RACGP

Royal Australian College *of* General Practitioners

Notifiable Data Breaches (NDB) scheme – Fact sheet

What is the NDB scheme?

The NDB scheme sets mandatory notification and control requirements for data breaches involving personal information held by an organisation. It outlines criteria for determining if a data breach is considered 'eligible' (notifiable) and the subsequent reporting requirements.

What is a data breach?

A data breach occurs when personal information held by an organisation is subject to unauthorised access or disclosure, or is lost.[1]

Does the NDB scheme apply to general practices?

Yes. Any entity that is considered to be a health service provider and that holds health information must comply with the NDB scheme. Access further information about what constitutes a health service here.

Why is the NDB scheme important to general practice?

General practices hold detailed personal information about patients. Reports have identified healthcare providers as significant sources of data breaches.[2]

Does the NDB scheme apply to data breaches relating to My Health Record?

No. If a data breach occurs from *within* a practice relating to the My Health Record system, a different reporting process applies. For further information on the required response, access the *Guide to mandatory data breach notification in the My Health Record system*.

What constitutes an eligible data breach?

An eligible data breach occurs when the following three criteria are satisfied:[1]

1. **Unauthorised access to personal information, unauthorised disclosure of personal information or loss of personal information has occurred**
   - Unauthorised access – personal information held by a practice is accessed by someone who is not permitted to have access. This may be an employee, an independent contractor or an external third party (such as a hacker).
   - Unauthorised disclosure – information held by a practice is made accessible or visible to others outside the practice (either intentionally or unintentionally).
   - Loss – accidental or inadvertent loss of personal information held by your practice, in circumstances where it is likely to result in unauthorised access or disclosure.

2. **The breach is likely to result in serious harm to one or more individuals**

   In this context, serious harm includes serious physical, psychological, emotional, financial or reputational harm. Examples may include identity theft, significant financial loss by an 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. For example, if a patient's bank details were accessed and used for fraudulent purchases through a Medicare data breach, this would be considered serious financial harm.

3. **The practice has not been able to prevent the likely risk of serious harm with remedial action**

   If a practice takes remedial action but cannot prevent the likelihood of serious harm, this constitutes an eligible data breach.

An eligible data breach has occurred – What do I do?

If you believe that your practice has experienced a data breach that meets the above criteria, you need to take immediate steps to contain the data breach by limiting further access or distribution, if possible. You must notify individuals at likely risk of serious harm. You must notify the Office of the Australian Information Commissioner (OAIC) as soon as practicable using the Notifiable Data Breach Form. The information you provide to individuals and the OAIC should include:

- the identity and contact details of your practice
- a description of the data breach
- the kinds of information concerned
- recommendations about the steps individuals should take in response to the data breach.

In the event of a data breach, you should promptly notify your practice's insurer and individual GPs' medical defence organisations.

How can my general practice reduce the risk and impact of data breaches?

You can mitigate the risk of data breaches by developing and maintaining practices, procedures and systems to ensure that personal information is protected from unauthorised access, unauthorised disclosure or loss. You should develop a clear data breach response plan to reduce the risk and impact of harm caused by data breaches. Access the RACGP's privacy and information security resources, including *Privacy and managing health information in general practice* and *Information security in general practice*.

Case study

An external hacker has infiltrated your practice management software and the Medicare data of approximately 100 patients has been accessed to obtain credit card details as part of a broader identity theft crime ring.

Has there been unauthorised access, disclosure or loss?

Yes, unauthorised access to the patients' information has occurred.

Is there risk of serious harm to one or more individuals?

Yes. Those patients whose Medicare data was infiltrated are at risk of identity theft.

Has the practice been able to prevent serious harm with remedial action?

No. The police investigation is ongoing.

This is a Notifiable Data Breach as it meets all three criteria. All affected patients must be contacted and the OAIC must be notified. As it does not relate to the MHR, the Australian Digital Health Agency does not need to be informed. For further case examples, refer to the OAIC website.

Additional OAIC resources

- Identifying eligible data breaches, www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response#part-1-data-breaches-and-the-australian-privacy-act
- PowerPoint presentation: Preparing for the Notifiable Data Breaches scheme, www.oaic.gov.au/resources/engage-with-us/consultations/notifiable-data-breaches/Preparing_for_the_NDB_scheme_webinar_slides.pdf

References

1. Office of the Australian Information Commissioner. Data Breach preparation and response – A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth). Sydney: OAIC, 2018. Available at www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response [Accessed 3 December 2018].
2. Office of the Australian Information Commissioner. Notifiable Data Breaches Quarterly Statistics Report: 1 April – 30 June 2018. Sydney: OAIC, 2018. Available at www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/notifiable-data-breaches-quarterly-statistics-report-1-april-30-june-2018 [Accessed 3 December 2018].