

# Privacy policy

Version 2.1 – March 2022

## Purpose

1. This policy sets out how the office of the National Health Practitioner Ombudsman collects, uses, stores and discloses personal and health information.
2. We use personal and health information to carry out our work under the Health Practitioner Regulation National Law (the National Law), the *Ombudsman Act 1976* (Cwlth), the *Privacy Act 1988* (Cwlth) and the *Freedom of Information Act 1982* (Cwlth).
3. The NHPO is a national organisation hosted by the Victorian Department of Health (the department). We choose to act consistently with the requirements of the *Privacy Act 1988* (Cwlth) and the Australian Privacy Principles.

## Collection of personal and health information

4. We try to only collect personal or health information if we need it to carry out our functions and activities.
5. Personal information is information or an opinion about an individual, or that could reasonably identify an individual. Information does not need to be true or recorded in a material form to be classified as personal information. Health information is any personal information that relates to an individual's health, including information about illness, injury or disability.
6. In general, the kind of personal information we collect may include a complainant or applicant's name, email and postal addresses, phone number, occupation and details about their complaint or matter. Much of the information we collect about complaints and freedom of information (FOI) review applications is considered sensitive because of the nature of our work.
7. We typically collect personal and health information in the following ways:
  - it is provided directly to us. For example:
    - a complainant or applicant makes an enquiry, complaint, or FOI review application to our office and provides us with their contact details or information about their matter
    - an individual provides information related to an investigation or review being conducting by our office
    - an individual applies for a job with us.
  - from a third party where it is not reasonable or practicable to collect the information directly from an individual. For example:

- from their authorised representative, if they have one
  - if a legal or official document mailed to an individual is returned to us, then we may need to request current contact details from another source.
  - through agencies (such as the Australian Health Practitioner Regulation Agency (Ahpra)) which are required under relevant legislation to provide information to us so that we can carry out our functions.
8. We may collect information when we make inquiries, investigate a complaint, or conduct an FOI review. We have broad discretion as to how to investigate matters and conduct reviews, including the information we can ask others to give to us.
  9. If we decide to conduct an investigation or a review, the complainant or applicant should expect that their personal information will be collected during this process. We may also collect information about a person associated with the matter (such as family members). If we open a file about the matter, it will also often include our opinion on it.
  10. We also collect information that individuals would reasonably expect to, or have consented to, sharing. This includes information from publicly available sources.
  11. Sometimes we are given personal information that we have not asked for (referred to as ‘unsolicited personal information’). When this happens, we assess whether we would be permitted under the Australian Privacy Principles to collect this information from the person whose personal information it is. If we could have collected it from that person during the course of our normal activities and functions, then we will retain the information. Otherwise, we will destroy the information or request that the individual destroy the information if we cannot.
  12. We endeavour to inform the individual if we collect personal information about them from someone else. However, in many cases this will not be reasonable because of the confidential nature of our work. For this reason, we generally cannot disclose that a complaint has been made to our office.

## Information online

### Website

13. Our website may record and log information for statistical purposes and to help us improve our services. This may include a site visitor’s:
  - IP address
  - date and time of the visit
  - pages accessed and documents downloaded
  - previous website visited
  - type of browser used.
14. We will not attempt to identify users of the website except where a law enforcement agency exercises a legal authority to inspect Internet Service Provider logs.
15. Our website service provider may also collect and use our website analytics data and may in extenuating circumstances access visitor information for the purpose of providing services to our

office. This may, for example, include security issue resolutions. If this occurs, we must be notified as soon as practicable about the incident and how the website or visitor information was accessed.

16. Our website may also contain links to other sites for general information. While we take reasonable care in linking to other websites, we are not responsible for the privacy compliance or the content of these other websites. Find out more about information we collect on our [website](http://www.nhpo.gov.au) at <www.nhpo.gov.au>.

### **Webform**

17. We use a web form hosted by our third-party case management system to allow users to, for example, make an enquiry or complaint or apply for an FOI review online. The information provided through this form is hosted by the provider of our case management system and is accessed through this system by our staff.

### **Social media**

18. Our social media terms of use require that social media users do not share personal or health information (including via private message or comment) on our Facebook or LinkedIn pages.
19. If social media users breach our terms of use, we reserve the right (where our social media channel allows) to remove this engagement. Repeated breaches of these terms of use may result in an individual being blocked or reported to the social media platform and other authorities at our discretion. This may include law enforcement if necessary.
20. We receive statistics on the reach, engagement and impact of our social media content from each platform. This data is grouped and not identifiable to any specific individual who has interacted with our social media pages. We use this data to improve social media users' experience across our digital platforms and measure the effectiveness of our social media communication.
21. We may also use information shared with us on social media to improve the handling of complaints to our office.
22. Social media users should familiarise themselves with the policies and terms and conditions of the social media platform they are using. Each platform has its own binding terms and conditions.
23. Our media policy provides further information about staff obligations when using social media, including measures to ensure staff safety on social media.

### **Anonymity and confidentiality**

24. We will do our best to engage with individuals who wish to remain anonymous or use a pseudonym. However, sometimes we are required by law to deal with individuals who have identified themselves, or it is impracticable for us to deal with an individual on an anonymous or pseudonymous basis.
25. We accept confidential complaints. A complainant may request that only limited information is disclosed to the entity that is the subject of a complaint or review. Our office or the relevant entity may, however, not have enough information to respond to a confidential complaint. This may mean that it is difficult to proceed with the matter.
26. In some circumstances, we may be compelled to share information about a confidential complaint with others, such as if the matter is the subject of legal proceedings.

27. We prefer that those seeking to make a confidential or anonymous complaint contact us by phone (if possible). This provides us with an opportunity to check our understanding of the complaint issues we need to consider and also to discuss the limitations we may face in progressing the matter. For more information about making a confidential or anonymous complaint please visit our [website](http://www.nhpo.gov.au): <www.nhpo.gov.au>.
28. We are generally unable to accept anonymous applications for a review of an FOI decision.

## How we use and disclose personal or health information

29. We use and disclose personal and health information for the reason it was collected (the primary purpose) to perform our roles and activities.
30. We cannot use or disclose personal and health information for another reason (a secondary purpose) unless an exemption applies. Exemptions include:
  - consent is given for the use or disclosure for a secondary purpose
  - we believe it is reasonably necessary for enforcement-related activities carried out by, or on behalf of, an enforcement body
  - a secondary purpose is required or authorised under an Australian law, or court or tribunal order.
31. We address some specific situations below, such as use and disclosure during complaints and reviews, in publications and to the media.
32. We may also use information for planning, funding, evaluation, and improving our services. Where appropriate and practicable, identifying details will be removed from information used for these purposes.

## Complaints and reviews

33. To ensure fairness and to assist in resolving a complaint and FOI review applications, we may disclose relevant information about the details of a complaint or application to the entity that is the subject of the complaint or application.
34. A complainant or applicant must provide authority for an individual to seek information about a matter before we will disclose this information. For example, we cannot provide progress updates or information about a complaint or application to friends, family members or legal representatives unless the appropriate authority is provided.

## Publications

35. We may publish information about our work, such as annual reports, performance reports, FOI review decisions and investigation reports. This includes publishing deidentified data and case studies (sometimes called 'stories').
36. We may disclose personal information in investigation reports to set out the grounds for the findings, conclusions and recommendations contained in the report. All identifying personal information will be removed unless it is fair and reasonable in the circumstances to do so.

37. We publish all FOI review decisions made by the Commissioner. All identifying personal information is removed from these decisions.

## Media

38. We may make statements to the media, participate in media interviews and deliver presentations in public forums about the functions and activities of our office.

39. We generally do not provide personal or health information related to a complaint or FOI review application to the media. In some circumstances we may do so if the individual has provided their consent or if it is in the public interest to do so.

## Quality of personal information

40. We take steps to ensure that personal information we collect is accurate and complete. This includes:

- recording information in a consistent format
- promptly adding updated or new information to existing records.

## Securing personal and health information

41. We take reasonable steps to protect information we hold from unauthorised or inappropriate access, use, modification, disclosure, or other interferences. For example, we ensure:

- password protection of electronic records
- paper files are safely secured in locked areas
- all staff and people engaged to carry out work on behalf of our office are permitted access to records containing personal information on a 'need-to-know' work-related basis only
- access to information is more tightly restricted if required. For example, virtual barriers may be created to prevent employees of third parties (such as consultants and contractors) who are engaged to carry out work on behalf of our office from accessing information contained in electronic records
- protective markings (information sensitivity labels) are applied to value and assess the sensitivity of information
- privacy impact assessments are undertaken to ensure projects comply with this policy.

42. When no longer required, personal information may be destroyed in a secure manner (except where archiving is required).

43. As outlined in our Service Charter, our office does not tolerate any harm, abuse or threats directed towards our staff at work, including the disclosure of a staff member's personal information for a secondary purpose without their consent.

44. If personal information provided through engagement with our office is shared without consent, we will take all reasonable steps to reduce any risk posed to our staff. This may include requesting that information is redacted, removed or made private, or referring a matter to another relevant body, such as the police or a media provider (such as Facebook).

## How we store information

45. Electronic copies of all personal and health information collected by our office, including information provided via telephone, email or post, will be stored in a secure, third-party hosted case management system. This system was custom built for our office and interacts with the department's document management system.
46. The personal and health information stored in our case management system will be accessed by our staff as they consider and respond to enquiries, complaints and FOI review applications. From time to time, technical support may also be provided by the case management system provider or from the department. Technical and support personnel are contractually required to maintain confidentiality and comply with this policy and relevant legislation.
47. The provider who hosts our case management system only stores information within an Australian government approved datacentre in Australia.
48. Publicly available information on our website is stored using public cloud infrastructure that may be onshore or offshore.

## Access to, and correction of, personal and health information

49. Anyone may ask for access to personal information we hold about them or ask that we correct that information. The person's identity will be verified before access to the relevant information is provided, or the information is corrected.
50. If we receive a request for access to personal information, we may choose to provide a copy of only the portions of information that contain the individual's personal information. This is assessed on a case-by-case basis depending on the purpose of the request.
51. If a document or other source of information contains reference to a third person, we may delete all reference to that third person when giving access to a document or other information to protect the privacy of that third person.
52. If we receive a request for a correction, we will assess whether it is reasonable in the circumstances to correct that information after considering why we hold that information. We may choose to add information to the information we already hold instead of removing personal information.
53. To request access to, or to correct, personal information we hold, please contact us on our contact details below.

## How to make a complaint

54. If anyone is dissatisfied with how we have handled their personal information, please let us know.
55. We welcome feedback and applications for a review of our decisions. We see this as an opportunity to address concerns, provide a better explanation of a decision or action and improve our services for others.
56. We request that the staff member who managed the matter is contacted first to discuss any concerns before a complaint is made, if possible.

## Contact us

Post	National Health Practitioner Ombudsman (NHPO) GPO Box 2630 Melbourne VIC 3001
Phone	1300 795 265
Email	<a href="mailto:complaints@nhpo.gov.au">complaints@nhpo.gov.au</a>
Website	<a href="https://nhpo.gov.au">https://nhpo.gov.au</a>

## Policy review

57. The Ombudsman and Commissioner will review this policy every three years in consultation with staff and relevant stakeholders.

Version	2.1
Responsible work area	Complaints and FOI unit, manager
Date introduced	15 February 2016
Date/s modified	October 2020, March 2022
Next scheduled review date	March 2025

To receive this document in another format phone 1300 795 265, using the National Relay Service 13 36 77 if required, or email <[complaints@nhpo.gov.au](mailto:complaints@nhpo.gov.au)>.

Authorised and published by the National Health Practitioner Ombudsman, 50 Lonsdale St, Melbourne.

GPO Box 2630

Melbourne VIC 3001

Phone 1300 795 265

[Email](mailto:complaints@nhpo.gov.au) National Health Practitioner Ombudsman <[complaints@nhpo.gov.au](mailto:complaints@nhpo.gov.au)>

National Health Practitioner Ombudsman [website](https://nhpo.gov.au) <<https://nhpo.gov.au>>

© National Health Practitioner Ombudsman, Australia, March 2022.