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 officers as to 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 which commenced on 22 February 2018 (the "Notifiable Data Breach Scheme"). Under this scheme, AHPRA is required by law to notify the National Health Practitioner Ombudsman and Privacy Commissioner (NHPOPC) (**Commissioner**) and individual/s affected by a data breach that is likely to result in serious harm (an "eligible data breach").

This procedure sets out how to identify and respond to a privacy breach and covers the additional steps that must be taken in accordance with the Notifiable Data Breach Scheme to respond if the incident is determined to be an eligible data breach.

Related documents

- Response worksheet
- Template emails and letters
- Serious Incident Report Templates
- 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

The following steps will happen in response to any privacy breach.

1 Immediate initial assessment

1.1 The officer who discovers or is otherwise alerted to what may be a breach of privacy must undertake an immediate initial assessment to determine if a breach may have occurred.

1.2 As part of the initial assessment the 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, the officer will seek advice from Business Services Legal.

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

1.4 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. Typically the most common privacy breaches happen when an individuals' personal information is stolen, lost or mistakenly disclosed. Privacy breaches can also include, for example, 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.

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

1.6 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.

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

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

2 Inform Line management

2.1 The AHPRA Officer will immediately report the breach to your immediate supervisor via email and copy in their State/Territory Manager or National Director.

2.2 The Initial Email to Line Management Notifying of Breach Template will be used.

3 Senior line management to assign an AHPRA officer to respond

3.1 The responsible State/Territory Manager or National Director will assign to an AHPRA Officer the responsibility of responding to the breach as per this procedure ('the assigned officer'). This will take the form of a reply to the initial email. The assigned officer will not be the officer who was apparently responsible for the breach.

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

3.3 The assigned officer must seek confirmation from the Senior FoI, Privacy and Complaints Officer as to whether the breach is (or may be) an "eligible data breach" under the Notifiable Data Breach Scheme. The relevant factors that the Senior FOI, Privacy and Complaints Officer will consider in determining whether there is or may have been an eligible data breach are outlined below.

What 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 (such as 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: in the event of uncertainty as to whether a breach is an eligible data breach, it should be treated as such.

NOTE: 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" for the purposes of the Act.

NOTE: Where the breach relates to a contracted service provider or involves another third party, Business Services Legal should be contacted to determine whether there are any additional obligations (including contractual obligations) relating to managing the breach.

Notification obligations for an "eligible data breach"

If AHPRA is aware that there are reasonable grounds to believe that there has been an eligible data breach, AHPRA must:

1. Prepare a statement ("Statement") that complies with the requirements set out below, and give a copy of the Statement to the Commissioner 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 or kinds 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.

2. Notify the affected individual/s in compliance with the requirements set out below, as soon as practicable after 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 statement.

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

If in doubt regarding AHPRA's legislative obligations with respect to an "eligible data breach", please contact the Director, People Programmes, Risk and Compliance or Business Services Legal.

3.4 The outcome of this confirmation is to be noted on the Serious Incident Form prepared by the assigned officer in accordance with step 7 of this procedure.

3.5 The Senior FoI, Privacy and Complaints Officer 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 officer to complete the Serious Incident Report in accordance with this procedure, and notify the affected individual/s in accordance with the legislative requirements set out above. **NOTE: No notification documentation is to be sent outside of AHPRA until advice has been sought from Business Services Legal, and approval granted by the National Executive.**

- if there are reasonable grounds to suspect that an eligible data breach *may* have occurred, in which case they will work with the assigned officer to complete a further reasonable and expeditious assessment following step 7 of this procedure to determine whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach. This further assessment will be completed as soon as practicable, and in no event will take longer than 30 days.

4 Document

4.1 The assigned officer 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.

4.2 The Response to Breach of Privacy Worksheet Template will be copied into the file and renamed appropriately. This worksheet will be kept up to date in the file.

5 Contain the breach

5.1 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.

5.2 The third party recipient of any personal information will be contacted by the fastest means possible via telephone or email or mail and 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.

5.3 A verbal request will be followed by correspondence to the third party asking to confirm that they have not retained any copies of the information in their possession. The Template Letter for Retrieving Information that has been Disclosed will be used.

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

5.5 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 Business Services Legal.

5.6 To determine what other steps might be immediately necessary, the assigned officer will (in collaboration with the Director, People Programmes, Risk and Compliance 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.

6 Disclosure and Apology

6.1 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 individuals affected.

6.2 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 breach disclosure is required.

Usually, if a data breach is serious, the affected individual/s should be advised, even if the breach is not an 'eligible data breach'

6.3 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.

6.4 In determining whether to disclose the data breach the assigned officer will take into account:

- 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 Commissioner and other third parties such as , the police or other law enforcement agencies, cyber security agencies or other regulators or professional bodies or the media 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 a data breach is an "eligible data breach" under the Notifiable Data Breach Scheme, AHPRA is required by law to notify the affected individual/s. Step 3 above sets out the additional notification steps to be taken by the assigned officer in collaboration with the Director, People Programmes, Risk and Compliance in the event of an "eligible data breach".

6.5 If the assigned officer forms the opinion that it is in the interests of the affected individual(s) **not** to disclose the breach, they must liaise with the Senior FoI, Privacy and Complaints Officer. If the Senior FoI Privacy and Complaints Officer agrees, then the serious incident reports should be endorsed that a decision was made not to disclose the breach including the reasons for the decision.

6.6 In all other cases (other than in the event of an "eligible data breach", in which step 3 of this procedure will apply) both the affected party and the recipient of the information will be advised by a letter from the State or Territory Manager (or the National Director as the case may be) as per the Template Letter Advising of a Privacy Breach.

7 Investigation and briefing

7.1 The assigned officer 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 Notifiable Data Breach Scheme) will liaise with the Senior FoI, Privacy and Complaints Officer 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 - Part 1 (initial) brief to the line Manager or Director, who will in turn brief the State or Territory Manager or National Director and copy in Business Services Legal. A template report set out at http://intranet/Corporate-Services/Risk-management/Resources-and-forms.aspx. The Part 1 brief will have as attachments draft letters to the affected registrant and the recipient of the information, or in the event of an "eligible data breach", the prepared statement and associated notification documentation.

7.2 The Part 1 brief will be completed and delivered to the State or Territory Manager or National Director within 2 working days of the discovery of the breach.

7.3 The assigned officer will then conduct an evaluation of the breach and author a Serious Incident Part 2 (investigation) brief (also at http://intranet/Corporate-Services/Risk-management/Resources-and-forms.aspx) to their Line Manager or Director who will in turn brief the State or Territory Manager or National Director and copy in Business Services Legal. The Part 2 brief will be completed within 10 working days of the discovery of the breach. It will include a conclusion of how the breach occurred –was it a systemic or human error. It will also outline any proposed remedial actions.

8 Reporting

8.1 The line Manager or Director, who receives the Part 1 report (see 7.2) will in turn brief the State or Territory Manager or National Director and copy in Business Services Legal.

8.2 The State or Territory Manager or National Director will ensure that the letters to the affected registrant and the recipient of the information are signed and sent.

8.3 The State or Territory Manager or National Director will report the breach by emailing the Serious Incident Report Part 1 and 2 to RiskManagement@ahpra.gov.au.

8.4 If a complaint is made by an affected person, the Senior FoI, Privacy and Complaints Officer will 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, for example the Director, Environment. Connectivity and Support Services , Director,

People Lifecycle Services and other Senior Management in accordance with the Serious Incident Communications Matrix (contained in the Critical Incident Management Plan).

8.5 The NE in its form as the Critical Incident Management Team will determine whether it is appropriate to inform the Commissioner and other third parties such as , the police or other law enforcement agencies, cyber security agencies or other regulators or professional bodies or the media about the data breach

9 Action

9.1 The State or Territory Manager or National Director will decide whether or not a further investigation is required to ascertain the causes of the breach and the actions necessary to prevent further breach.

9.2 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 Officer	A person employed directly with AHPRA in a permanent ongoing role, on a temporary or fixed term contract, or on a casual basis.
Eligible Data Breach	AHPRA is required by law to notify the Commissioner and individual's affected by a data breach that is likely to result in serious harm.
Notifiable Data Breach Scheme	The Part IIIC of *The Privacy Act 1988* (Cth) incorporates a mandatory data breach notification scheme that came into force on 22 February 2018. The scheme requires agencies to notify individuals in the event that 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 Management	An AHPRA employee who supervises AHPRA Officers and who has authority to escalate a breach directly to the State/Territory Manager or 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.'
Protected Information	'Protected information' is defined in sec 214 the National Law as *"information that comes to a person's knowledge in the course of, or because of the person exercising functions under this law"* Section 216 of The National Law establishes a duty of confidentiality that applies to a person *'exercising functions under the Law'* and *'must not disclose to another person protected information'*, except in limited circumstances set out in the National Law.

Document control

Approver	
Policy Number	
Date Approved	
Date Commenced	
Date for Review	
Policy Sponsor	
Sections modified	

ATTACHMENTS (to be uploaded to the Intranet)

Attachment 1 - Response to Breach of Privacy Worksheet

Registrant: Date of Breach
Assigned officer:

No	Action	Reference	Notes	Completed
1	Immediate initial assessment	1.1, 1.2		
2	Inform senior management	2.1, 2.2 Email to Line Management Notifying of Breach Template used		
3	Senior line management to assign an AHPRA officer to respond	3.1, 3.2		
4	Document	4.1, 4.2 Response to Breach of Privacy Worksheet Template used		
5	Contain the breach	5.1 to 5.4 Template Letter for Retrieving Information that has been disclosed used		
6	Disclosure and apology	6.1, 6.2 Template Letter Advising of a Privacy Breach used		
7	Investigation and briefing	7.1 – 7.3		
8	Reporting	8.1 - 8.3		
9	Action	9.1		

Attachment 2

Template emails and letters

Initial email to line management notifying of breach (with example of the sort of information to include)

To: My line manager

CC: Director for my State/Territory or National Director; Director, People Programmes, Risk and Compliance; Business Services 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 eg

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 officer who sent the letter

I recommend that:

I *[or another officer]* be appointed to resolve the breach and undertake the Response to a Privacy Breach Procedure.

Template letter for retrieving information that has been disclosed

[Ins 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

[National Director or State Manager]

Template letter advising of a privacy breach

[Ins contact details and date]

Dear [ ]

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 eg 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:

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

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

2. by telephone – 1300 795 265

3. via email – complaints@nhpopc.com.au

4. 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

Attachment 3

Serious Incident Report Templates Part 1 and 2 can be located at http://intranet/Corporate-Services/Risk-management/Resources-and-forms.aspx