Data Breach Protocol

A data breach is when personal information held by an entity is lost or subject to unauthorised access, modification, disclosure or tother misuse or interference. Examples of a data beach are when a device containing personal information of clients is lost or stolen, an entity's database containing personal information is hacked or an entity mistakenly provides personal information to the wrong person.

STEP 1: Contain the breach and do a preliminary assessment

1a Contain the breach

- Stop any unauthorised practice
- Recover the records
- Shut down the system that was breached. (Contact IT phone: 1300 136 757)
- Resetting passwords for user accounts that may have been compromised and advising users to change other accounts on which they use the same password.
- Recall or delete information such as recalling emails, asking unintended recipients to destroy copies or disabling links that have been mistakenly posted.

Take care to ensure that steps taken to contain the breach don't inadvertently compromise the integrity of any investigation.

If it is not practical to shut down the system, or if it would result in loss of evidence, then revoke or change computer access privileges or address weaknesses in physical or electronic security.

Assess whether steps can be taken to mitigate the harm an individual may suffer as a result of a breach.

1b Initiate a preliminary assessment

The Practice Manager of the Clinical School (Joanne Henderling 07 3232 7090) will lead the initial assessment.

- What personal information does the breach involve?
- What was the cause of the breach?
- What is the extent of the breach?
- What are the harms (to affected individuals) that could potentially be caused by the breach?
- How can the breach be contained?

UnitingCare *Clinical School*

Document Name: Data Breach Protocol	Created: Oct 2017	Version: 5
Author: Head of Clinical School	Effective Date: Oct 2017	Next Review: Dec 2025
Authorised by: Dr Stephen Cook	Reviewed: August 2024	

1c Consider who needs to be notified immediately

- Determine who needs to be made aware of the breach (internally and potentially externally) at this preliminary stage.
- It may be appropriate to notify the affected individuals immediately (for example, where there is a high level of risk of serious harm to affected individuals).
- Escalate the matter internally as appropriate, including informing the DMS Office
- If the breach appears to involve theft or other criminal activity, it will generally be appropriate to notify the police.
- If the data breach is likely to involve a real risk of serious harm to individuals, or receive a high level of media attention, inform the OAIC.
  Office of the Australian Information Commissioner
  Phone 1300 363 992
  Email enquiries@oaic.gov.au
  Website www.oaic.gov.au

Other matters

- Where a law enforcement agency is investigating the breach, consult the investigating agency before making details of the breach public.
- Be careful not to destroy evidence that may be valuable in determining the cause or would allow the agency or organisation to take appropriate corrective action.
- Ensure appropriate records of the suspected breach are maintained, including the steps taken to rectify the situation and the decisions made.

UnitingCare Clinical School

STEP 2: Evaluate the risks associated with the breach

2a Consider the type of personal information involved

- ***Does the type of personal information that has been compromised create a greater risk of harm?***
  For example, government-issued identifiers such as Medicare numbers, driver's licence and health care numbers, health information, and financial account numbers. A combination of personal information typically creates a greater risk of harm than a single piece of personal information.
- ***Who is affected by the breach?***
  Employees, contractors, the public, clients, service providers, other agencies or organisations?

2b Determine the context of the affected information and the breach

- ***What is the context of the personal information involved?***
  For example, a list of customers on a newspaper carrier's route may not be sensitive information. However, the same information about customers who have requested service interruption while on vacation may be more sensitive.
- ***What parties have gained unauthorised access to the affected information?***
  Employee records containing information about employment history such as performance and disciplinary matters or a co-worker's mental health might be particularly sensitive if exposed to other employees in the workplace and could result in an individual being the subject of humiliation or workplace bullying.
- ***Have there been other breaches that could have a cumulative effect?***
  A number of small, seemingly insignificant, breaches could have a cumulative effect
- ***How could the personal information be used?***
  Could the information be used for fraudulent or otherwise harmful purposes, such as to cause significant embarrassment to the affected individual?
  Could the compromised information be easily combined either with other compromised information or with publicly available information to create a greater risk of harm to the individual?

2c Establish the cause and extent of the breach

- ***Is there a risk of ongoing breaches or further exposure of the information?***
  What was the extent of the unauthorised access to or collection, use or disclosure of personal information, including the number and nature of likely recipients and the risk of further access, use or disclosure, including via mass media or online?
- ***Is there evidence of theft?***
  Evidence of theft could suggest a greater intention to do harm and heighten the need to provide notification to the individual, as well as law enforcement.
- ***Is the personal information adequately encrypted, anonymised or otherwise not easily accessible?***
  Is the information rendered unreadable by security measures that protect the stored information? Is the personal information displayed or stored in such a way so that it cannot be used if breached?
- ***What was the source of the breach?***

For example, did it involve external or internal malicious behaviour, or was it an internal processing error? Does the information seem to have been lost or misplaced?
The risk of harm to the individual may be less where the breach is unintentional or accidental, rather than intentional or malicious.

- ***Has the personal information been recovered?***
  For example, has a lost laptop been found or returned? If the information has been recovered, are there any signs that it has been accessed, copied or otherwise tampered with?
- ***What steps have already been taken to mitigate the harm?***
  Has the agency or organisation contained the breach? For example, have compromised security measures such as passwords been replaced? Has the full extent of the breach been assessed? Are further steps required?
- ***Is this a systemic problem or an isolated incident?***
  When checking the source of the breach, it is important to check whether any similar breaches have occurred in the past. Sometimes, a breach can signal a deeper problem
  with system security. This may also reveal that more information has been affected than initially thought, potentially heightening the awareness of the risk posed.
- ***How many individuals are affected by the breach?***
  If the breach is a result of a systemic problem, there may be more people affected than first anticipated.
  If the breach affects many individuals, the scale of the breach may create greater risks that the information will be misused. The agency or organisation's response should be proportionate.
  While the number of affected individuals can help gauge the severity of the breach, it is important to remember that even a breach involving the personal information of one or two people can be serious, depending on the information involved.

2d Assess the risk of harm to the affected individuals

- ***Who is the recipient of the information?***
  Is there likely to be any relationship between the unauthorised recipients and the affected individuals?
  Or was the recipient a trusted, known entity or person that would reasonably be expected to return or destroy the information without disclosing or using it?
- ***What harm to individuals could result from the breach?***
  Examples include:
  • identity theft
  • financial loss
  • threat to physical safety
  • threat to emotional wellbeing
  • loss of business or employment opportunities
  • humiliation, damage to reputation or relationships, or
  • workplace or social bullying or marginalisation.

2e Assess the risk of other harms

- ***Other possible harms, including to the agency or organisation that suffered the breach***

Examples include:

• the loss of public trust

• reputational damage

• loss of assets

• financial exposure

• regulatory penalties

• extortion

• legal liability

- Breach of secrecy provisions in applicable legislation

STEP 3: Notification

3a Deciding whether to notify affected individuals

Consider whether obligations under APP 11 (Appendix A) require us to notify affected individuals and the OAIC (as a 'reasonable step' to ensure the security of personal information held).

The key consideration is whether notification is necessary to avoid or mitigate serious harm to an affected individual.

Consider the following factors when deciding whether notification is required:

- What is the risk of serious harm to the individual as determined by step 2?
- What is the ability of the individual to avoid or mitigate possible harm if notified of a breach (in addition to steps taken by the agency or organisation)? For example, would an individual be able to have a new bank account number issued to avoid potential financial harm resulting from a breach? Would steps such as monitoring bank statements or exercising greater vigilance over their credit reporting records assist in mitigating risks of financial or credit fraud?
- Even if the individual would not be able to take steps to fix the situation, is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual?
- What are the legal and contractual obligations to notify, and what are the consequences of notification?

3b Notification process

When to notify?

- In general, individuals affected by the breach should be notified as soon as reasonably possible.
- If law enforcement authorities are involved, check with those authorities whether notification should be delayed to ensure that the investigation is not compromised.
- Delaying the disclosure of details about a breach of security or information systems may also be appropriate until that system has been repaired and tested or the breach contained in some other way.

How to notify?

- In general, the recommended method of notification is **direct** – by phone, letter, email or in person – to the affected individuals.
- Indirect notification, either by website information, posted notices, media, should generally only occur where direct notification could cause further harm, is cost-prohibitive, or the contact information for affected individuals is not known.
- Preferably, notification should be 'standalone' and should not be 'bundled' with other material unrelated to the breach, as it may confuse recipients and affect the impact of the breach notification.
- In certain cases, it may be appropriate to use multiple methods of notification.
- Notification might increase the risk of harm, such as by alerting the person who stole the laptop of the value of the information on the laptop, if it would not otherwise be apparent.
- To avoid being confused with 'phishing' emails, email notifications may require special care. For example, only communicate basic information about the breach, leaving more detailed advice to other forms of communication.

Who should notify?

- Typically, the agency or organisation that has a direct relationship with the customer, client or employee should notify the affected individuals.
- This includes where a breach may have involved handling of personal information by a third party service provider, contractor or related body corporate.
- Joint and third party relationships can raise complex issues. The issues in play in each situation will vary. Organisations and agencies will have to consider what is best on a case by case basis. However some relevant considerations might include:
  - Where did the breach occur?
  - Who does the individual identify as their 'relationship' manager?
  - Does the agency or organisation that suffered the breach have contact details for the affected individuals? Are they able to obtain them easily? Or could they draft and sign off the notification, for the lead organisation to send?

Who should be notified?

- Generally, it should be the individual(s) affected by the breach. However, in some cases it may be appropriate to notify the individual's guardian or authorised representative on their behalf.
- There may be circumstances where carers or authorised representatives should be notified as well as, or instead of, the individual.
- Where appropriate, clinical judgement may be required where notification may exacerbate health conditions, such as acute paranoia.

3c What should be included in the notification?

The content of notifications will vary depending on the particular breach and the notification method. In general, the information in the notice should help the individual to reduce or prevent the harm that could be caused by the breach. Notifications should include the types of information detailed below:

- **Incident Description —** Information about the incident and its timing in general terms. The notice should not include information that would reveal specific system vulnerabilities.
- **Type of personal information involved —** A description of the type of personal information involved in the breach. Be careful not to include personal information in the notification, to avoid possible further unauthorised disclosure.
- **Response to the breach —** A general account of what the agency or organisation has done to control or reduce the harm, and proposed future steps that are planned.
- **Assistance offered to affected individuals —** What the agency or organisation will do to assist individuals and what steps the individual can take to avoid or reduce the risk of harm or to further protect themselves.
  For example, whether the agency or organisation can arrange for credit monitoring or other fraud prevention tools, or provide information on how to change government issued identification numbers (such as a driver's licence number).

- **Other information sources —** Sources of information designed to assist individuals in protecting against identity theft or interferences with privacy.
  The OAIC's website at www.oaic.gov.au and the Attorney-General's Department website at www.ag.gov.au/www/agd/agd.nsf/page/Crimeprevention_Identitysecurity provide this guidance.

- **Agency/ Organisation contact details —** Contact information of areas or personnel within the agency or organisation that can answer questions, provide further information or address specific privacy concerns.
  Where it is decided that a third party will notify of the breach, a clear explanation should be given as to how that third party fits into the process and who the individual should contact if they have further questions.

- **Whether breach notified to regulator or other external contact(s) —** Indicate whether the agency or organisation has notified the OAIC or other parties listed in the table at 3(d).
- **Legal implications —** The precise wording of the notice may have legal implications; organisations and agencies should consider whether they should seek legal advice. The legal implications could include secrecy obligations that apply to agencies.
- **How individuals can lodge a complaint with the agency or organisation —** Provide information on internal dispute resolution processes and how the

- **Credit card companies, financial institutions or credit reporting agencies —** If their assistance is necessary for contacting individuals or assisting with mitigating harm.

- **Professional or other regulatory bodies —** If professional or regulatory standards require notification of these bodies. For example, other regulatory bodies, such as the Australian Securities and Investments Commission, the Australian Competition and Consumer Commission, and the Australian Communications and Media Authority have their own requirements in the event of a breach.

- **Other internal or external parties not already notified —** Agencies and organisations should consider the potential impact that the breach and notification to individuals may have on third parties, and take action accordingly. For example, third parties may be affected if individuals cancel their credit cards, or if financial institutions issue new cards.
  Consider:
  - third party contractors or other parties who may be affected
  - internal business units not previously advised of the breach, (for example, communications and media relations, senior management), or
  - union or other employee representatives.
- **Agencies that have a direct relationship with the information lost/stolen —** Agencies and organisations should consider whether an incident compromises Australian Government agency identifiers such as TFNs or Medicare numbers. Notifying agencies such as the Australian Taxation Office for TFNs or Medicare Australia for Medicare card numbers may enable those agencies to provide appropriate information and assistance to affected individuals, and to take steps to protect the integrity of identifiers that may be used in identity theft or other fraud.

STEP 4: Prevent future breaches

Once the immediate steps are taken to mitigate the risks associated with the breach, we need to take the time to investigate the cause and consider whether to review the existing prevention plan or, if there is no plan in place, develop one.

A prevention plan should suggest actions that are proportionate to the significance of the breach, and whether it was a systemic breach or an isolated event.
This plan may include:

- a security audit of both physical and technical security
- a review of policies and procedures and any changes to reflect the lessons learned from the investigation, and regular reviews after that (for example, security, record retention and collection policies)
- a review of employee selection and training practices, and
- a review of service delivery partners (for example, offsite data storage providers).

UnitingCare Clinical School

Appendix A – APP 11

Australian Privacy Principle 11 – security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:
(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

11.2 If:
(a) an APP entity holds personal information about an individual; and

(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and

(c) the information is not contained in a Commonwealth record; and

(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

The entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.