

Deidentifying Advanced Practice Recognition (vocational) pathway application case studies

This guidance is developed for all members lodging deidentified reports or case studies as part of an Advanced Practice Recognition application in a vocational pathway. The guidance assists members to deidentify evidence appropriately, upholding required standards under existing privacy legislation.

Osteopathy Australia sources this guidance as an original product of the Office of the Australian Information Commissioner.

This guidance is based upon [deidentification policies and procedures from the Office of the Australian Information Commissioner](#).

Read the guidance carefully before lodging evidence for the application process.

Members should use the provided consent form template with any patients or organisations to which your case studies are based upon.

Keep the signed consent form within your files and do not return a copy to Osteopathy Australia.

What does deidentification involve?

Deidentification involves removing or altering personal identifiers; it involves applying techniques or controls required to remove, obscure, aggregate, alter and/or protect data in ways that it is no longer about an identifiable (or reasonably identifiable) individual.

When information does not disclose an individual or organisation, it is not identifying personal information, which means it presents less privacy concerns. Deidentifying information enables it to be more broadly shared or made publicly available while still complying with the privacy principles, protecting the privacy of the individual, and ensuring the information remains appropriate for its intended use.

How to deidentify

Deidentification generally includes two steps. The first is the removal of direct identifiers, such as an individual's name, address or other directly identifying information. The second is taking one or more of the following steps:

- Providing access to only a fraction of the total existing records or data, thereby creating uncertainty that any person is included in the dataset
- Removing quasi-identifiers. For example, specific dates, work addresses, or income levels unique to an individual, or which in combination with other information, is reasonably likely to identify an individual or organisation

- Combining information or data that is likely to enable identification into categories. For example, age may be combined and expressed in ranges (25-35 years) rather than single years (27, 28). Extreme values above an upper limit or below a lower limit may be placed in an open-ended range such as an age value of 'less than 15 years' or 'more than 80 years'
- Altering information likely to enable identification in a small way, such that the aggregate information or data is not significantly affected — 'tolerable error'
- Swapping information enabling identification. For example, a person from a town in Australia may speak a language unique in that town. The specific spoken language could be placed in a broader category or replaced with a similar related language
- Creating new values from original data so that the overall totals, values and patterns are preserved, but do not relate to any specific individual or organisation
- 'Hashing' (blacking out) of identifiers — techniques that will obscure the original identifier, rather than remove it altogether, usually for the purposes of linking different datasets together (but without sharing the information in an identified form).

Choosing a deidentification technique

When picking a technique, consider the context of the information to be deidentified.

- Consider the sensitivity of the information to be deidentified
- Consider who will have access to the information, and for which purpose
- Consider whether the information contains unique or uncommon indirect or quasi-identifiers that could enable identification
- Consider whether the information will be targeted for identification by the receiving audience because of who or what it relates to
- Consider whether there is other information available publicly or elsewhere that could be matched up or used to identify an individual or organisation
- Consider what harm may result from identification.

Assess whether any chosen deidentification techniques, and any controls are appropriate to manage identification risk.

All Advanced Practice Recognition panels are bound by confidentiality agreements, and while this adds further protection, it does not negate your responsibility to prevent individual or organisational identification.

Deidentification is not necessarily a perfectible process in all instances.

Privacy requirements do not require deidentification to be absolute. Privacy will be satisfied, and information will be suitably deidentified, when the risk of an individual being reidentified is very low.

Questions and concerns

Please contact Osteopathy Australia's Senior Policy Officer – Clinical Excellence for a confidential discussion before application lodgement if you would like any clarification:

Phone: (02) 9410 0099

Email: clinicalpolicy@osteopathy.org.au