Office of the Information Commissioner
Queensland

Interpreting the legislation –*Information Privacy Act 2009*

Health agencies – data security (NPP 4)

This guideline does not reflect the current law.

It reflects the *Information Privacy Act 2009* as it existed prior to 1 July 2025.

It has been provided for the use of agencies and Ministers dealing with privacy complaints or compliance issues that occurred before 1 July 2025, and for bound contracted service providers to whom the pre-1 July 2025 IP Act continues to apply.

1.0 Overview

Health agencies are required to comply with the National Privacy Principles (**NPPs**) set out in the *Information Privacy Act 2009* (Qld) (**IP Act**).

NPP 4 requires a health agency[1] to protect the personal information it holds from unauthorised or inappropriate dealings, and to de-identify personal information once it is no longer needed for any purpose.

2.0 NPP 4 - data security

(1) A health agency must take reasonable steps to protect the personal information it holds from misuse, loss and unauthorised access, modification or disclosure.

(2) If the personal information is no longer needed for any purpose for which the information may be used or disclosed under NPP 2, a health agency must take reasonable steps to ensure that the individual the subject of the personal information can no longer, and can not in the future, be identified from the personal information.

Note—
Subsection (2) will apply subject to the requirements of the Public Records Act 2023 *providing for the retention of records.*

3.0 Data security

[1] In this Guideline references to 'a health agency' include bound contracted service providers of a health agency

NPP 4(1) requires that a health agency to have security safeguards in place to protect personal information, including health information. The safeguards apply equally to personal information held in paper form, electronically, as film, photographs, audio or video recording or any other media.

If personal information is not securely stored and managed there is an increased risk of privacy breaches. The principle requires that steps be taken to protect information against both accidental loss and intentional breach.

Practices that may lead to breaches of security include:

- leaving files containing personal information unattended at a public counter
- not disposing of records in a secure manner
- inadequate controls regarding which staff can access information; for example, inadequate user ID and password control on a database
- storing sensitive data on a laptop computer that is taken 'off-site' and not stored securely
- emailing confidential information.

A health agency must take reasonable steps to protect the personal information it holds. If this does not occur, a health agency will breach NPP 4, even if no misuse, loss, unauthorised access, modification or disclosure actually takes place.

Queensland Government Information Standard 18, Information Security (IS18) requires all departments and agencies to:

- establish an appropriate information security culture
- satisfy the 10 mandatory information security principles set out in IS18
- implement security measures beyond the minimum requirements commensurate with the information's value, business significance and sensitivity
- adhere to all legal and legislative requirements.

A health agency, its employees and agents must manage information in their custody so as to assure confidentiality, integrity and availability, taking into account its value, business significance and sensitivity, and within legal requirements.

4.0 Permanent deidentification of health information

4.1 Reasonable steps to deidentify

The management of documents held by a health agency will fall first under the Public Records Act 2023 (Qld), which may prohibit their destruction or amendment. NPP 4 is to be applied subject to the

requirements of the (PR Act) and any relevant Retention and Disposal schedules made under that Act.

NPP 4 requires a health agency to take reasonable steps to ensure that personal information is deidentified, for now and for the future. It does not require the destruction of documents when they are no longer needed for any purpose, however it does not prohibit destruction as a method of deidentifying personal information.

Personal information will be deidentified where the individual the subject of the information can no longer, and in the future will not be able to, be identified from the personal information. Deidentification must be permanent, which means that a health agency will not be able to match the deidentified information with other records to re-establish the identity of people.

A deidentification procedure would not be complete if, from the resulting information, the identity of an individual could be reasonably ascertained. The test relates to the definition of personal information. Once personal information is properly deidentified the information will no longer fit the definition. This will also take it outside the ambit of the IP Act, which means that the obligations in the NPPs will no longer apply.

What will constitute reasonable steps to deidentify personal information should be determined based on the circumstances of each case. It will also involve a consideration of the documents which contain the personal information. For example, the reasonableness of steps taken to deidentify personal information contained in electronic records will depend on the medium on which the data is stored and the available methods for erasing or amending data.

Reasonable steps could include:

- considering the capacity of a health agency to reidentify the information
- careful consideration of the identifying nature of every aspect of the information
- setting up safeguards that ensure future collections or uses will not reidentify the information
- ensuring departmental identifiers are removed from the information, where a health agency uses the same identifier for all of an individual's records.

Reasonable steps could also include ensuring that the deidentified information cannot be reidentified in the hands of an organisation receiving data. See *Privacy Guideline Section 4 – Key Concepts* for a discussion of 'reasonable'.

4.2 No longer needed for any purpose

NPP 4(2) specifies that the personal information must no longer be needed for any purpose for which the information may be used or

disclosed under NPP 2. This includes any legal requirement or authorisation that the information be retained in its complete form.

This means that the purpose for which it is retained in an identified form can be either the primary purpose of collection or for any other purpose which fits within the exception in NPP 2.

However, similar to the principles governing collection of information, there must be a genuine expectation that the information will be needed for that purpose. Information will often have great statistical and research value and can inform and guide public policy decisions. NPP 4(2) does not require that the information be deidentified, nor does it authorise retention of it in an identified form. This means that, for personal information in documents which are not required to be kept unamended under the *2023* (Qld) a health agency must turn its mind to whether the personal information is or will be needed for a permitted purpose.

This purpose must be specific and identifiable, rather than undefined and hypothetical. NPP 4(2) does not authorise retention of information 'just in case' it may be needed for some future use by the organisation or by a third party.

For additional information and assistance please refer to the OIC's privacy guidelines, or contact the Enquiries Service on 07 3234 7373 or email enquiries@oic.qld.gov.au.

First published 30 June 2009 and Last Updated 5 December 2024

Changes to legislation after the update date are not included in this document

This guideline does not reflect the current law.

It reflects the *Information Privacy Act 2009* as it existed prior to 1 July 2025.

It has been provided for the use of agencies and Ministers dealing with privacy complaints or compliance issues that occurred before 1 July 2025, and for bound contracted service providers to whom the pre-1 July 2025 IP Act continues to apply.