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 privacy breach) and provides direction to Ahpra Officers 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

- Serious Incident Report
- Privacy Statement
- Privacy Policy
- Staff Privacy Guide

Relevant legislation

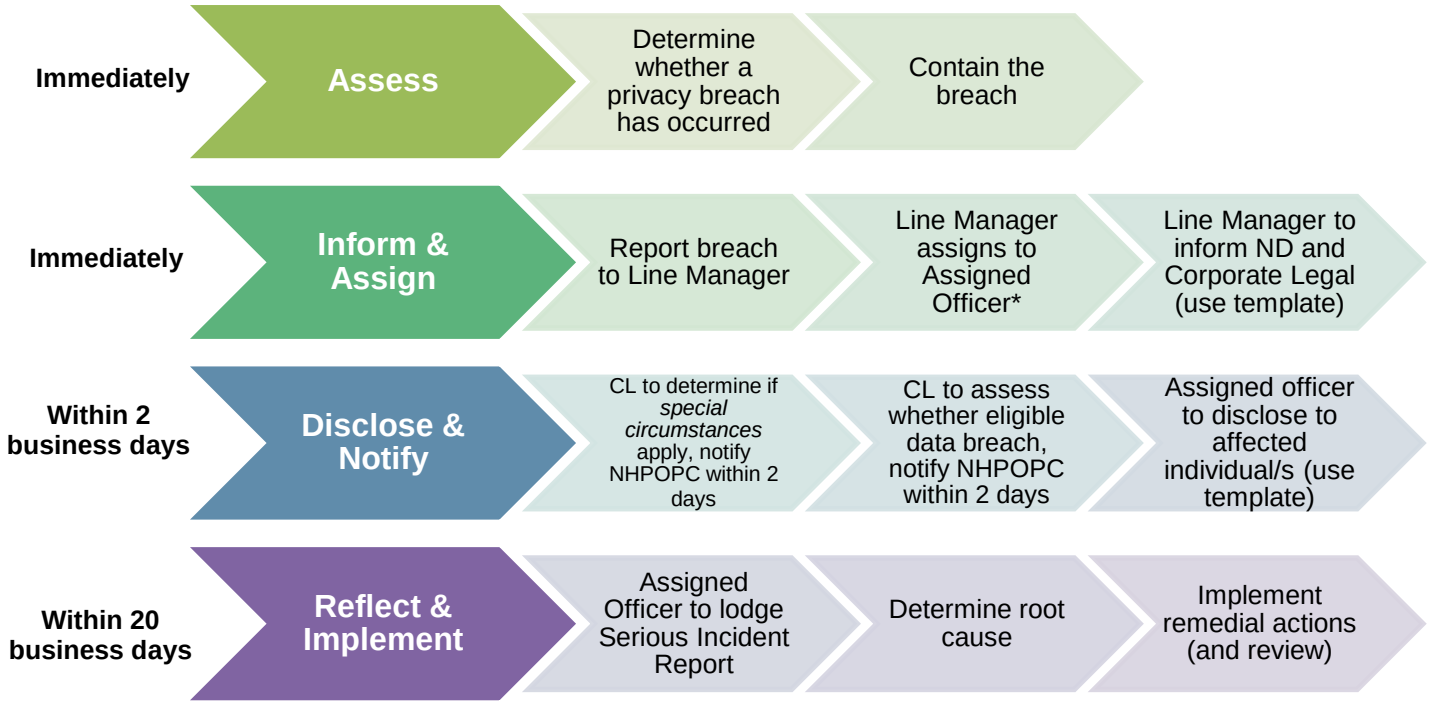
- *Health Practitioner Regulation National Law* (as in force in each State and Territory)
- *Privacy Act 1988* (Cth)

Procedure

Overview

The following is a summary of the steps that must be taken in response to any privacy breach or suspected privacy breach in line with the timeframes set out in the diagram below. Each of these steps is explained in detail in the Procedure.

The steps outlined in the Procedure will often be undertaken concurrently.



* The Assigned Officer should be the manager of the team where the breach occurred.

Assess

1. Determine whether a privacy breach has occurred

1.1. The Ahpra Officer 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.

1.2. As part of the initial assessment the Ahpra Officer 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 by emailing corporate.legal@ahpra.gov.au.

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

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 officer 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.

1.4. When disclosing personal information, Ahpra staff must consider whether the disclosure is permitted or authorised under the *Health Practitioner Regulation National Law* (as in force in each State and Territory) (the **National Law**) and/or the *Privacy Act* 1988 (Cth).

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

- 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 containing 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.

1.6. A privacy breach 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.

Inform

2. Report breach to Line Manager

2.1. The Ahpra Officer must immediately report the privacy breach to their Line Manager via email.

2.2. The email must contain as much information as possible, including:

- the time and date of the privacy breach or the suspected privacy breach (copies of relevant correspondence/documents to be attached);
- the time and date the privacy breach or suspected data breach was discovered;
- the type of personal information involved;
- the cause and extent of the privacy breach;
- the actions undertaken to contain the privacy breach; and
- whether any of the *special circumstances* listed in section 7.2 apply.

Use *Initial Email to Line Manager Notifying of Breach Template* (**Attachment 1**).

Contain

3. Contain the breach

3.1. The immediate priority is to contain the privacy breach. The Ahpra Officer who discovers the privacy breach or is otherwise alerted to a privacy breach should complete this step immediately or immediately after reporting the privacy breach to their Line Manager.

3.2. Containing the breach may include stopping the unauthorised practice, shutting down a system that was breached, addressing security weaknesses or retrieving information from a third party.

3.3. If the privacy breach relates to information being sent to a third party, the Ahpra Officer must contact the third-party recipient by the fastest means possible (telephone/email). The third-party recipient must be informed of the privacy breach and asked to return or destroy the information, or to delete any electronic records without first reading, making copies or forwarding them to any other party.

3.4. A verbal request must be followed by written correspondence to the third party asking them to confirm that they have not retained any copies of the information and have destroyed / deleted the information in their possession.

3.5. Sometimes privacy breaches are not discovered immediately. If this occurs, the Assigned Officer (refer to section 5) must consult with Corporate Legal via email (Corporate.Legal@ahpra.gov.au) about the best way to contain the privacy breach.

Use *Template Email for Retrieving Information that has been Disclosed*

Ahpra notified recipient of the breach (**Attachment 2**).
Recipient notified Ahpra of the breach (**Attachment 3**).

3.6. Where necessary and feasible, steps must be taken to prevent further release of personal information. If this involves securing or shutting down breached systems or revoking or changing computer access

codes, the Assigned Officer (in collaboration with the National Director Organisational Risk & Resilience or Corporate Legal) will contact the IT Security Manager and ensure the shutdown/changes occur as soon as possible.

3.7. 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 auditing relevant computer systems. If there is any doubt as to the evidence that ought to be kept seek advice from Corporate Legal.

3.8. To determine what other steps might be immediately necessary, the Assigned Officer will assess the risks associated with the privacy breach including seeking advice from Corporate Legal and/or the National Director Organisational Risk & Resilience. The Assigned Officer should take 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 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– this might cause difficulties in personal or professional relationships and put the person whose privacy was breached at risk;
- whether the breach occurred once or on multiple occasions;
- whether the breach has been stopped if there is any potential for ongoing breach;
- whether the information disclosed was encrypted or otherwise protected;
- the number of individuals affected;
- whether the privacy breach was caused by a systemic problem or an isolated incident; and
- what steps have been taken to deal with the harm.

Inform

4. Line Manager to report breach

4.1. Upon being informed of the privacy breach, the Line Manager must immediately inform (via email) the National Director; Corporate Legal and National Director, Organisational Risk and Resilience.

4.2. The email must contain as much information as is available and address the same points outlined in section 2.2.

Use *Email to National Director(s) and Corporate Legal Notifying of Breach Template* (**Attachment 4**).

Assign

5. Line Manager to assign an Ahpra Officer to respond

5.1. The Line Manager must assign responsibility for responding to the privacy breach to an Ahpra Officer (**Assigned Officer**) by emailing the Assigned Officer. The Assigned Officer should be the manager of the team responsible for causing the privacy breach but must **not** be the staff member who was responsible for the privacy breach.

5.2. The Assigned Officer will conduct a preliminary investigation into the circumstances of the privacy breach and will liaise with Corporate Legal for guidance and assistance. This investigation must be conducted as expeditiously as possible.

5.3. The Assigned Officer must undertake this responsibility on an urgent basis as a priority to other work. The Assigned Officer is expected to exercise professional judgment and the assignment ought to be declined if other work cannot be rescheduled.

5.4. The Assigned Officer will create a separate file in Content Manager, named as '[Affected person Surname], [First name] – Breach of Privacy'.

5.4.1. The file should be created in the matter where the breach occurred. For example, if a privacy breach occurred in respect of a registration or notification matter, the sub-folder should be created within that registration application matter or notification matter. The following steps can be taken to create a folder in Content Manager:

> Right click on the applicable parent folder > select "*New*" > select "*New Record*" > a Dialogue box will appear, select "*Folder Divider for Corporate Folder*" > label the folder as *'[Affected person Surname] [First name] – Breach of Privacy*'

5.5. At all stages, contemporaneous notes should be kept together with all emails and other documents to ensure a complete record of the privacy breach response is available for review and auditing.

> Use *Response to Breach of Privacy Worksheet Template* (**Attachment 5**), copy into the file and rename appropriately. This worksheet must be kept up to date in the file.

6. Discuss NHPOPC notification

6.1. Ahpra has an obligation to notify the NHPOPC within two business days of the existence of a special circumstance or an eligible data breach. Therefore, it is imperative that the initial email to the Line Manager and Corporate Legal (refer to sections 2 and 4) set out all the relevant circumstances.

6.2. The assessment of the privacy breach (as either an eligible data breach or one where a special circumstance applies) will be undertaken by Corporate Legal.

7. Does a special circumstance apply?

7.1. As detailed in section 2.2, the Ahpra Officer who discovers or is otherwise alerted to a privacy breach must consider whether a *special circumstance* applies and include this analysis in the initial email to their Line Manager.

7.2. 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).

Disclose & Notify

7.3. If a special circumstance is determined by Corporate Legal to exist, Corporate Legal must disclose the privacy breach to the NHPOPC within two business days.

7.4. All correspondence to the NHPOPC will be drafted and sent by Corporate Legal.

8. 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.

8.1. *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).

8.2. *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 privacy breach is an eligible data breach, it should be treated as such.
- Where Ahpra has taken reasonable steps to contain the privacy 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 privacy 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.

8.3. Corporate Legal will determine if there are reasonable grounds to believe that the privacy breach constitutes an eligible data breach, in which case disclosure must be made to the NHPOPC within two business days.

Disclose & Notify

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

8.4.1. Prepare a statement (**Statement**) that complies with the requirements set out below and give a copy of the Statement to the NHPOPC within two business days after it becomes so aware.

8.5. The Statement must set out:

8.5.1. the identity and contact details of Ahpra;

8.5.2. a description of the eligible data breach that Ahpra has reasonable grounds to believe has happened;

8.5.3. the kind(s) of information concerned;

8.5.4. recommendations about the steps that individuals should take in response to the eligible data breach; and

8.5.5. if another entity is involved in the privacy breach, the identity and contact details of that entity.

Disclose & Notify

9. Disclose to affected individual/s

Where the breach is an eligible data breach

9.1. Where the privacy breach is an eligible data breach the Assigned Officer must notify the affected individual/s within two business days after becoming aware of the breach. The affected party will be advised by a letter signed by a National Manager.

> Use *Template Letter Advising of a Privacy Breach* (**Attachment 6**).

9.2. The notification to the affected individual should also advise them of the Statement made to the NHPOPC (refer to section 8.5). The letter to the affected party should:

9.2.1. if practicable, take reasonable steps to notify them of the contents of the Statement; or

9.2.2. if practicable, take reasonable steps to notify them of the contents of the Statement if the privacy breach is an eligible data breach; or

9.2.3. if neither section 9.2.1 or 9.2.2 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.

9.3. 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.

9.4. The outcome of this confirmation is to be noted on the Serious Incident Report prepared by the Assigned Officer.

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

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

9.6. While disclosure is an important mitigation strategy, it will not always be an appropriate response to a privacy 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.

9.7. Prompt disclosure to individual(s) in the event of a serious breach of privacy can help them mitigate the damage by taking steps to protect themselves. In determining whether to disclose the privacy breach the Assigned Officer will consider:

9.7.1. the level of harm to the individual;

9.7.2. the ability of the individual to take specific steps to mitigate any such harm;

9.7.3. 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 or professional bodies about the data breach; and

9.7.4. 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?

9.8. If the Assigned Officer forms the opinion that it is in the interests of the affected individual(s) not to disclose the privacy 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 privacy breach to the affected individual(s) including the reasons for the decision.

9.9. Subject to section 9.8, both the affected party and the recipient of the information will be advised by a letter signed by a National Manager.

Use *Template Letter Advising of a Privacy Breach* (**Attachment 6**).

Where the affected individual makes a complaint

9.10. 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 officers 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).

9.11. The National Executive 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).

Reflect & Implement

10. Reflect & Implement

10.1. The Assigned Officer must lodge a Serious Incident Report (SIR) within 20 business days of discovering the privacy breach which must include:

10.1.1. the time and date of the privacy breach or the suspected privacy breach;

10.1.2. the time and date the privacy breach or suspected privacy breach was discovered;

10.1.3. the type of personal information involved;

10.1.4. the cause and extent of the breach;

10.1.5. a complete list of persons involved in the breach, including their position and contact details;

10.1.6. the corrective actions identified or implemented and the Ahpra Officer responsible for the corrective actions;

10.1.7. a conclusion of how the breach occurred (i.e. if it was a systemic or human error);

10.1.8. whether a disclosure was made to the NHPOPC or the affected individual(s); and

10.1.9. any proposed remedial actions.

10.2. 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.

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

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

Definitions

Term	Definition
Ahpra Officer	A person employed directly with Ahpra in a permanent ongoing role, on a temporary or fixed term contract, or on a casual basis.
Assigned Officer	The Assigned Officer is an Ahpra employer who is responsible for responding to the breach of privacy. The Assigned Officer must not be the officer who was apparently responsible for the breach.
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.
Line Manager	An Ahpra employee who supervises Ahpra Officers and who has authority to escalate a breach directly to the National Director.
National Health Practitioner Ombudsman and Privacy Commissioner (NHPOPC)	Provides oversight of bodies in the National Registration and Accreditation Scheme (National Scheme), including Ahpra and the 15 National Boards.
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.
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	19 October 2020
Date Commenced	19 October 2020
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 Officer and replaced with Corporate Legal; and Tidy up of language throughout the Procedure. 9 April 2021: o Review and re-draft of procedure to simplify process and incorporate feedback from NHPOPC. 23 February 2022 o Amend the signatory of the letters to the affected party and the recipient of the information from the National Director to a National Manager to increase efficiencies 28 March 2022 o Review and re-draft of procedure to clarify the steps in the process and incorporate feedback from the Notifications function areas, including but not limited to: o the level of detail to include in emails informing Line Manager, Corporate Legal, National Directors of the breach of privacy; o clarification of the timeframes to notify the NHPOPC and the affected individual(s); o the level of detail to include in the SIR; o definition section; and o review of the language in the accompanying attachments. 4 August 2022 o amendments to Attachment 6 to include prompts re: steps affected party should take, and remedial actions implemented by Ahpra.

Attachment 1: Template initial email to Line Manager notifying of breach (with example of the type of information to include)

To: My Line Manager

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:

[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. The letter included the full name, residential address and email address of the registrant.

I was not the Ahpra officer who sent the letter.

I have not taken further steps at this time to contain the breach.

I have reviewed the special circumstances listed in section 7.2 of Procedure to Respond to a Breach of Privacy (**Procedure**) and confirm that [*no special circumstances apply / the following special circumstance applies {insert applicable item(s) from section 7.2}*].

I recommend that:

I *[or another officer]* be appointed to resolve the breach and undertake the steps outlined in the Procedure.

In line with the Procedure, please notify the National Director and Corporate Legal.

Yours faithfully,

Attachment 2: Template email for retrieving information that has been disclosed (Ahpra notified recipient of the breach)

[Insert contact details and date]

Dear [XX]

Re: Inadvertent release of information

As discussed with you via telephone on [*insert date*] [*an email / a letter*] was sent to in error.

I confirm our discussion that [*you have returned the documents to Ahpra / not retained any copies either in hard or electronic form / destroyed or deleted the information / have not shown or forwarded the document to another person.*]

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 3: Template email for retrieving information that has been disclosed (recipient notified Ahpra of the breach)

[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 on [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 email notification to National Director; Corporate Legal and National Director Organisational Risk & Resilience notifying of breach (with example of the type of information to include)

To: National Director; Corporate Legal; National Director Organisational Risk & Resilience

From: Line Manager

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:

[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:

[*e.g. 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 officer who sent the letter and have been notified by [insert name of the person who discovered the breach / author of Attachment 2].

At this stage, we believe that [*no special circumstances as listed in section 7.2 of Procedure to Respond to a Breach of Privacy (**Procedure**) apply / the following special circumstance applies {insert applicable item from section 7.2} as listed in section 7.2 of Procedure to Respond to a Breach of Privacy (**Procedure**) applies*].

I [*or another officer (cc'ed into this correspondence)*] have been appointed as the Assigned Officer to resolve the breach and undertake the steps outlined in the Procedure.

Yours sincerely

Attachment 5: Response to Breach of Privacy Worksheet

Date of Breach:

Affected individual/s:

Assigned officer:

No	Action	Notes	Date completed
1.	Immediate initial assessment		
2.	Inform Line Manager		
3.	Contain the breach		
4.	Line Manager assigns to Assigned Officer		
5.	Line Manager informs National Directors and Corporate Legal		
6.	Assigned officer begins investigation		
7.	Corporate Legal assess whether special circumstances apply		
8.	Corporate Legal assess whether eligible data breach		
9.	Disclose to affected individual/s		
10.	Determine root cause		
11.	Implement remedial actions and set date for review		
12.	Lodge Serious Incident Report		

Attachment 6: Template letter to affected individual(s) 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 section 9 'Statement requirements' of the Procedure to Respond to a Breach of Privacy].

I sincerely apologise for this *[administrative oversight/error].* I also want to assure you that remedial actions have been implemented to significantly reduce the likelihood of this occurring again. Specifically, *[provide details of the remedial action that has been taken to minimise the risk of this type of breach occurring again].*

In order to protect your information, it is recommended that you take the following steps:

- *[explain the steps the individual should take in response to the breach – e.g. changing account passwords or being alert to possible scams resulting from the breach]*

[OR if no action is recommended]: You are not required to take any steps in response to this correspondence.

You have a right to make a complaint to the National Health Practitioner Privacy Commissioner, who is also the National Health Practitioner Ombudsman. Please see the office's contact details below. You can also find out more about making a privacy complaint to the Commissioner here: https://www.nhpo.gov.au/commissioner-complaints.

Contact details

Phone: 1300 795 265 (a translating and interpreting service is available via 131 450)

Office hours are 9:00am to 5:00pm AEST, Monday to Friday (excluding public holidays). A voicemail service is also available.

Online complaint form: https://www.nhpo.gov.au/make-a-complaint-to-the-commissioner

Email: complaints@nhpo.gov.au

Post: National Health Practitioner Ombudsman, GPO Box 2630, Melbourne, Victoria, 3001

Should you wish to discuss this matter further, please contact <INSERT AHPRA STAFF MEMBER CONTACT DETAILS.>

Yours sincerely

National Manager