Transactions Act 2011
Evidence Act 1906, Acts Amendment (Evidence) Act 2000
Freedom of Information Act 1992
Freedom of Information Regulations 1993
Health Act 1911
Health and Disability Services (Complaints) Act 1995
Health Legislation Administration Act 1984
Hospital and Health Services Act 1927
Mental Health Act 1996
Public Sector Management Act 1994
State Records Act 2000

15. NATIONAL & INTERNATIONAL STANDARDS / SPECIFICATIONS

## WA HEALTH DATA BREACH INCIDENT REPORTING FORM

### PART A - Information to be completed by staff reporting the incident

<table>
<thead>
<tr>
<th>Information</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full name</td>
<td></td>
</tr>
<tr>
<td>HE Number</td>
<td></td>
</tr>
<tr>
<td>Position Title and Department</td>
<td></td>
</tr>
<tr>
<td>Contact information</td>
<td></td>
</tr>
</tbody>
</table>

### Details of the Incident

<table>
<thead>
<tr>
<th>Details of the Incident</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date, time, duration and location of the breach.</td>
<td></td>
</tr>
<tr>
<td>How was the breach discovered?</td>
<td></td>
</tr>
<tr>
<td>Description of the incident, including what WA Health systems may be affected.</td>
<td></td>
</tr>
<tr>
<td>Cause of the breach (if known).</td>
<td></td>
</tr>
<tr>
<td>Was any other staff member notified or witnessed the incident at the time?</td>
<td></td>
</tr>
</tbody>
</table>

### DATA BREACH IMPACT SEVERITY RATING

Refer to Appendix B.


Provide reasoning for the allocation of the impact rating:

**Signature:**

**Date:**
<table>
<thead>
<tr>
<th>PART B - Information to be completed by the Data Custodian</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full name and HE number</strong></td>
</tr>
<tr>
<td><strong>Position Title and Department</strong></td>
</tr>
<tr>
<td><strong>Contact information</strong></td>
</tr>
</tbody>
</table>

Do you agree with the Data Breach Impact Severity Rating?  **YES**  **NO**  (circle answer)

If no, please document the amended rating and reasoning:

### Details of the Incident

- **Who does the data breach affect?** (e.g. staff, patients, general public, other government agencies, any third party).
- **Estimated number of individuals affected.**
- **Description of immediate actions taken to contain the data breach.**
- **Was anyone else notified of the data breach?** (i.e. health service, university, police etc.) Contact details and when.
- **Cause and estimated cost of the data breach (if known).**
- **Has evidence been preserved? Please specify.**
- **Is further investigation considered necessary and how will this be undertaken?**
- **Have steps been taken to prevent the breach from occurring again?**

**Signature:**  
**Date:**
## DATA BREACH IMPACT SEVERITY RATINGS FORM

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

<table>
<thead>
<tr>
<th>Impact Type</th>
<th>Impact Severity</th>
<th>Severity</th>
<th>Level of reporting required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact on Government finances, economic or commercial interests</td>
<td>1. NEGLIGIBLE</td>
<td>No or negligible impact – consequences resolved by routine operations</td>
<td>Report required to be submitted to Data Custodian</td>
</tr>
<tr>
<td></td>
<td>2. LOW</td>
<td>Minor impact on finances, economic or commercial interests</td>
<td>Report required to be submitted to Data Custodian and Data Steward</td>
</tr>
<tr>
<td></td>
<td>3. MEDIUM</td>
<td>Moderate impact – disadvantage caused to the government in commercial or policy negotiations</td>
<td>Report to be submitted to Data Custodian, Data Steward and if appropriate Director General</td>
</tr>
<tr>
<td></td>
<td>4. HIGH</td>
<td>Substantial – damage to finances, economic or commercial interests</td>
<td>Report to be submitted to Data Custodian, Data Steward, Director General and the Minister for Health</td>
</tr>
<tr>
<td></td>
<td>5. VERY HIGH</td>
<td>Substantial – damage to finances, economic or commercial interests</td>
<td>Report to be submitted to Data Custodian, Data Steward, Director General and the Minister for Health</td>
</tr>
<tr>
<td>Impact on development or operation of major government policy</td>
<td>No or negligible impact – consequences resolved by routine operations</td>
<td>Minor – impact on efficiency or effectiveness, managed internally</td>
<td>Report required to be submitted to Data Custodian</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Impede effective development or operation – significant review or changes required</td>
<td>Report required to be submitted to Data Custodian, Data Steward and if appropriate Director General</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Seriously impede development or operation – project or program may not survive</td>
<td>Report to be submitted to Data Custodian, Data Steward, Director General and the Minister for Health</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Substantially impede operation or development</td>
<td>Report to be submitted to Data Custodian, Data Steward, Director General and the Minister for Health</td>
</tr>
</tbody>
</table>

## WA HEALTH POTENTIAL CAUSES AND EXPECTED RESPONSES FOR DATA BREACHES

### TYPE OF DATA BREACH – INFORMATION SECURITY

Theft or loss of any fixed or portable ICT asset that:

- is owned by WA Health, or an individual but used for WA Health business purposes, or used by a third party for hosting WA Health applications systems or data
- has been used to process or store WA Health information, or information from other agencies that is in the custody of WA Health.

This includes desktop or laptop computers, network drives, servers, mobile devices, portable storage devices, media devices and similar assets that contain WA Health information.

<table>
<thead>
<tr>
<th>Expected Response</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Report the theft or loss to Health Information Network (HIN) Helpdesk in accordance with the <em>Information Security Policy (OD 0389/12)</em>.</td>
<td>Loss/theft must be reported immediately.</td>
</tr>
<tr>
<td>HIN to disable access to all accounts associated with systems accessible from the asset.</td>
<td>Relevant accounts are to be disabled as soon as the report is received by HIN.</td>
</tr>
<tr>
<td>Determine what information was stored on the asset and how it was protected.</td>
<td></td>
</tr>
<tr>
<td>Complete a WA Health Data Breach Incident Form (Part A) and assign a Data Breach Impact Severity Rating.</td>
<td></td>
</tr>
<tr>
<td>Send the Data Breach Incident Form to the Data Custodian or relevant manager for action.</td>
<td></td>
</tr>
<tr>
<td>Data Custodian to ensure the correct Data Breach Impact Severity Rating has been allocated.</td>
<td></td>
</tr>
<tr>
<td>Data Custodian to complete Part B of the WA Health Data Breach Incident Form and liaise with HIN on reporting the theft or loss to WA Police.</td>
<td></td>
</tr>
<tr>
<td>Data Custodian to compile a report and circulate to the relevant positions as indicated on the Data Breach Impact Severity Ratings Form.</td>
<td></td>
</tr>
</tbody>
</table>
**Appendix C**

**Abuse of privileges in a networked environment:**

Changes to access privileges in a networked environment that have not been approved through an official process. This includes unauthorised changes to data, installation of unauthorised software and similar incidents.

**Expected Response**

- Report the breach to HIN Helpdesk in accordance with the *Information Security Policy (OD 0389/12)*.
- HIN to suspend the privileged account and to determine which systems, devices, networks or information have been accessed using the account in the past 12 months.
- HIN to analyse logs for all systems, devices or networks accessed using the compromised account in the last 12 months, and determine what unauthorised activities may have occurred.
- HIN to audit configurations of all systems, devices or networks accessed using the compromised account to determine what unauthorised changes have been made.
- Complete a WA Health Data Breach Incident Form (Part A) and assign a Data Breach Impact Severity Rating.
- Send the Data Breach Incident Form to the Data Custodian for action.
- Data Custodian to ensure the correct Data Breach Impact Severity Rating has been allocated.
- Data Custodian to complete Part B of the WA Health Data Breach Incident Form, including feedback from HIN regarding their investigation.
- Data Custodian to compile a report and circulate to the relevant positions as indicated on the Data Breach Impact Severity Ratings Form.
- Disciplinary action to be determined depending on the severity of the incident.

| Immediate account suspension. |
| Analysis/audits to be started within 24 hours of the report. |
| Remedial and disciplinary action to be taken as soon as reviews are complete. |
Unauthorised changes to system files

This includes incidents such as changes to network profiles, local user or device configuration files, access control lists and similar incidents.

**Expected Response**

- Report the breach to HIN Helpdesk in accordance with the *Information Security Policy (OD 0389/12)*.
- HIN to compare the actual file content against the authorised content and identify changes made.
- HIN to analyse logs to determine when the changes were made and who made them.
- HIN to review all related or similar systems to determine the extent of unauthorised changes, which systems are affected, how and when they were made and who made them.
- If required, HIN to roll back to previous secure baseline and re-boot system/device to implement roll back.
- Complete a WA Health Data Breach Incident Form (Part A) and assign a Data Breach Impact Severity Rating.
- Send the Data Breach Incident Form to the Data Custodian for action.
- Data Custodian to ensure the correct Data Breach Impact Severity Rating has been allocated.
- Data Custodian to complete Part B of the WA Health Data Breach Incident Form, including feedback from HIN regarding their investigation.
- Data Custodian to compile a report and circulate to the relevant positions as indicated on the Data Breach Impact Severity Ratings Form.
- Disciplinary action to be determined depending on the severity of the incident.

| Investigation started within 24 hours of the incident report. | Subsequent timing dependent on the severity and extent of issues discovered. | Remedial and disciplinary action to be taken as soon as reviews are complete. |
# Password Confidentiality

**Sharing, stealing or loss of passwords or other authentication tokens.**

<table>
<thead>
<tr>
<th>Expected Response</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Report the breach to HIN Helpdesk in accordance with the <a href="https://example.com">Information Security Policy (OD 0389/12)</a>.</td>
<td></td>
</tr>
<tr>
<td>- HIN to determine what accounts have had their passwords compromised.</td>
<td></td>
</tr>
<tr>
<td>- HIN to disable any affected accounts.</td>
<td></td>
</tr>
<tr>
<td>- Investigate how password confidentiality was compromised e.g. through weak or guessable passwords, writing the password down, sharing the password with colleagues, key loggers, theft or loss of security tokens or similar activities.</td>
<td></td>
</tr>
<tr>
<td>- Complete a WA Health Data Breach Incident Form (Part A) and assign a Data Breach Impact Severity Rating.</td>
<td></td>
</tr>
<tr>
<td>- Send the Data Breach Incident Form to the Data Custodian for action.</td>
<td></td>
</tr>
<tr>
<td>- Data Custodian to ensure the correct Data Breach Impact Severity Rating has been allocated.</td>
<td></td>
</tr>
<tr>
<td>- Data Custodian to complete Part B of the WA Health Data Breach Incident Form, including feedback from HIN regarding their investigation.</td>
<td></td>
</tr>
<tr>
<td>- Data Custodian to compile a report and circulate to the relevant positions as indicated on the Data Breach Impact Severity Ratings Form.</td>
<td></td>
</tr>
<tr>
<td>- Disciplinary action to be determined depending on the severity of the incident.</td>
<td></td>
</tr>
</tbody>
</table>

**Investigation to start within 72 hours of the incident report.**

**Remedial and disciplinary action to be taken as soon as reviews are complete.**
## TYPE OF DATA BREACH – PERSONAL HEALTH INFORMATION

Compromise of classified or sensitive data.

Unauthorised release or disclosure of WA Health information classified as Protected (internal) or Confidential, whether intentional or unintentional, to a known party who does not have approved access to the information, or to an unknown party, or to an uncontrolled environment (e.g. to the internet, social media etc.). This includes incidents caused by improper handling of classified WA Health data.

### Expected Response
- Complete a WA Health Data Breach Incident Form (Part A) and assign a Data Breach Impact Severity Rating.
- Send the Data Breach Incident Form to the Data Custodian for action.
- Data Custodian to ensure the correct Data Breach Impact Severity Rating has been allocated.
- Data Custodian to work with the appropriate parties to determine the extent of the information compromise.
- If the compromise occurred at a third party location (e.g. an existing hosting environment), or was caused by a staff member of a third party, determine what legal contract applies and work with Legal and Legislative Services and the Data Steward to review contract terms and determine the next course of action.
- If a user (employee, contractor, consultant, etc.) was responsible for the compromise, contact the appropriate Supervisor, Manager, or Director and begin investigation. Possible disciplinary action or possible termination may need to be considered.
- In the case of contractors, or other third party personnel, consider discontinuance of the third party’s contract with WA Health.
- Data Custodian to complete Part B of the WA Health Data Breach Incident Form.
- Data Custodian to compile a report and circulate to the relevant positions as indicated on the Data Breach Impact Severity Ratings Form.
- Disciplinary action to be determined depending on the severity of the incident.

Investigation started within 24 hours of incident report.

Subsequent timing dependent on severity and extent of issues discovered.

Remedial and disciplinary action to be taken as soon as reviews are complete.
## Unauthorised access to data or information systems.

Unauthorised access to WA Health data, whether intentional or unintentional by internal or external parties.

<table>
<thead>
<tr>
<th>Expected Response</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Complete a WA Health Data Breach Incident Form (Part A) and assign a Data Breach Impact Severity Rating.</td>
<td></td>
</tr>
<tr>
<td>• Send the Data Breach Incident Form to the Data Custodian for action.</td>
<td></td>
</tr>
<tr>
<td>• Data Custodian to ensure the correct Data Breach Impact Severity Rating has been allocated.</td>
<td></td>
</tr>
<tr>
<td>• Data Custodian to work with HIN to determine the extent of the information compromise.</td>
<td></td>
</tr>
<tr>
<td>• For successful unauthorised logons from a remote location:</td>
<td>Investigation started within 24 hours of incident report.</td>
</tr>
<tr>
<td>o Data Custodian, in conjunction with HIN, to ensure the protection of remote access services and the application or system accessed, as appropriate.</td>
<td></td>
</tr>
<tr>
<td>o HIN to identify the source of the attack including IP addresses and any known port numbers.</td>
<td></td>
</tr>
<tr>
<td>• For successful unauthorised logon from within WA Health premises or other authorised third party premises:</td>
<td>Subsequent timing dependent on the severity and extent of issues discovered.</td>
</tr>
<tr>
<td>o Data Custodian, in conjunction with HIN, to consider the contribution poor credential management may have made to the incident e.g. weak passwords, inadequate password reset mechanisms, authentication mechanisms not strong enough etc.</td>
<td></td>
</tr>
<tr>
<td>o Where appropriate, Data Custodian to recommend to take action to strengthen the authentication of the identity and access management for the information or systems.</td>
<td></td>
</tr>
<tr>
<td>• Data Custodian to complete Part B of the WA Health Data Breach Incident Form, including feedback from HIN regarding their investigation.</td>
<td></td>
</tr>
<tr>
<td>• Data Custodian to compile a report and circulate to the relevant positions as indicated on the Data Breach Impact Severity Ratings Form.</td>
<td></td>
</tr>
<tr>
<td>• Disciplinary action to be determined depending on the severity of the incident.</td>
<td>Remedial and disciplinary action to be taken as soon as reviews are complete.</td>
</tr>
</tbody>
</table>
### TYPE OF DATA BREACH – CORPORATE, FINANCIAL OR MEDICAL WORKFORCE INFORMATION

Violation or breach of WA Health policies, standards or guidelines.

A deliberate, negligent or reckless non-compliance with WA Health policies, standards or an accidental or unintentional non-compliance with WA Health guidelines.

#### Expected Response
- Complete a WA Health Data Breach Incident Form (Part A) and assign a Data Breach Impact Severity Rating.
- Send the Data Breach Incident Form to the Data Custodian for action.
- Data Custodian to ensure the correct Data Breach Impact Severity Rating has been allocated.
- Data Custodians to work with the appropriate parties to determine the extent of the potential violation.
- If the violation occurred at a third party location or was caused by a staff member of a third party, determine what legal contract applies and work with Legal and Legislative Services and the Data Steward to review contract terms and determine the next course of action.
- If a user (employee, contractor, consultant etc.) was responsible for the violation or breach, the Data Custodian is to contact the appropriate Manager, Supervisor or Director for disciplinary action and possible termination. In the case of contractors, or other third party personnel, consider discontinuance of the contract with WA Health.
- Data Custodian to complete Part B of the WA Health Data Breach Incident Form.
- Data Custodian to compile a report and circulate to the relevant positions as indicated on the Data Breach Impact Severity Ratings Form.
- Disciplinary action against the staff member is to be determined depending on the severity of the incident.

Investigation to start within 24 hours of incident report.

Remedial and disciplinary action to be taken as soon as reviews are complete.
Violation or breach of legislative requirements.

A deliberate, negligent or reckless non-compliance with legislation that WA Health is required to adhere to in relation to information management.

### Expected Response
- Complete a WA Health Data Breach Incident Form (Part A) and assign a Data Breach Impact Severity Rating.
- Send the Data Breach Incident Form to the Data Custodian for action.
- Data Custodian to ensure the correct Data Breach Impact Severity Rating has been allocated.
- Data Custodian to work with the appropriate personnel to determine the extent of the potential violation.
- Data Custodian is to identify the personal information compromised (e.g. name, address, Medicare number, other unique identifiers, medical and health information, etc.).
- Determine the number of individuals affected.
- Determine where the compromise occurred (including reviewing, in conjunction with HIN, test, development and production application environments, pre and post processing and production data warehouse environments).
- Data Custodian to notify Data Steward and Legal and Legislative Services, and if applicable Director General, that a privacy violation or breach has been reported and provide them with an overview of the situation. Cooperate with all parties as required and keep them informed of the status of the incident.
- If the breach or violation occurred at a third party location or was caused by a staff member of a third party, determine what legal contract applies and work with relevant services to review contract terms and determine the next course of action.
- If a user (employee, contractor, consultant etc.) was responsible for the breach, contact the appropriate Supervisor, Manager or Director for disciplinary action and possible termination. In the case of contractors, temporaries or other personnel, consider discontinuance of the contract with WA Health.
- Data Custodian to complete Part B of the WA Health Data Breach Incident Form.
- Data Custodian to compile a report and circulate to the relevant positions as indicated on the Data Breach Impact Severity Ratings Form.
- Disciplinary action against the staff member is to be determined depending on the severity of the incident.

<table>
<thead>
<tr>
<th>Investigation to start within 24 hours of incident report.</th>
<th>Remedial and disciplinary action to be taken as soon as reviews are complete.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expected Response</td>
<td></td>
</tr>
<tr>
<td>Complete a WA Health Data Breach Incident Form (Part A) and assign a Data Breach Impact Severity Rating.</td>
<td></td>
</tr>
<tr>
<td>Send the Data Breach Incident Form to the Data Custodian for action.</td>
<td></td>
</tr>
<tr>
<td>Data Custodian to ensure the correct Data Breach Impact Severity Rating has been allocated.</td>
<td></td>
</tr>
<tr>
<td>Data Custodian to work with the appropriate personnel to determine the extent of the potential violation.</td>
<td></td>
</tr>
<tr>
<td>Data Custodian is to identify the personal information compromised (e.g. name, address, Medicare number, other unique identifiers, medical and health information, etc.).</td>
<td></td>
</tr>
<tr>
<td>Determine the number of individuals affected.</td>
<td></td>
</tr>
<tr>
<td>Determine where the compromise occurred (including reviewing, in conjunction with HIN, test, development and production application environments, pre and post processing and production data warehouse environments).</td>
<td></td>
</tr>
<tr>
<td>Data Custodian to notify Data Steward and Legal and Legislative Services, and if applicable Director General, that a privacy violation or breach has been reported and provide them with an overview of the situation. Cooperate with all parties as required and keep them informed of the status of the incident.</td>
<td></td>
</tr>
<tr>
<td>If the breach or violation occurred at a third party location or was caused by a staff member of a third party, determine what legal contract applies and work with relevant services to review contract terms and determine the next course of action.</td>
<td></td>
</tr>
<tr>
<td>If a user (employee, contractor, consultant etc.) was responsible for the breach, contact the appropriate Supervisor, Manager or Director for disciplinary action and possible termination. In the case of contractors, temporaries or other personnel, consider discontinuance of the contract with WA Health.</td>
<td></td>
</tr>
<tr>
<td>Data Custodian to complete Part B of the WA Health Data Breach Incident Form.</td>
<td></td>
</tr>
<tr>
<td>Data Custodian to compile a report and circulate to the relevant positions as indicated on the Data Breach Impact Severity Ratings Form.</td>
<td></td>
</tr>
<tr>
<td>Disciplinary action against the staff member is to be determined depending on the severity of the incident.</td>
<td></td>
</tr>
</tbody>
</table>
## TYPE OF DATA BREACH – ENVIRONMENTAL

Other events including physical or environmental factors.

Events which result in a loss of integrity of information, systems or networks. This includes fire, storms and floods, biological agents, chemical spills, power outages or similar events.

**Expected Response**

- Complete a WA Health Data Breach Incident Form (Part A) and assign a Data Breach Impact Severity Rating.
- Send the Data Breach Incident Form to the Data Custodian for action.
- Data Custodian to ensure the correct Data Breach Impact Severity Rating has been allocated.
- Data Custodian to work with the Disaster Preparedness and Management Unit (DPMU). Data Custodian to complete Part B of the WA Health Data Breach Incident Form.
- Data Custodian to compile a report and circulate to the relevant positions as indicated on the Data Breach Impact Severity Ratings Form.

Investigation commencing is dependent on the type and extent of the incident.
This page is intentionally left blank