Procedure to Respond to a Breach of Privacy

Parent policy

This document is a procedure supporting Ahpra's Privacy Policy.

Scope

This procedure sets out the roles and responsibilities for managing a privacy breach (or suspected breach) and provides direction to Ahpra employees on how to respond to such a breach.

Responding to a privacy breach quickly and efficiently can substantially decrease the impact of a breach on individuals, reduce the costs associated with dealing with a breach and reduce the potential reputational damage that can result from a breach.

Ahpra is subject to a mandatory data breach notification scheme (**NDB Scheme**). Under the NDB Scheme, where a data breach that is likely to result in serious harm to affected individual/s (**eligible data breach**), Ahpra is required by law to notify the National Health Practitioner Ombudsman and Privacy Commissioner (**NHPOPC**) and the affected individual/s.

This procedure explains:

- how to identify and respond to a privacy breach;
- the steps to follow in the event of a privacy breach;
- how to assess whether the privacy breach is an eligible data breach; and
- how to comply with the NDB Scheme if the breach is an eligible data breach.

Related documents

- Response worksheet
- Template emails and letters
- Serious Incident Report
- Privacy Statement
- Privacy Policy
- Staff Privacy Guide

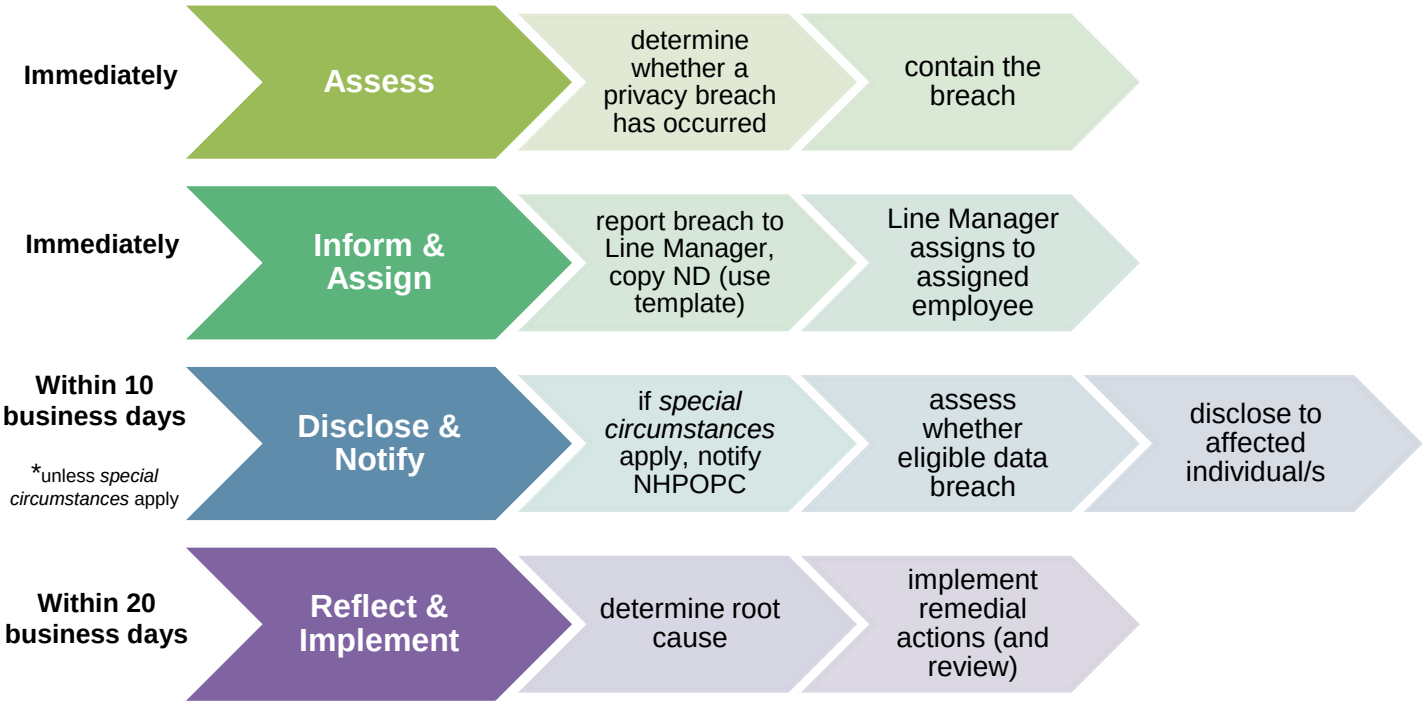
Relevant legislation

- *Health Practitioner Regulation National Law* (as in force in each State and Territory)
- *Privacy Act 1988* (Cth)

Procedure

Overview

The following steps must happen in response to any privacy breach or suspected privacy breach in line with the timeframes set out in the diagram below.



1. Assess

1.1 Determine whether a privacy breach has occurred

1.1.1 The employee who discovers or is otherwise alerted to a privacy breach (or suspected privacy breach) must undertake an immediate initial assessment to determine if a breach has occurred.

1.1.2 As part of the initial assessment the employee will determine (if possible) the author of the breach. If there is any doubt as to whether a privacy breach has, or may have, occurred, seek advice from Corporate Legal.

> A breach of privacy occurs when personal information is lost or subject to unauthorised access, modification, use or disclosure or other misuse.

1.1.3 A privacy breach can be the result of a deliberate act (e.g. theft) or the unintended consequence of an act or omission by an employee or agency. Privacy breaches can also include the unauthorised collection, use or disclosure of, or access to, personal information, or failure to take reasonable steps to protect personal information that Ahpra holds.

1.1.4 When disclosing personal information, Ahpra staff must consider whether the disclosure is permitted or authorised.

1.1.5 Some examples of actions that could lead to a breach of privacy:

- accidentally sending an email to the wrong person (e.g. if your computer automatically populates the recipient's email address);
- personal information provided to a third party by mail, email or via telephone where this was not authorised (e.g. a researcher or journalist asks you for personal or protected information

regarding a practitioner or practitioners and you disclose this information without making sure you are authorised to do so);

- the loss of hard copy files of personal information;
- failing to properly secure personal information (e.g. you leave personal or protected information about a practitioner open on your desk when you leave the office);
- the disposal of personal information in a non-secure manner;
- unauthorised access to personal information on computer files (e.g. you decide to look up personal information about a practitioner out of curiosity, not because you need to for work);
- failure to remove personal information from documents being distributed to third parties; and
- an Ahpra database (including a database that is controlled by a third party contracted service provider) containing personal information is hacked.

1.1.6 A breach of privacy will not occur in the following circumstances of disclosure:

- when it is in the exercise of a function under or for the purposes of the National Law;
- to a co-regulatory authority where authorised or required by the National Law;
- where it is authorised or required by the law of a participating jurisdiction;
- where it is otherwise permitted by law;
- when there is current, informed and specific consent of the person to whom the information relates;
- where the disclosure does not identify the person's identity;
- where it has been disclosed in public proceedings before a responsible tribunal;
- when the information is accessible to the public; or
- when it is otherwise authorised by the Ministerial Council in accordance with the National Law.

1.2 Contain the breach

1.2.1 An immediate priority is to contain the breach. This may include stopping the unauthorised practice, shutting down a system that was breached, addressing security weaknesses or the retrieval of information from a third party.

1.2.2 The third-party recipient of any personal information must be contacted by the fastest means possible (telephone/email), informed of the breach of privacy, and asked to return or destroy the information, or to delete any electronic records without first reading, making copies or forwarding to any other party.

1.2.3 A verbal request must be followed by correspondence to the third party asking to confirm that they have not retained any copies of the information in their possession.

Use *Template Letter for Retrieving Information that has been Disclose*d (**Attachment 3**).

1.2.4 Where necessary and feasible, steps must be taken to prevent further release of personal information – this could be as simple as ensuring that the latest postal address is retained on file. If it involves securing or shutting down breached systems or revoking or changing computer access codes, the

assigned employee will contact the IT Security Manager and ensure the shutdown or changes occur as soon as possible.

1.2.5 Steps must also be taken to prevent the loss of evidence in relation to the breach – for example, obtaining a copy of email databases or the investigation of relevant computer systems. If there is any doubt as to the evidence that ought to be kept seek advice from Corporate Legal.

1.2.6 To determine what other steps might be immediately necessary, the assigned employee will (in collaboration with the National Director Organisational Risk & Resilience or Corporate Legal in the event of a possible eligible data breach), assess the risks associated with the breach, taking into account factors such as:

- the amount and nature of the personal information that has been disclosed - for example, health related information may cause significant risk of harm; similarly credit or debit card numbers could be used in combination for identity theft;
- the risk of harm arising from the disclosure - for example whether contact information has been disclosed which may present a risk of family violence;
- whether the person whose privacy was breached is known to the recipient of the data – this might cause difficulties in personal or professional relationships and put the person whose privacy was breached at risk;
- did the breach occur once or on multiple occasions;
- has the breach been stopped or is there is any potential for ongoing breach;
- was the information accessible or was it encrypted or otherwise protected;
- was the information lost or stolen and the surrounding circumstances;
- was one or a number of individuals affected;
- whether it was a systemic problem or an isolated incident; and
- what steps have been taken to deal with the harm.

2. Inform

2.1 Report breach to Line Manager

2.1.1 The Ahpra Employee must immediately report the breach to their Line Manager via email and copy in their National Director.

> Use *Initial Email to Line Manager Notifying of Breach Template* (**Attachment 2**).

2.2 Line Manager to assign an Ahpra employee to respond

2.2.1 The Line Manager must assign to an Ahpra Employee the responsibility of responding to the breach (**assigned employee**). This will take the form of a reply to the initial email. The assigned employee must not be the employee who was apparently responsible for the breach.

2.2.2 The Line Manager who receives notification of the Serious Incident report will in turn brief the National Director and copy in Corporate Legal.

2.2.3 The assigned employee will conduct a preliminary investigation into the circumstances of the breach and when necessary (including in the event of a possible eligible data breach under the NDB Scheme) will liaise with Corporate Legal for guidance and assistance. This investigation must be conducted as expeditiously as possible. The circumstances of the response will be documented in a Serious Incident Report.

Use *Serious Incident Report*
(access **here**).

2.2.4 The assigned employee must undertake this responsibility on an urgent basis at the expense of other work. The assigned employee is expected to exercise professional judgment and the assignment ought to be declined if other work cannot be rescheduled.

2.2.5 The assigned employee must seek confirmation from Corporate Legal as to whether the breach is (or may be) an "eligible data breach" under the NDB Scheme. The relevant factors that Corporate Legal will consider in determining whether there is or may have been an eligible data breach are outlined below in section 3.2.

2.2.6 The assigned employee will create a separate file in TRIM, named as '[*Affected person Surname] [First name] – Breach of Privacy*'. At all stages, contemporaneous notes of the response will be maintained together with all emails and other documents to ensure a complete record of the event is available for review and auditing.

Use *Response to Breach of Privacy Worksheet Template* (**Attachment 1**), copy into the file and rename appropriately. This worksheet must be kept up to date in the file.

3. Disclose

3.1. Notify NHPOPC if *special circumstances* apply

3.1.1 The following circumstances are considered to be "special circumstances":

- some or all of the information released includes NHPOPC material (e.g. emails to/from the NHPOPC's office);
- the affected individual is made aware of the breach by a third party (e.g. an email is incorrectly sent to a third party and that third party notifies the affected individual before Ahpra has an opportunity to do so);
- the breach is likely to attract media coverage; and
- the breach is a systemic and/or large-scale breach (e.g. an Ahpra database containing personal information has been hacked).

3.1.2 If any of the above circumstances apply, Corporate Legal must be notified immediately so that the NHPOPC can be notified within 2 business days.

3.1.3 Note that all correspondence to the NHPOPC must be drafted and sent by Corporate Legal.

3.2. Assess whether breach is an eligible data breach

An eligible data breach arises where a reasonable person would conclude that there is a *likely* risk of *serious harm* to any of the impacted individuals as a result of a breach.

Likely means more probable than not having regard to all relevant matters, including:

- the security measures in place by Ahpra (e.g. is the data encrypted/password protected, and what is the likelihood that these measures could be overcome);
- the extent and sensitivity of the information; and

- the potential for exploitation or misuse of the information (e.g. potential for identity theft).

Serious harm may include physical harm, financial/economic harm, emotional harm (e.g. embarrassment or humiliation), psychological harm and reputational harm. As assessment of the risk of serious harm should consider the specific circumstances of the breach.

Note –

- If it is unclear whether a breach is an eligible data breach, it should be treated as such.
- Where Ahpra has taken reasonable steps to contain the data breach, such that there is no longer a likely risk of serious harm to the individual/s, the breach will not be an eligible data breach.
- Where the breach relates to a contracted service provider or involves another third party, Corporate Legal must be notified and provided with the relevant signed contract to determine whether there are any additional obligations (including contractual obligations) relating to managing the breach.

3.3. Disclose to affected individual/s

3.3.1. Where the breach is an eligible data breach

Corporate Legal will determine if there are reasonable grounds to believe that an eligible data breach has occurred, in which case they will work with the assigned employee to complete the Serious Incident Report in accordance with this procedure and notify the affected individual/s in accordance with legislative requirements.

NOTE: No notification documentation is to be sent outside of Ahpra until advice has been sought from Corporate Legal and approval granted by the National Executive.

If there are reasonable grounds to believe that there has been an eligible data breach, Corporate Legal must:

I. Prepare a statement (**Statement**) that complies with the requirements set out below and give a copy of the Statement to the NHPOPC as soon as practicable after it becomes so aware.

Statement requirements

The Statement must set out:

(a) the identity and contact details of Ahpra; and

(b) a description of the eligible data breach that Ahpra has reasonable grounds to believe has happened; and

(c) the kind(s) of information concerned; and

(d) recommendations about the steps that individuals should take in response to the eligible data breach; and

(e) if another entity is involved in the data breach, the identity and contact details of that entity.

II. Notify the affected individual/s in compliance with the requirements set out below, as soon as practicable after the Statement has been completed.

Notification requirements

(a) if practicable, take reasonable steps to notify the contents of the Statement to each of the individuals to whom the information relates; or

(b) if practicable, take reasonable steps notify the contents of the Statement to each of the individuals who are at risk from the eligible data breach; or

(c) if neither a) nor b) apply, publish a copy of the Statement on Ahpra's website (and a National Board's website if relevant), and take reasonable steps to publicise the contents of the Statement.

Ahpra can use any method to notify individuals (for example telephone call, SMS, mail, email, social media post or in-person conversation), so long as the method is reasonable.

The outcome of this confirmation is to be noted on the Serious Incident Form prepared by the assigned employee.

3.3.2. Where the breach is <u>not</u> an eligible data breach

Disclosure to the affected individual(s) of a data breach can be an important mitigation strategy that has the potential to benefit both Ahpra and the individual/s affected.

While disclosure is an important mitigation strategy, it will not always be an appropriate response to a breach. Providing disclosure about low risk breaches can cause undue anxiety and de-sensitise individuals to disclosure. Each incident needs to be considered on a case-by-case basis to determine whether a disclosure is required.

Prompt disclosure to individual(s) in the event of a serious privacy breach can help them mitigate the damage by taking steps to protect themselves.

In determining whether to disclose the data breach the assigned employee will consider:

- the level of harm to the individual;
- the ability of the individual to take specific steps to mitigate any such harm;
- whether it is appropriate to inform the NHPOPC and other third parties such as, the police or other law enforcement agencies, cyber security agencies, other regulators, professional bodies about the data breach; and
- 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?

If the assigned employee forms the opinion that it is in the interests of the affected individual(s) not to disclose the breach, they must liaise with Corporate Legal. If Corporate Legal agrees, then the serious incident report should be endorsed that a decision was made not to disclose the breach including the reasons for the decision.

In all other cases (other than in the event of an eligible data breach) both the affected party and the recipient of the information will be advised by a letter from the National Director.

Use *Template Letter Advising of a Privacy Breach* (**Attachment 4**).

3.3.3. Where the affected individual makes a complaint

If a complaint is made by an affected individual, Corporate Legal must be informed in order to enter the details into the complaints database. Other relevant employees will also be informed

depending on the nature of the breach, in accordance with the Serious Incident Communications Matrix (contained in the Critical Incident Management Plan).

The NE in its form as the Critical Incident Management Team will determine whether it is appropriate to inform the NHPOPC where such a complaint has been made (if this has not already occurred).

4. Reflect & Implement

4.1 The Serious Incident Report must be completed within 20 business days of the discovery of the breach and must include a conclusion of how the breach occurred (i.e. if it was a systemic or human error) and any proposed remedial actions.

4.2 The National Director will decide whether a further investigation is required to ascertain the causes of the breach and the actions necessary to prevent further breaches.

4.3 A review of the implementation of the actions will be scheduled for a reasonable period after the breach in order to ascertain compliance.

Definitions

Term	Definition
Ahpra Employee	A person employed directly with Ahpra in a permanent ongoing role, on a temporary or fixed term contract, or on a casual basis.
Notifiable Data Breach Scheme	The Part IIIC of *The Privacy Act 1988* (Cth) incorporates a mandatory data breach notification scheme. The scheme requires agencies to notify individuals if a privacy breach relating to their personal information is likely to result in serious harm. The main purpose of the scheme is to reflect community expectations that agencies are accountable for privacy protection, and to permit individuals to take steps to reduce their risk of harm in the event of an eligible data breach.
Line Manager	An Ahpra employee who supervises Ahpra Employees and who has authority to escalate a breach directly to the National Director.
Personal Information	'Personal information' is defined in s 6 of *The Privacy Act 1988* (Cth) to mean 'information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in material form or not.

Document control

Approver	National Executive
Procedure Number	
Date Approved	11 May 2021
Date Commenced	11 May 2021
Date for Review	11 May 2022
Policy Owner	Executive Director, Regulatory Operations
Sections modified	19 October 2020: o Role titles amended in line with organisational restructure o Changes made to accommodate new online form for serious incidents 17 December 2020: o Removal of references to Senior FOI and Privacy Employee and replaced with Corporate Legal; and Tidy up of language throughout the Procedure. 11 May 2021: o Review and re-draft of procedure to simplify process and incorporate feedback from NHPOPC.

Attachment 1: Response to Breach of Privacy Worksheet

Date of Breach:

Affected individual/s:

Assigned employee:

No	Action	Notes	Date completed
1.	Immediate initial assessment		
2.	Contain the breach		
3.	Inform Line Manager		
4.	Line Manager assigns to assigned employee		
5.	Assess whether special circumstances apply		
6.	Assess whether eligible data breach		
7.	Disclose to affected individual/s		
8.	Determine root cause		
9.	Implement remedial actions and set date for review		

Attachment 2: Template initial email to Line Manager notifying of breach (with example of the type of information to include)

To: My Line Manager

CC: National Director; National Director, Organisational Risk and Resilience; Corporate Legal

Subject: **Re Breach of Privacy** - SURNAME, First Name - **Occurred** Date - **Discovered** Date

Dear [name],

This is an initial notification of a potential breach of privacy.

The facts are:

[here provide a chronology of events - date first text second e.g.

01.06.12 letter generated from registration to registrant requesting further information about qualifications;

02.06.12 letter to registrant sent to old address.

At this stage I have confirmed that:

The letter sent to the registrant's former address is likely to result in a breach of privacy if opened by the new occupants.

I was not the Ahpra employee who sent the letter

I recommend that:

I *[or another employee]* be appointed to resolve the breach and undertake the steps outlined in the Procedure to Respond to a Breach of Privacy.

Attachment 3: Template letter for retrieving information that has been disclosed

[Insert contact details and date]

Dear [XX]

Re: Inadvertent release of information

Thank you for advising Ahpra that you have received information relating to [YY].

I confirm our discussion via telephone of [insert date] that you have returned the documents to Ahpra / not retained any copies either in hard or electronic form / destroyed or deleted the information.

I sincerely apologise for your becoming involved in the breach of the privacy of another practitioner/ I sincerely apologise for your becoming involved in this breach of privacy [if the recipient is not a practitioner].

Ahpra is committed to managing its processes in line with our privacy policy and with the *Privacy Act 1988* (Cth). I also want to assure you that remedial actions have been implemented to significantly reduce the likelihood of this occurring again.

Yours sincerely

Attachment 4: Template letter advising of a privacy breach

[Insert contact details and date]

Dear [XX]

Re: Potential breach of your privacy

The purpose of this letter is to inform you of a potential breach of your privacy.

[provide details of the breach of privacy e.g. chronology of letters etc. and the response to recover the breach]. If this is a mandatory notification the letter must contain the information set out in part 3.3 'Statement requirements' of the Procedure to Respond to a Breach of Privacy

I sincerely apologise for this administrative oversight. I also want to assure you that remedial actions have been implemented to significantly reduce the likelihood of this occurring again.

You have a right to make a complaint to the National Health Practitioner Ombudsman and Privacy Commissioner in relation to this matter. The Commissioner may be contacted as follows:

in writing – to the National Health Practitioner Ombudsman and Privacy Commissioner,

Level 2, 50 Lonsdale Street Melbourne, Victoria, 3000.

by telephone – 1300 795 265

via email – complaints@nhpopc.com.au

or by downloading a complaint form from the website www.nhpopc.gov.au. Should you wish to discuss this matter further, please contact

Yours sincerely