ACT Government | ACT Health

POLICY DOCUMENT

Data Breach Policy and Procedure

Document number	**AHDPD-81:2021**
Effective date	October 2023
Review date	October 2024
Author branch	Data Analytics Branch
Endorsed by	Executive Board (Operational)
Audience	All ACTHD Staff
Version number	2.0

Contents

Policy Statement

Organisations collecting data about people have responsibilities to manage that data safely. How the ACT Health Directorate (ACTHD) protects the confidentiality and security of the data it holds is prescribed in legislation including the *Health Records (Privacy and Access) Act 1997* (ACT) and the *Information Privacy Act 2014* (ACT). The *Information Privacy Act 2014* (ACT) contains 13 Territory Privacy Principles that set standards, rights and obligations for the collection, use, disclosure, storage, access and correction of personal information.

ACTHD is committed to safeguarding the privacy and security of the information it holds or hosts. The community expects that any information provided to the government about them will be safe from unauthorised access or disclosure.[1]

Purpose

This policy describes the steps that are necessary to manage a data breach or near-miss data breach occurring within the ACTHD and the policies that underpin these processes.

Scope

This policy applies to all ACTHD workers, including permanent, temporary and casual employees, external contractors, consultants and volunteers.

ACTHD workers are required to comply with all obligations in relation to privacy and data protection as directed in relevant legislation and policies.

This policy covers all corporate, business, clinical and operational information held by ACTHD. It includes information acquired from external sources or provided to ACTHD by external data custodians and accessed through ACTHD systems.

Background

To assist in achieving ACTHD's vision of 'a healthier Canberra' and ensuring 'our public health system meets our community's needs, now and into the future',[2] ACTHD collects or acquires a wide range of data. Data is a critical enabler. It is a foundational tool that facilitates the undertaking of many vital functions, including policy or clinical decision-making, informing safety and quality improvements, and performance reporting and evaluations. As outlined in the *ACT Health Protective Security Policy Framework,* ACTHD has obligations to protect the information it holds and for it to be accessed only by those with a 'need-to-know'.

1 OAIC Australian Community Attitudes to Privacy Survey 2020
2 ACT Health Directorate Strategic Plan 2020-2025.

The Office of the Australian Information Commissioner (OAIC) states that a data breach has occurred where **personal information** is accessed or disclosed without authorisation, or is lost. Examples include intentional, malicious actions by an internal or external party; human error; failure to comply with security requirements; loss of a device such as a laptop or thumb drive; a failure in information handling; or a failure of security systems.[3]

A **data breach** is said to have occurred where **personal information** is accessed or disclosed without authorisation, or is lost.

Near-miss data breaches may also occur. These are potential data breaches or events that almost became a data breach, yet the issue was identified in time. Reporting near-miss data breaches enables underlying system failures to be addressed so that future incidents may be prevented.[4,5]

DATA BREACH EXAMPLES

SECURITY SYSTEM FAILURE: A worker clicks on a link in an email (spear-phishing) that leads to the downloading of malware to ACTHD's servers. This allows a hacker to access and extract personal information.

NO 'NEED-TO-KNOW' (SNOOPING): A worker accesses the clinical records of a 'celebrity' patient or family member when they are not part of the treating team.

NEAR-MISS DATA BREACH EXAMPLE

A worker **almost** accidentally emails a spreadsheet containing person information to the wrong recipient.

Data breaches can result in significant harm to an individual's physical or mental well-being. Breaches may lead to financial loss, or reputational damage. Data breaches can also adversely affect ACTHD's reputation, finances, interests, or operations; or diminish the public's trust in the organisation or government more broadly.

Personal information

The *Information Privacy Act 2014* (ACT) defines **personal information** as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable—
(i) whether the information or opinion is true or not; and (ii) whether the information or opinion is recorded in a material form or not; but does not include personal health information about the individual.'

3 OAIC Part 1: Data breaches and the Australian Privacy Act — OAIC
4 Data Breach Statistics https://www.data-breach-statistics.com/data-breach-near-miss/
5 BMet https://www.bmet.ac.uk/about-bmet/governance/data-protection/data-breach/

Examples of personal information are an individual's name, signature, address, phone number, date of birth, credit information, employee record information, photographs, internet protocol (IP) addresses, voice print, facial recognition biometrics, or location.[6]

Some personal information may not in itself identify a person (a photograph or date of birth for example), but when combined with other information, such as that found on the internet, it may be possible to establish an identity.[7] Where any personal information is inappropriately disclosed, *regardless of whether an individual is identifiable or not*, the disclosure should be treated as a data breach.

Where any personal information is inappropriately disclosed, *regardless of whether an individual is identifiable or not,* the disclosure should be treated as a data breach.

Personal information also includes sensitive information[8], but does not include personal health information (which is dealt with by separate legislation outlined below).

Sensitive information

Sensitive information is personal information that is:[9]

a) about the individual's:
- racial or ethnic origin, or
- political opinions, or
- membership of a political association, or
- religious beliefs or affiliations, or
- philosophical beliefs, or
- membership of a professional or trade association, or
- membership of a trade union, or
- sexual orientation or practices, or
- criminal record, or

(b) genetic information about the individual, or

(c) biometric information about the individual that is to be used for the purpose of automated biometric verification or biometric identification, or

(d) a biometric template that relates to the individual.

6 OAIC What is personal information?
7 OAIC Data breach preparation and response (oaic.gov.au) page 7
8 *Information Privacy Act 2014* (ACT)
9 *Information Privacy Act 2014* (ACT)

Personal health information

Personal health information is governed by separate requirements set out in the *Health Records (Privacy and Access) Act 1997* (ACT). Privacy Principle 10 of the *Health Records (Privacy and Access) Act 1997* (ACT) states that 'a record keeper … must not disclose personal health information about a consumer from the record to an entity other than the consumer' unless under certain conditions.

The *Health Records (Privacy and Access) Act 1997* (ACT) defines **personal health information** as 'any personal information, whether or not recorded in a health record— (a) relating to the health, an illness or a disability of the consumer; or (b) collected by a health service provider in relation to the health, an illness, or a disability of the consumer.' A 'consumer' is defined broadly and includes any individual who uses, or has used, a health service.

The *Health Records (Privacy and Access) Act 1997* (ACT) provides a separate process for complaints which is managed by the Health Services Commissioner, as part of the ACT Human Rights Commission.

The Notifiable Data Breach Scheme

The OAIC primarily deals with issues covered by the *Privacy Act 1988* (Cth). This Act does not cover local, state or territory government agencies, as most jurisdictions have equivalent privacy legislation. The *Privacy Act 1988* (Cth), does however, apply to all Australian *private* sector health service providers.[10]

The Notifiable Data Breach Scheme (NDBS) requires an organisation subject to the *Privacy Act (1988)* (Cth) to notify the OAIC about 'eligible data breaches'. The NDBS was established under the *Privacy Act (1988)* (Cth) to ensure that individuals whose personal information had been involved in a data breach can take timely action to reduce harm, such as changing their online passwords.

ACT government agencies are not subject to the *Privacy Act 1988* (Cth) (except in relation to some specific requirements in relation to Tax File Numbers), but there is an informal arrangement that exists where ACT public sector agencies voluntarily report eligible data breaches under the NDBS. At ACTHD, an eligible data breach must be reported to the OAIC.

Where the breach involves Tax File Numbers, it is a legal requirement for ACTHD to report this to the OAIC via the NDBS.

Where the breach involves Tax File Numbers, it is a legal requirement for ACTHD to report this to the OAIC via the NDBS.

10 OAIC Privacy in your state

An eligible data breach is a breach where:[11]

- there is **unauthorised access** to; **or unauthorised disclosure** of personal information held by an entity (or information is **lost** in circumstances where unauthorised access or disclosure is likely to occur), AND
- it is likely to result in **serious harm** to any of the individuals to whom the information relates, AND
- the entity has been unable to prevent the likely risk of serious harm with remedial action.

An eligible data breach must be reported to the OAIC.

An NDBS-eligible data breach is reported using the form available at the OAIC website.

Unauthorised access includes staff viewing personal information where they have no need-to-know, or through malicious hacking. Examples of unauthorised **disclosure** include accidental or intentional publication or emailing the personal information of one or more individuals. **Loss** includes leaving hard copy documents, unsecured computers or portable storage devices containing personal information in public areas.

Serious harm resulting from a data breach may be physical, psychological, emotional, financial, or reputational in form.

In circumstances where ACTHD has successfully implemented remedial action that has prevented a likely risk of serious harm to affected individuals, the event may no longer meet the eligible data breach criteria and OAIC notification may no longer be required.

If steps to address a data breach can be completed quickly so that there is no resulting harm, it is not mandatory to notify the OAIC under the NDBS.

Depending on the nature of the breach, ACTHD may have other reporting obligations or may voluntarily report an incident to organisations such as ACT Policing. There may also be other reporting obligations, such as those under the *National Cancer Screening Register Act 2016* (Cth) or the *My Health Records Act 2012* (Cth).

11 OAIC Report a data breach - Home (oaic.gov.au)

Response Plan

Taking quick action to reduce or prevent harm following a data breach is important to assist in building community trust in government agencies. The OAIC has published guidance on best practice data breach management processes.[12] This involves developing a data breach response plan that describes the strategy to identify a breach and manage it from start to finish. How ACTHD manages a data breach is outlined below.

Accountabilities and responsibilities

The Executive Group Manager (EGM), Policy Partnerships and Programs is accountable for managing a rapid and appropriate response to a data breach. The EGM is also accountable for the review and management of near-miss breaches. The EGM may direct the Director, Data Strategy and Governance to convene a Data Breach Response Team to manage a data breach. The EGM may choose to report significant breaches to the ACTHD Director-General or the Minister for Health.

The Data Breach Response Team is responsible for managing the breach in a timely manner.

All staff have a responsibility to report any data breach to a supervisor as soon as the event has been detected.

All data breaches and near-miss data breaches must be reported to the Data Strategy and Governance team: HealthDataGovernance@act.gov.au

All staff have a responsibility to report any data breach to a supervisor as soon as the event has been detected.

Supervisors have a responsibility to ensure that the person identifying the incident submits a Data Breach Notification Form to the Data Strategy and Governance team.

The Director, Data Strategy and Governance is responsible for ensuring that all data breaches are lodged on the Data Breach Registry. The EGM will direct quarterly reporting from the Data Breach Registry. These reports will be provided to the ACT Health Digital Committee.

These responsibilities are described in more detail in the sections below. **Appendix One** (Table A1) is a flow chart of the steps that need to be undertaken following identification of a breach, including responsibilities and time frames for completion of activities.

12 OAIC Data breach preparation and response - Home (oaic.gov.au)

Data Breach Response Team membership

The EGM may direct the Data Breach Response Team to manage a reported data breach. The EGM may determine that a breach does not need to be managed by the Data Breach Response Team, in instances for example, where the breach has been contained and where no harm will occur to individuals or the organisation.

Where the EGM considers that additional expertise is required to manage a more complex data breach, Data Breach Response Team membership can incorporate relevant experts from across the organisation. Depending on the nature of the data breach, expertise could be drawn from the roles listed in **Table 1**. Other roles can also be considered, as requested by the EGM.

Any necessary legal advice can be requested from the ACT Government Solicitor. To request legal advice, contact ACT Health Governance and Risk, who can assist to facilitate the request, or contact the ACT Government Solicitor outposted to ACTHD.

Table 1: Additional expertise that may be included in a Data Breach Response Team

Function	Role	Responsibility
Coordinator	Director, Data Strategy and Governance	Leads and coordinates the response to the data breach and reports progress to the EGM
Privacy champion	Privacy Officer	Privacy advice
Data knowledge	Business area Director, Senior Director or Executive	Provide advice regarding affected data; extent and nature of breach
ICT security	Chief Information Security Officer	Provide advice on IT systems security
Corporate risk management	Director, Enterprise Risk Management	Provide advice on corporate risk management
Communications	Senior Director, Strategic Communications	Assists notifications to affected individuals Manages media and external stakeholder communications
Information and records management	Senior Director, Office of the CIO	Advises on security and monitoring controls of ACTHD administrative records

ACTHD staff with specific expertise in areas relevant to data breach management, such as the Chief Information Security Officer or the Communication team, will advise the data breach response team or Accountable Officer about the most appropriate external experts to consult where internal expertise is insufficient to adequately manage an incident.

Breach management

The OAIC identifies four steps to manage a data breach: 1) contain; 2) assess; 3) notify; and 4) review. In ACTHD, the first step (contain) is the immediate responsibility of the business area, while the last three steps (assess, notify and review) are the responsibility of the Data Breach Response Team. In ACTHD, the person identifying a breach or near-miss also has a responsibility to **report** the incident to their supervisor.

The most appropriate response to a breach needs to be determined on a case-by-case basis. For example, it may be necessary to undertake steps 1) to 3) simultaneously or in quick succession, or to notify affected individuals before any containment or assessment of the breach has occurred.

Business area responsibilities

Report

The person who identifies an actual, suspected or near-miss data breach must report the incident to *any* supervisor. The business unit identifying the breach may differ from the business unit where the breach originated.

Immediately following supervisor notification and at the completion of any activities that the supervisor has directed be undertaken to contain the breach, the person identifying the breach is required to complete a Data Breach Notification Form, which can be found on the ACTHD Policy Register and HealthHQ. The completed form is to be sent to the Data Strategy and Governance team (HealthDataGovernance@act.gov.au) within **one business day.** The Director will register the breach or near-miss on the Data Breach Registry and activate the Data Breach Response Team if necessary.

ACTHD executive and managers should foster and actively encourage the reporting of data breaches and near-misses. People make mistakes and staff should feel confident that they can report unintentional breaches without concern that there will be adverse consequences for them. Unless breaches and near-misses are reported, system changes cannot be implemented to better protect personal information.

People make mistakes and staff should feel confident that they can report unintentional breaches without concern that there will be adverse consequences for them.

Contain

The business area should try to contain the breach as soon as the event has been identified. This could lead to the recovery of the personal information before it is accessed inappropriately. The approach to containment should be agreed with the business area supervisor. Assess whether the personal information is still being disclosed, and what can be immediately done to secure the information or stop its continued disclosure.

Immediate remediation may include:

- tracing and recovering all copies of the data
- **immediately contacting the Chief Information Security Officer, where there is a suspected IT security breach**
- changing access codes or passwords.

EXAMPLE OF CONTAINMENT (ADAPTED FROM OAIC WEBSITE)

A data file, which includes the personal information of numerous individuals, is sent to an incorrect recipient outside ACTHD. The sender realises the error and contacts the recipient, who advises that the data file has not been accessed.

The sender regards the recipient as reliable and trustworthy, as in this instance, they are from another government agency. The sender confirms that the recipient has not copied the file and that the file has been permanently deleted. In the circumstances, the sender and supervisor decide that there is no likely risk of serious harm.

Business areas should only manage the breach during the period immediately following identification of the incident by attempting to retrieve the disclosed information. **The Data Breach Response Team has the responsibility of overall management of the breach.**

All relevant information should be saved to the enterprise records management system (Objective).

Business areas should only manage the breach during the period immediately following identification of the incident by attempting to retrieve the disclosed information.

Data Breach Response Team responsibilities

Extensive resources are available on the OAIC website to assist the Data Breach Response Team with the assessment, notification and review components of breach management.

Assess

Appendix Two provides guidance for the Data Breach Response Team when assessing a breach.

Using all the evidence that is available and under the direction of the EGM, the Data Breach Response Team will systematically assess the nature and scope of the breach. The OAIC states that the assessment must be completed within a maximum of 30 calendar days, but emphasises that the process should be completed **as quickly as possible**, to limit any harm that may arise.[13] This comprehensive assessment should include gaining an understanding of the type information involved int the breach; likely cause; whether there was misconduct;

13 OAIC Data breach preparation and response

extent (number of records or documents); whether there is a likelihood of harm for involved individuals; and, whether any further steps can be taken to remediate harm.

Where the Data Breach Response Team considers that a breach may cause harm to one or more individuals and that harm cannot be mitigated by ACTHD, **an appropriate response plan must be developed and submitted to the EGM within three business days.**

Where the Data Breach Response Team considers that a breach may cause harm to one or more individuals and that harm cannot be mitigated by ACTHD, an appropriate response plan must be developed and submitted to the EGM within three business days.

Notify

Once the extent and nature of the breach has been assessed by the Data Breach Response Team, the response plan may include notifying affected individuals about the breach. Others may also need to be notified, such as the OAIC's NDBS, a law enforcement agency, or, where the breach included acquired or hosted data, it may be necessary to contact external data custodians.

Notification should occur as soon as practicable following the assessment of the incident. The response team or Accountable Officer will work with the business area or Strategic Communications team to consider the most appropriate way to notify individuals (by phone, email or letter for example) depending on the extent and nature of the incident.

In some instances, it may not be feasible to notify individuals potentially impacted by a data breach. In these cases, ACTHD must publish a 'statement prepared for the [Australian Information] Commissioner on its website and take reasonable steps to bring its contents to the attention of individuals at risk of serious harm'.[14] This may require publication of the breach on ACTHD website for a period of at least six months.

Where an eligible data breach is reported to the OAIC, or where the Accountable Officer considers there is potential for a third party to lodge a personal injury claim, the ACT Insurance Authority in the Chief Minister, Treasury and Economic Development Directorate must also be notified.

Business areas must not contact affected individuals or external data custodians. This is the responsibility of the Data Breach Response Team. Consider too, that notifying individuals about a breach that is unlikely to lead to harm may cause unnecessary stress or anxiety.

Business areas must not contact affected individuals or external data custodians. This is the responsibility of the Data Breach Response Team.

14 Part 4: Notifiable Data Breach (NDB) Scheme - Home (oaic.gov.au)

The Data Breach Response Team should consider who is best placed to notify affected individuals. The Team should also assess if, how and when the breach is reported publicly, particularly where a law enforcement agency is investigating the incident.

Where the data breach involves information from one or more external data custodians, obligations under the NDBS are applicable to each affected agency. The OAIC allows that NDBS compliance by one agency is compliance by all agencies – only one agency is required to report the incident. This is to be determined by the affected agencies, but OAIC suggests that the agency with the most direct relationship with the affected individuals is chosen to report the breach to the NDBS.

Where the data breach involves information from one or more external data custodians, obligations under the NDBS are applicable to each affected agency.

Where a data breach involves information from one or more external data custodians, the Director Data Strategy and Governance in consultation with the Accountable Officer or the data breach response team, will work with external custodians to determine an agreed approach to notify affected individuals.

For data breaches to be eligible for reporting to the NDBS, an objective assessment must be undertaken 'from the perspective of a reasonable person, [that] the data breach would be likely to result in serious harm to an individual whose personal information was part of the data breach.' A reasonable person means a 'person in the entity's [organisation's] position (rather than the position of an individual whose personal information was part of the data breach or any other person), who is properly informed, based on information immediately available or following reasonable inquiries or an assessment of the data breach.' [15]

When assessing the **likelihood of serious harm,** the Data Breach Response Team should consider, for example:

- whether the disclosed information was protected by passwords or other measures
- the nature of the information involved (such as identifying, health or financial data)
- the possible intentions of those who receive or find the information
- the number of individuals involved - the more people's personal information is involved, the more likely it may be that at least some will experience serious harm.

Each incident is assessed by the Data Breach Response Team on a case-by-case basis, and their actions, and timeliness of implementation of these actions, may vary for each breach.

ACT Human Rights Commission

Where an incident involves the unauthorised disclosure of personal health information, the Data Breach Response Team should also consider notifying the ACT Health Services Commissioner.

15 OAIC Data beach preparation and response, page 33

Review

A review occurs once all previous steps have been completed. During this phase, the Data Breach Response Team assesses what lessons about the management of personal information can be learned from the breach or near-miss. This may include initiating a security review, changing a system or process, establishing an audit schedule, reviewing policies and procedures, or establishing a training program. Breaches should be considered alongside any similar past incidents to determine whether there may be a systematic process failure.

The end-to-end management of the data breach or near-miss must be documented in the Data Breach Registry and stored on the enterprise records management system.

Roles and Responsibilities

Position	Role	Contact
All ACTHD Employees	• Responsible for reporting a suspected or confirmed data breach or near miss to a supervisor. • Participate in investigations as required. • Documentation of all data breach-related actions and decisions. • Complete and submit a Data Breach Notification Form.	Various
EGM, Policy Partnerships and Programs	• Accountable for the management of responses to all data breaches. • Directs and supports the Data Breach Response Team. • Ensures compliance with the relevant privacy legislation.	02 5124 9392 ACTHealthPolicyPartnerships-Programs@act.gov.au
Data Breach Response Team	• Under the direction of the EGM, responsible for the management and implementation of the Data Breach Response Plan.	
Director, Data Strategy and Governance	• Responsible for maintaining the Data Breach Registry • Manages the Data Breach Response Team • Maintains the data breach response plan.	HealthDataGovernance@act.gov.au

Records Management

All staff are responsible for documenting any information about a data breach on the enterprise records management system.

Related Documents

Legislation

- Health Records (Privacy & Access) Act 1997
- Information Privacy Act 2014 (ACT)
- Privacy Act 1988 (Cwth)

Supporting Documents

- ACT Health Directorate Information Privacy Policy
- The ACT Health Protective Security Policy Framework

Evaluation

Outcome Measures	Method	Responsibility
Staff understand their responsibilities and are comfortable reporting data breaches or near misses	Data Breach Registry may indicate an increase in reporting	All staff

Version Control

This document is due for review every two years, or after a major Data Breach incident.

Version	Date	Comments
0.1	07/10/2021	
0.2	17/11/2021	Major revision
0.3	06/12/2021	Review of legislative components by ACT Government Solicitor outposted to ACTHD
1.0	08/06/2022	Update to change accountable officer and Division; other minor changes
2.0	17/07/2023	OAIC review suggestions, Data Strategy and Governance, DAB

Disclaimer: *This document has been developed by the ACTHD specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at his or her own risk and the ACTHD assumes no responsibility whatsoever.*

Appendix One: Data breach response

TABLE A1: Data Breach Response flow chart

Responsible area		Activity
BUSINESS AREA	Staff member identifying the incident	**REPORT** a suspected or known data breach, or near-miss to a supervisor **WHEN? Immediately**
		A data breach has occurred where personal information is accessed or disclosed without authorisation, or is lost. A near-miss is an event that almost became a data breach, yet the issue was identified in time.
	Staff member identifying the incident and the supervisor	**CONTAIN** a suspected or known data breach **WHEN? Immediately**
		Take immediate steps to limit any further access or distribution.
	Staff member identifying the incident	**DATA BREACH NOTIFICATION FORM** **WHEN?** Immediately following supervisor notification
		Complete a Data Breach Notification Form for ALL data breaches and near-misses. Return the form to HealthDataGovernance@act.gov.au
EXECUTIVE GROUP MANAGER (EGM)	The EGM, Policy Partnerships and Programs and the Data Breach Response Team with guidance from others	**ASSESS** **WHEN**: As soon as possible
		The EGM will determine whether the Data Breach Response Team should be convened to undertake a systematic assessment of the breach.
		DEVELOP A DATA BREACH RESPONSE PLAN **WHEN:** Where the Data Breach Response Team considers that a breach may cause harm to one or more individuals and that harm cannot be mitigated by ACTHD, a Data Breach Response Plan must be completed **within 3 business days**.
		Based on the assessment, develop and implement a Data Breach Response Plan.
		IF THE BREACH IS LIKELY TO CAUSE HARM, A NOTIFICATION PROCESS MUST OCCUR
		- **NOTIFY THE OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER, OTHERS**
		Depending on the assessment outcomes, it may be necessary to notify the Office of the Australian Information Commissioner (OAIC). Consider whether others, such as the police or other data custodians need to be notified.
		- **NOTIFY AFFECTED INDIVIDUALS**
		Refer to the OAIC website for guidance on notifying affected individuals. Consider who within ACTHD is best placed to undertake this task.
		REVIEW
		Review the incident to prevent future breaches.

Appendix Two: Assessment guide

Although the Data Breach Response Team can determine their own methods, the OAIC has suggested a three-staged approach (**Table A2**) for assessing a data breach.[16]

An assessment must be completed expeditiously and in no more than 30 days.

All data breach-related information, management, processes and outcomes must be documented on the enterprise records management system.

TABLE A2: Three-staged assessment guide

Stage	Considerations
Initiate	Is it necessary for the Data Breach Response Team to undertake an assessment? The EGM makes this determination.
Investigate quickly	Gather relevant information from all sources including the Data Breach Notification Form. Consider the type of personal information involved, the circumstances of the breach, and the nature of any harm to individuals. Can further remedial action be undertaken to mitigate risks of harm to affected individuals or ACTHD? Who now has access to the information? What might be their intentions? What are the next steps?
Evaluate	Is the breach likely to result in serious harm to any of the affected individuals AND ACTHD has been unable to prevent serious harm with remedial action (i.e. an 'eligible data breach')? If an 'eligible data breach', report it to the OAIC under the NDBS and notify affected individuals.

16 OAIC Assessing a suspected data breach