Australian Government
National Health and Medical Research Council

BUILDING
A HEALTHY
AUSTRALIA

NHMRC Response Plan for data breaches involving personal or sensitive information

NHMRC

Publication Details

Publication title:	NHMRC Response Plan for data breaches involving personal or sensitive information
Published:	May 2018 v1.1 updated March 2022
Publisher:	National Health and Medical Research Council
NHMRC Publication reference:	PR4
Online version:	www.nhmrc.gov.au/guidelines/publications/PR4
ISBN Online:	978-1-86496-022-8
Suggested citation:	NHMRC Response Plan for data breaches involving personal or sensitive information, Canberra: National Health and Medical Research (2018) v1.1 updated March 2022

Copyright

Contact us

To obtain information regarding NHMRC publications or submit a copyright request, contact:

E: nhmrc.publications@nhmrc.gov.au

or call (02) 6217 9000

NHMRC Response Plan for data breaches involving personal or sensitive information

Introduction

NHMRC is committed to protecting the privacy of its officials and stakeholders. An overview of how NHMRC collects, stores and uses personal and sensitive information[1] is provided in the NHMRC Privacy Policy.

NHMRC has a number of controls in place for the collection, storage and use of personal and sensitive information, which aim to protect this information from loss or unauthorised use or disclosure. Controls are also in place to enable NHMRC to promptly identify **data breaches**. Should NHMRC become aware of, or suspect, a data breach, NHMRC will act to mitigate the breach and, where possible, take remedial action to reduce the potential for serious harm to the affected individuals. In the event of an **eligible data breach**, NHMRC will (in accordance with the *Privacy Act 1988* (Privacy Act)) promptly notify the affected individual/s and the Australian Information Commissioner.

For the purposes of this Response Plan:

- A '**data breach**' is any unauthorised access to or unauthorised disclosure of personal or sensitive information, or a loss of personal or sensitive information, that NHMRC holds.
- an '**eligible data breach**' occurs when three criteria are met:
  - There is unauthorised access to, or unauthorised disclosure of personal information, or a loss of personal information, that NHMRC holds,
  - This is likely to result in serious harm to one or more individuals, and
  - NHMRC has not been able to prevent the likely risk of serious harm with remedial action[2].

This Response Plan outlines the responsibilities and actions to be taken in the event of a known or suspected data breach involving personal or sensitive information. It is reviewed periodically for currency and relevance.

1 For the purposes of this Response Plan, *Personal information* and *sensitive information* have the same meaning as defined in section 6(1) of the Privacy Act. This definition is also detailed in the NHMRC Privacy Policy.

2 See Section 26WE of the Privacy Act.

Background

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* amended the Privacy Act to establish the Notifiable Data Breaches (NDB) scheme in Australia. It applies to all agencies and organisations with personal information security obligations under the Privacy Act.

The NDB scheme introduced an obligation to notify individuals whose personal information is involved in a data breach that is **likely to result in serious harm**[3].

Privacy Responsibilities at NHMRC

All NHMRC staff should familiarise themselves with the Australian Privacy Principles (APPs) and the NHMRC Privacy Policy. The APPs must be complied with, through individual actions and organisational practices. Breaching an APP is interference with the privacy of the individual. Serious or repeated interference with a person's privacy by an APP entity (like the NHMRC) incurs a civil penalty of 2,000 penalty units which is $420,000 (subject to an indexation formula)[4].

NHMRC will respond to all data breaches on a case-by-case basis, and do so promptly to minimise any adverse impact on an individual. The Executive Director of the Research Quality & Priorities Branch is NHMRC's **Privacy Champion**. The Privacy Champion will review the causes of all data breach/es and any relevant practices and policies, and report to the General Manager and to the Chief Executive Officer.

The details of all data breaches, including investigations into their cause and effect and any remedial action taken, will be recorded by the **Privacy Officer/s** to support the regular review of NHMRC's privacy policies and practices.

This Response Plan is available on the NHMRC website for the information of all officials and stakeholders. This is consistent with NHMRC's obligations under the Information Publication Scheme requirements of the *Freedom of Information Act 1982*.

NHMRC may take action under the *Public Service Act 1999* in relation to an NHMRC official for any deliberate or repeated breaches of the APPs.

Key Steps in responding to a suspected Data Breach

Prompt internal reporting

Any staff member who becomes aware of, or suspects, a data breach must promptly report the data breach to their Director, Executive Director **and** the ITSA[5].

The minimum information that is to be provided is:

- incident description including the time and circumstances of the breach
- type of personal information involved

3 Exceptions do apply in limited circumstances– see for example sections 26WF, 26WN and 26WP of the Privacy Act. See *Attachment A* for more information.

4 See section 13G of the Privacy Act.

5 Via itsa@nhmrc.gov.au.

- whether an IT or communication system is involved
- number of affected individual/s
- reporter's assessment of the cause of the breach and the impact on the individual/s and NHMRC
- whether the affected individual/s are aware of the data breach issue
- a summary of any remedial action already taken and the outcome/impact of this action.

The ITSA will then report all instances involving personal information to the Privacy Officer/s[6].

> Regardless of perceived severity, **all** data breaches **must** be promptly reported. NHMRC centrally records **all** data breaches in accordance with its obligations under the Privacy Act.

Contain & take remedial action

In consultation with your Director*, your priority is to **contain** the data breach where possible. This means taking immediate **remedial action** to limit any further access or distribution of the relevant personal information. This may involve:

- recovering the documents or recalling an email sent in error
- contacting the information recipient and requesting that they do not open the offending email and instead delete it
- requesting ITSA to remove or change computer access privileges.

* It may be practicable to take some remedial action (e.g. email recall) before you report the incident. Ensure that your report provides details of any remedial actions already taken. The Privacy Officer/s must keep official records of all breaches and any actions taken.

Assess & take additional remedial action

The Privacy Officer/s will report matters (including breaches) to the NHMRC Privacy Champion. Where necessary, the Privacy Officer/s and/or the Privacy Champion will seek advice from NHMRC's Legal Advisors.

The Privacy Champion, in consultation with the relevant Executive Director (where necessary), will consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved (see *Attachment A*).

- If there are **reasonable grounds** to believe that the data breach is likely to result in serious harm, and remedial action (which is an exception) has not been able to prevent the risk of serious harm, then this is an '***eligible* data breach**'. The Privacy Champion will consider whether any additional remedial action can be taken.
- If there are **only grounds to suspect** that the data breach may result in serious harm, then NHMRC must conduct a formal assessment. The assessment process is to include:
  - **Initiation:** the Privacy Champion will promptly assign a team or person to undertake the assessment[7]
  - **Investigation:** the Assessor/s will promptly gather relevant information about the incident to determine what has occurred

6 Via nhmrc.privacy@nhmrc.gov.au.

7 See *Attachment A – Who should form the Assessment Team?* for further guidance.

– **Evaluation:** the Assessor/s will make an evidence-based decision about whether serious harm is likely, for consideration by the Privacy Champion.

This assessment is to be conducted expeditiously and all reasonable steps are to be taken to ensure that the assessment is conducted within **30 calendar days** of NHMRC becoming aware of the breach. If it cannot be completed within 30 days, the Assessor/s must document why this is the case.

The Privacy Officer/s must keep official records of the assessment process.

At any time, including during an assessment, NHMRC should take steps to reduce any potential harm to individuals caused by a suspected or eligible data breach.

If remedial action is successful in preventing serious harm to affected individuals, notification is not required as remedial action is an exception (see below).

Notify affected individuals[8]

a) Where **serious harm is likely** and **remedial action has not been able to prevent the risk of this serious harm** to any of the individuals whose information was involved:

- the Privacy Officer/s, in consultation with the Privacy Champion, must prepare a statement for the Australian Information Commissioner that contains:
  - the NHMRC Privacy Champion's contact details
  - a description of the breach
  - the kind/s of information concerned
  - recommended steps for affected individuals to assist them to take steps to mitigate or avoid harm.

  This statement must be submitted electronically via the form on the OAIC Website.

- NHMRC must also notify affected individuals, and inform them of the contents of the statement made to the Commissioner – unless an exception applies[9]. It is good practice to provide an explanation of what NHMRC is doing to prevent further breaches. Legal Services should be consulted before offering any formal apology.

  There are three options for notifying[10]:

  – **Option 1:** Notify all individuals
  – **Option 2:** Notify only those individuals at risk of serious harm

  If neither of these options are practicable:

  – **Option 3:** Publish the statement on the NHMRC website and take reasonable steps to bring its contents to the attention of individuals at risk of serious harm.

8 If the breach involves more than one entity, only one entity needs to undertake the required notifications. The NDB scheme allows the entities to decide who notifies, however, the OAIC suggests that the entity with the most direct relationship with the individuals at risk of serious harm should undertake the notification. See *Data breaches involving more than one organisation, the Office of the Australian Information Commissioner, December 2017*.

9 Exceptions do apply in limited circumstances– see *Attachment A*.

10 The NBD scheme provides flexibility. Whether a particular option is practicable involves consideration of the time, effort, and cost of notifying individuals. These factors should be considered in light of the capabilities and capacity of the entity.

Detailed guidance on 'how' to notify individuals is provided in the OAIC resource: *Notifying individuals about an eligible data breach*.

b) Where serious harm **is not** likely[11]:

- The decision to notify affected individuals is at the Privacy Champion's discretion.
- This discretion must not be used to reduce the risk of a complaint being made about NHMRC or to avoid any other legal or contractual obligations. A notification decision must be made in the best interests of the affected individual/s and in light of NHMRC's obligations to be transparent, accountable and to act in good faith.
- Notification to the Australian Information Commissioner is not required.

Prevention & review

The Privacy Champion will, in consultation with the relevant Executive Director, review the circumstances of the data breach and take action to prevent further breaches. This may include:

- fully investigating the cause of the breach, including consulting the ITSA
- developing a prevention plan
- conducting audits to ensure the plan is implemented
- updating security/response plan
- considering changes to policies and procedures
- revising staff training practices.

In reviewing the breach, the following are to be covered:

- whether there have been previous data breaches that may have a cumulative effect[12]
- whether there are other harms possible, including to NHMRC – e.g. loss of assets, regulatory penalties or legal liabilities.

The relevant Executive Director is to take actions necessary, in consultation with relevant senior managers and the Director of Human Resources, if the data breach has been identified as a result of staff misconduct or misbehaviour, which could result in a breach of the APS Code of Conduct.

In extreme cases, such action may require reporting the incident to other relevant bodies, including police or law enforcement.

11 Including where remedial action has been successful in preventing serious harm to affected individuals.

12 The Privacy Officer/s will maintain a database of breaches to allow the identification of systemic issues or training needs.

Attachment A: Notifiable Data Breaches (NDB) scheme

Key points:

- NHMRC has an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.
- The Australian Information Commissioner expects NHMRC to have practices, procedures and systems in place to comply with our information security obligations under APP 11, enabling suspected data breaches to be promptly identified, reported to relevant personnel, and assessed if necessary.
- The NDB scheme requires NHMRC to notify particular individuals and the Australian Information Commissioner about '*eligible* data breaches'.
- If NHMRC experiences a data breach, the first step is to contain the breach where possible and take remedial action. It must then assess whether the data breach is likely to result in serious harm to the individuals involved.
- If NHMRC has reasonable grounds to *believe that it has* experienced an eligible data breach, it must notify individuals and the Australian Information Commissioner about the breach as soon as practicable, unless an exception applies.
- In contrast, if NHMRC *only suspects that it may have* experienced an eligible data breach; it must quickly assess the situation to decide whether or not this has been an eligible data breach.
- An assessment must be reasonable and expeditious.
- The NDB scheme provides entities with the opportunity to take positive steps to address a data breach in a timely manner, and avoid the need for notification. At any time, including during an assessment, NHMRC should take steps to reduce any potential harm to individuals caused by a suspected or eligible data breach. If remedial action is successful in preventing serious harm to affected individuals, notification is not required.

What is an 'Eligible data breach' under the NDB scheme?

An 'eligible data breach' occurs when three criteria are met:

- there is unauthorised access to, or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds,
- this is likely to result in serious harm to one or more individuals, and
- the entity has not been able to prevent the likely risk of serious harm with remedial action.

What constitutes 'serious harm' and how does one determine whether it is 'likely'?

'Serious harm' is not defined by the Privacy Act. The OAIC has provided the following advice:

- Serious harm can be physical, psychological, emotional, financial or reputational harm.
- Entities should consider a broad range of potential harms. E.g.
  - identity theft
  - significant financial loss by the individual
  - threats to an individual's physical safety
  - loss of business or employment opportunities
  - humiliation, damage to reputation or relationships
  - workplace or social bullying or marginalisation.

- Entities should assess the risk of serious harm, having regard to the likelihood of the harm eventuating for individuals whose personal information was part of the data breach and the consequences of the harm.
- Understanding whether serious harm is likely or not requires an evaluation of the context of the data breach. E.g.
  - *Whose personal information was involved in the breach?*
  - *How many individuals were involved?*
  - *Do the circumstances of the data breach affect the sensitivity of the personal information?*
  - *How long had the information been accessible?*
  - *Is the personal information adequately encrypted, anonymised, or otherwise not easily accessible?*
  - *What parties have gained, or may have gained, unauthorised access to the personal information?*
- Whether a data breach is likely to result in serious harm requires an objective assessment, determined from the viewpoint of a reasonable person.

Section 26WG of the Privacy Act details the following (non-exhaustive) matters as relevant in determining whether access or disclosure would likely, or would not be likely, to result in serious harm:

- the kind or kinds of information
- the sensitivity of the information
- whether the information is protected by one or more security measures
  - if the information is protected by one or more security measures—the likelihood that any of those security measures could be overcome
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information
- if a security technology or methodology[13]:
  i) was used in relation to the information; and
  ii) was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information;

  the likelihood that the persons, or the kinds of persons, who:

  iii) have obtained, or who could obtain, the information; and
  iv) have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates;
  v) have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology
- the nature of the harm
- any other relevant matters.

A more detailed discussion of 'serious harm' and 'likelihood' is provided in the OAIC resource: *Identifying eligible data breaches, December 2017*.

13 If the security technology or methodology is encryption, an encryption key is an example of information required to circumvent the security technology or methodology.

Who should form the Assessment Team?

Possible Data Breach Assessment Team roles and skills include:

- a team leader – to coordinate the assessment team and report to the Privacy Champion.
- a privacy officer – to bring privacy expertise to the team.
- legal support – to identify legal obligations and provide advice.
- a risk management officer – to assess the risks.
- the Information Technology Security Advisor (ITSA) – to help establish the cause and impact of a data breach that involved an ICT system.
- information and records management expertise – to assist in reviewing security and monitoring controls related to the breach and to provide advice on the recording of the response.
- Human Resources support – if the breach is due to the actions of a staff member, which could result in a breach of the APS Code of Conduct.
- media/communications expertise – to assist in communication with affected individuals and dealing with the media and external stakeholders.

The roles and skills listed above are intended as a guide only and the membership of the Assessment Team will depend on the circumstances of the data breach. A single person may perform multiple roles and/or the assessment may be undertaken by one individual.

The role of team leader should be carefully considered. The team leader should have sufficient ability and authority to effectively manage the various sections within NHMRC whose input is required without needing to seek permissions. This is to ensure that the assessment is not unnecessarily delayed.

What exceptions apply?

Under the Privacy Act NHMRC is not required to notify an eligible data breach in certain circumstances, including, where:

- remedial action results in the conclusion that the access/disclosure would not be likely to result in serious harm (section 26WF)
- the eligible data breach is that of another entity (section 26WM)
- the CEO believes on reasonable grounds that notification would be likely to prejudice one or more of NHMRC's enforcement activities e.g. action taken under the *Research Involving Human Embryos Act 2002* or the *Prohibition of Human Cloning for Reproduction Act 2002* (section 26WN)
- compliance would be inconsistent with a secrecy provision, or a prescribed secrecy provision (section 26WP).

The Australian Information Commissioner may also use his/her discretion under section 26WQ to declare that an APP entity does not need to comply with the notification requirements in relation to a specific eligible data breach.

Should the Privacy Champion consider that an exception applies; the Privacy Champion will seek the advice of NHMRC's Legal Advisors.

Further guidance:

- *Identifying eligible data breaches*, the Office of the Australian Information Commissioner, December 2017
- *Assessing a suspected data breach*, the Office of the Australian Information Commissioner, December 2017
- *Exceptions to notification obligations*, the Office of the Australian Information Commissioner,
- *Data breaches involving more than one organisation*, the Office of the Australian Information Commissioner, December 2017
- *Notifying individuals about an eligible data breach*, the Office of the Australian Information Commissioner
- *What to include in an eligible data breach statement*, the Office of the Australian Information Commissioner

nhmrc.gov.au