Privacy management plan

industry.nsw.gov.au/nrar

Published by NSW Department of Planning, Industry and Environment

Natural Resources Access Regulator Privacy Management Plan

First published August 2020

More information

Natural Resources Access Regulator

industry.nsw.gov.au/nrar

PUB20/831

Contents

1. Introduction

The Natural Resources Access Regulator (NRAR) is an independent regulator established under the *Natural Resources Access Regulator Act 2017* (NRAR Act). NRAR is responsible for compliance and enforcement measures for natural resources management legislation, which currently includes the *Water Management Act 2000* and the *Water Act 1912* and associated regulations.

We are independent, but we are still a NSW Government agency—a public sector agency bound by the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act) to protect the privacy of our clients, staff and others about whom we hold personal and health information. To do so, we must:

- prepare and implement a privacy management plan in accordance with section 33 of the PPIP Act
- comply with the information protection principles specified in Part 2 of the PPIP Act
- comply with the health privacy principles specified in Part 3 of the HRIP Act.

Our privacy management plan sets out:

- our policies and practices for complying with the PPIP Act and the HRIP Act, including the information protection principles and health privacy principles
- how we will inform our staff about these policies and practices so that we properly manage and protect private information
- our procedures for dealing with privacy internal reviews under Part 5 of the PPIP Act
- other relevant matters about protecting the private information we hold.

1.1. Purpose of this document

We take the privacy of our staff and stakeholders seriously and will manage and protect private information, using this privacy management plan as a reference and guidance tool. This privacy management plan:

- details our commitment to protecting the privacy of our stakeholders, staff and others about whom we hold private information
- explains our functions and activities and the main types of private information we deal with when carrying out these functions and activities
- identifies how the requirements of the PPIP Act and the HRIP Act apply to the private information we manage and how these requirements interact with our obligations under the *Government Information (Public Access) Act 2009* (GIPA Act)
- explains our strategies to comply with the PPIP Act and HRIP Act
- provides our staff with the necessary knowledge and skills to manage private information appropriately
- ensures you understand how to make a complaint or request an internal review if you are concerned that your privacy may have been breached

- ensures you understand how to request access to your private information or an amendment of that information to ensure it is accurate
- explains how we will be transparent and accountable in how we manage private information.

2. Definitions

Commercially sensitive information includes:

- any matter that, if disclosed, would place a business at a substantial commercial disadvantage in relation to other businesses or potential businesses, whether at present or in the future
- any intellectual property in which a business has an interest
- a business' financing arrangements
- a business' cost structure or profit margins
- a business' full base case financial model (for government contractors).

Health information is a specific type of personal information and is defined in section 6 of the HRIP Act as information or an opinion about:

- the physical or mental health or a disability (at any time) of an individual
- an individual's express wishes about the future provision of their health services
- a health service provided, or to be provided, to an individual.

Health information also includes other personal information that is:

- collected relating to provision of a health service
- connected with the donation of an individual's body parts, organs or body substances
- genetic information about an individual arising from health service provisions that could potentially predict the health of the individual or their relative.

Health information may include psychological reports, blood tests or X-rays and information about a person's medical appointment.

Natural resources management legislation is defined in section 3(1) of the *Natural Resources Access Regulator Act 2017* as the *Natural Resources Access Regulator Act 2017*, *Water Management Act 2000*, *Water Act 1912* and any other Act or parts of an Act administered by a relevant Minister that is prescribed by the regulations.[1]

Personal information is defined in section 4 of the PPIP Act. It is essentially any information or opinions about a person where that person's identity is apparent or can be reasonably ascertained. Personal information can include a person's name, address, information about a person's sexual preferences, financial information and photos.

Personal information may be:

- written records

[1] To date, no other Acts/parts of Acts have been prescribed by the regulations.

- electronic records, photos, images, video or audio footage and maps
- biometric information, such as fingerprints, blood and records of genetic material.

The PPIP Act excludes certain types of information from the definition of personal information. The most significant exemptions relevant to NRAR apply to information:

- about people who have been dead for more than 30 years
- contained in publicly available publications
- arising out of a royal commission or special commission of inquiry
- contained in Cabinet and executive council information
- about a person's suitability for public sector employment.

Private information is a generic term used in this plan that includes commercially sensitive information, personal information and health information.

Privacy principles include the information protection principles prescribed in the *Privacy and Personal Information Protection Act 1998* and the health privacy principles prescribed in the *Health Records and Information Privacy Act 2002*.

Both the information protection principles and health privacy principles contain 12 principles about how to collect, store, access, amend, use and disclose private information. The health privacy principles include another three specific principles for health information in relation to identifiers and anonymity and transferrals and linkages. How we apply the information protection principles and health privacy principles is discussed in section 4.

3. About NRAR

As an independent regulator established under the NRAR Act, we are guided by our legislative objectives to:

- ensure effective, efficient, transparent and accountable compliance and enforcement measures for the natural resources management legislation
- maintain public confidence in the enforcement of the natural resources management legislation.

To do this, we will:

- promote compliance with the objectives of the Water Management Act and the Water Act
- achieve best-practice management and regulation of surface water and groundwater, floodplains and controlled activities
- take a risk-based and outcome-focused approach to regulation
- guide officers' decision-making and action by the adoption of a graduated and proportionate response to legislative non-compliance
- ensure decisions on enforcement action are transparent to the community.

We seek to build community confidence as a trusted, credible, effective, efficient and transparent regulator. To do this, we have developed policies and strategies to help us better

mitigate risks, deliver greater certainty for the regulated and wider community and achieve sustainable use of, and access to, natural resources. These include the following:

- our regulatory framework
- our regulatory policy
- our regulatory priorities
- our code of ethics and conduct
- our ethics framework: *Embedding ethics in NRAR's DNA*
- our guidelines on reporting alleged breaches of the Water Management Act and Water Act: *Compliance with water legislation*
- our prosecution guidelines
- a public register of information about enforcement actions taken by or on behalf of NRAR.

For more information about us and to view these policies and strategies, see the NRAR website.

We have also committed to developing and maintaining a quality management system in accordance with AS/NZS ICO 9001:2016.[2]

This Privacy management plan is part of our policy framework and quality management system.

For our staff:
The WATERS electronic document library is a key part of our quality management system and is where all the electronic records sit. You can find all our strategic documents (policies and plans), systems, business processes and procedures, work instructions and other supporting tools in WATERS. These materials include information about the collection, storage, access, amendment, use and disclosure of private information. You can also find this privacy management plan in WATERS.

3.1. NRAR's functions

Our functions are specified in section 11 of the NRAR Act. They include:

- preparing strategies, policies and procedures relating to enforcement powers under the natural resources management legislation
- advising and reporting to the minister about the administration of the natural resources management legislation
- providing advice or reports to the minister
- publishing details of enforcement actions taken for offences under the natural resources management legislation
- carrying out prescribed functions under the Water Management Act, including water licensing and approvals, monitoring and audit and investigations and enforcement.

[2] See NRAR Quality Policy Statement, August 2019.

3.2. Private information NRAR deals with

In carrying out our functions, we collect and hold private information within our systems, or are provided with access to private information collected and held by others, through sharing agreements.

Private information is primarily collected and held for the purpose of carrying out prescribed functions under the Water Management Act. For example, we may collect private information when processing applications for licences and approvals, responding to enquiries, handling complaints, investigating alleged non-compliance and taking enforcement action. We also collect and hold private information when recruiting and managing staff.

The private information we collect and hold typically includes:

- names
- addresses or property information
- phone numbers and email addresses
- licenses and approvals—current and applied for
- relationship information, such as those between spouses or employees and organisations
- safety alerts, including cautions
- summaries of compliance activities and the enforcement actions we have undertaken, including penalty infringement notices, advisory letters, directions and complaints received.

While NRAR does not directly provide a health service, we do hold some health information. For example, in relation to employees, we hold information about their sick leave or workers compensation matters. We may also hold health information that has been provided to us as part of carrying out our functions.

4. How NRAR complies with the privacy principles

This section explains how we will comply with the privacy principles. We must comply with all the privacy principles unless an exemption applies. If an exemption applies, the way we comply with the privacy principles may differ from what is explained in this section. Section 5 explains how and when exemptions may apply.

The PPIP Act and HRIP Act contain privacy principles about the collection, storage, access, amendment, use and disclosure of private information. The principles establish the legal obligations and standards for collecting and dealing with private information to minimise the risk of misuse of that information. They also give you the right to request access to your private information or to ask for amendments to that information to ensure it is accurate.

The degree of sensitivity of the private information influences the way in which we apply the privacy principles. The more sensitive the nature of the information, the higher the level of care that our staff use when dealing with such information, particularly where disclosure to a third party is being considered.

For our staff

You should familiarise yourself with the privacy principles and remember these top five tips:

- be aware of what private information is
- be aware of what private information is involved in your work
- be aware of the rules about what you can and can't do with private information
- be cautious when dealing with private information
- seek advice from the Information Access and Privacy Unit when in doubt or when starting a new project that touches on private information.

As part of the NSW Government's Planning, Industry and Environment cluster, we are supported by the Information Access and Privacy Unit (or GIPA team) within the Department of Planning, Industry and Environment.

By following the link on WATERS to the department's intranet home page, you can find:

- contact details for the Information Access and Privacy Unit
- general information about applying the privacy principles.

From the department's intranet home page, you can also navigate to 'managing information' and 'requests for information' through the link to 'ethics and conduct'.

Information about applying the privacy principles is part of the following mandatory induction training for new staff:

- code of conduct
- ethics and values
- records management.

You can also find fact sheets and other information on the Information and Privacy Commission website: www.ipc.nsw.gov.au/privacy/privacy-resources-public-sector-agencies.

4.1. Collecting private information

The collection of private information is covered by information protection principles 1 to 4 and health privacy principles 1 to 4. These privacy principles relate to the lawful, direct, open and relevant collection of private information.

We collect and receive people's private information in a variety of ways to perform our services and functions. The collection of this information may be in writing, over email, through the NRAR website enquiry form or the request for assistance form, over the phone, by fax or in person at an NRAR office.

Lawful

We limit what we collect. We collect personal information only for lawful purposes that are directly related to our work as an independent regulator responsible for water licensing and approvals, monitoring and audit and investigations and enforcement, as provided for in the natural resources management legislation. We only collect personal information that is reasonably necessary for us to carry out our work and we ensure that the collection of private information is not excessive or an unreasonable intrusion.

We decide what level of information is appropriate to be collected for each enquiry on a case-by-case basis, with the understanding that the details collected must contain enough information to be an accurate record of the issue and assistance given, but should not contain unnecessary or irrelevant private information.

For our staff
If you plan to collect information, ask yourself, ‘Do I need this private information to do my job?’ If not, do not collect the private information. If you are not sure whether the information you are asking for is private information, ask yourself, ‘Can I figure out who this person is if I put two and two together?’ If you can, you are probably dealing with private information.

Direct

There are several ways that information can be collected. Information may be:

- collected from you through your direct actions with us, such as registering on the NRAR website, applying for a licence, informing us of an allegation, complaint or issue, paying for a service by credit card, taking a test or responding to questionnaires or surveys
- collected from you through your direct actions with another public sector agency that has a sharing agreement with us (see section 5.2 for more information about information shared between public sector agencies)
- observed, such as by our staff during a site inspection or collected through online cookies
- derived, which means mechanically collected. This information includes records of the number of times the NRAR website is visited, how often a service is requested, or some other arithmetic process applied to data to predict future demand for services. Information collected in this way is likely to be de-identified so it would be impossible to specifically identify individuals
- inferred, which means that statistical information is drawn from the information we hold. This could include response scores or the number of services requested. Information collected in this way is likely to be de-identified so it would be impossible to specifically identify individuals.

At NRAR, we collect personal information directly from you wherever possible unless an exemption applies. Section 5 explains how and when exemptions may apply. You may also authorise someone else to provide personal information on your behalf. Similarly, if we require personal information about an individual under 16 years, we will collect the information from their parent or guardian.

Open

When we collect personal information from you, we will explain that we are collecting personal information and:

- why we are collecting your personal information
- what we will use your personal information for and who is likely to receive it
- that we will not disclose or transfer your personal information without your consent, unless otherwise lawfully authorised to do so
- that you have a right to access, modify and suppress your personal information.

We will also explain whether you have a legal requirement to provide the private information to us, and the consequences of not providing the information. If there is no legal requirement, we will explain that the information is being collected voluntarily.

In most cases we meet these requirements by including a privacy statement or collection notice on application or questionnaire forms used to collect the private information or on the NRAR website when seeking submissions.

For our staff
We have built considerations about the collection of private information into our work practices and procedures. For example, our application forms include a privacy statement and we have procedures in place for interviewing witnesses and suspects. If you are developing new in web-based transactions, forms, surveys, questionnaires or other instruments, you are responsible for meeting the requirements of this privacy management plan by including a collection notice. Template collection notices can be found in WATERS.

Relevant

We will take reasonable steps to ensure that the personal information we collect is:

- being collected as part of carrying out our legislative function
- relevant to the purpose for which it has been collected
- not excessive
- accurate, up to date and complete
- not an unreasonable intrusion into your personal affairs.

4.2. Storing private information

The storage of private information is covered by information protection principle 5 and health privacy principle 5. At NRAR, we are committed to:

- securely keeping your private information and protecting it from unauthorised access, use, modification or disclosure
- keeping your private information no longer than necessary
- disposing of your private information appropriately.

Storing information securely

As part of the NSW Government's Planning, Industry and Environment cluster, we are supported by the Digital Solutions Group of the department for system security. The Digital Solutions Group is continuously improving its ability to protect and defend our online systems from cyber attacks, in line with NSW's cybersecurity strategy and policy. This is achieved by designing better digital solutions, reducing the number of vulnerabilities in systems, restricting access privileges, expanding cybersecurity knowledge and strengthening our ability to withstand and quickly recover from cyber attacks and other cyber-related incidents.

We manage the security of your private information from external threats by integrating security into the architecture, policies and procedures of the core applications and systems we use, particularly our:

- network
- complaints and incidents reporting system (CIRAM)

- water licensing system (WLS)
- feedback system (Feedback Assist)
- electronic document management system (Content Manager 9).

These systems are designed in accordance with the Digital Solutions Group's requirement for a 'defence in depth' approach, in which a series of defensive mechanisms are layered in order to protect valuable data and information.

NRAR's network is protected by an enterprise-grade firewall and intrusion prevention and detection system to monitor network traffic to block a wide range of known vulnerability exploits. We apply an information and communication technology policy and staff use passwords and, where possible, encrypt information to ensure personal information is protected and kept secure. All staff must comply with the NRAR code of ethics and conduct.

All applications are built on top of enterprise-ready services from Amazon Web Services in Australia. Amazon Web Services is a leading provider of managed services and has achieved a high standard regarding its security certifications (ISO 27001, ISO 27017 and ISO 27018), including SOC 1, 2 and 3 type 2 certifications. The Amazon Web Services network is protected against denial-of-service attacks.

CIRAM enables us to record and manage all compliance-related activities and to lower risks associated with compliance and regulation. The tool has been developed and is managed by the third-party vendor, Bay Technology, while being hosted by the Digital Solutions Group in Amazon Web Services. It is designed to comply with standards that include selected *Australian Government information security manual* controls that ensure secure software-development practices, role-based access controls, protection of data in transit by encryption and adequate event logging. Daily reviews are performed by Bay Technology.

WLS is a web-based portal that provides our staff with a consolidated workspace of applications that directly relate to water regulation activities. WLS is owned and managed by WaterNSW, while being hosted by the Digital Solutions Group in Amazon Web Services. WaterNSW uses third-party security specialists to find and fix vulnerabilities in the IT infrastructure and the application.

Feedback Assist is built on the principle of 'no wrong door'. It provides you with an easily accessible contact point for lodging a complaint and provides us with a mechanism for tracking and managing complaints. It is built on Salesforce technologies and is provided and managed by the NSW Government's Customer Service cluster. Complaints made through our website are tracked and managed through Feedback Assist.

Content Manager 9 (CM9) is our electronic document and records management system and it plays a role in keeping private information secure. Classified information is not permitted to be kept digitally in CM9. CM9 also has functions that allow staff to restrict access to records and protect sensitive information. All staff using CM9 must abide by the NRAR code of ethics and conduct, records management policies and procedures and any associated legislation. User activity in CM9 leaves audit trails that clearly show the documents a user has accessed. Users must complete a training course which covers protecting personal and sensitive information before they can have access to CM9. Hard copy files are protected by security measures, such as physically securing sensitive files in locked rooms or cabinets.

For our staff
Cybersecurity is a rapidly evolving challenge. It is important that we take some simple steps to help protect our systems and information. These include that you: • do not share or reuse your passwords • physically secure your devices if you are travelling for work with them • do not use public wi-fi with sensitive data • think twice before opening email attachments and/or links • talk to the Digital Information Office before purchasing or using any new information, communications and technology services, software or devices to ensure they are secure and meet our cybersecurity requirements, now and in the future • report cybersecurity incidents or breaches to the Digital Information Office service centre • use dissemination-limiting markers and access controls to label and restrict access to any sensitive information you capture in CM9. You can find information about using these markers and controls by following the link on WATERS to the department's intranet home page. From the department's intranet home page, search for 'CM9 quick guides' • take advantage of the cybersecurity online training available to all NRAR staff. **For our people leaders:** • determine what information communication and technology access an employee, contractor or third party should have • ensure employees have the right level of access—no more and no less • ensure the timely amendment of existing access when employees leave or change their role, including revocation of access where appropriate.

In addition to the systems outlined above, we are working with the department to develop the Metering Data Acquisition Service. The Metering Data Acquisition Service will collect, ingest, store and share extraction metering data with multiple agencies including NRAR, WaterNSW and the department.

The Metering Data Acquisition Service is a critical government information system that requires physical data and cybersecurity. For this reason, the Digital Solutions Group were on the Metering Data Acquisition Service tender panel and have been consulted during development.

The Metering Data Acquisition Service system has the following components:

- Amazon Simple Storage Service bucket for storage of unedited datalog files in the cloud. The Metering Data Acquisition Service's transmission of data is encrypted end to end
- eagle.io platform (including back-end database, data ingestion processes, alerts and alarms, operator graphical user interface tools and web-publishable dashboards). Every interaction with the system is authenticated to ensure the user performing the interaction or operation has permission to do so
- approved secure telemetry service provider networks. Outbound connections from local intelligence units in the field to the Metering Data Acquisition Service eagle.io platform are made through private telemetry networks— encrypted virtual networks—not visible on the internet. Each local intelligence unit has a unique identifier, static IP address or other unique device number that is assigned to them depending on the

network they use. eagle.io also has measures in place to prevent malicious interference with the data as it travels from the local intelligence unit to the cloud. This includes protection against spoofing of data loggers with fake consumption data. Currently there is one approved private telemetry network, the Telstra machine-to-machine virtual private network

- field equipment (dataloggers) connected to the Metering Data Acquisition Service. Water meters are secured by tamper-evident seals and are compliant with Australian Standard AS 4747. Dataloggers, modems and data cables are also secured by tamper seals or switches and some devices have password protection.

Information is kept no longer than necessary and disposed of appropriately

We will not keep personal information any longer than is necessary. Once personal information is no longer required, NRAR staff will ensure it is securely disposed of and protected from misuse.

The NSW records management policy and the *State Records Act 1998* provide guidance on storing information. The retention and disposal authority relevant to a record will be followed. For example, records relating to compensation claims, financial management or industrial relations are kept for a minimum of seven years after action is completed.

4.3. Accessing accurate private information

Access to private information and the accuracy of private information is covered by information protection principles 6 to 8 and health privacy principles 6 to 9. These privacy principles relate to being transparent about what private information is being stored/used, allowing you to access your private information and allowing you to update, correct or amend your private information. These privacy principles also interact with our obligations under the GIPA Act.

Transparent data collection

We seek to build community confidence as a trusted, credible, effective, efficient and transparent regulator. To do this we work with the community, encouraging you to notify us when you believe a breach of the Water Management Act or Water Act has occurred or is occurring. When you report a breach using our hotline (1800 633 362), email (nrar.enquiries@nrar.nsw.gov.au) or online form, we will record your report and ensure we handle all the information you provide in accordance with the GIPA Act and the PPIP Act.

If you have provided a postal or email address in your report, you will receive an acknowledgement letter or email. An NRAR officer conducting the risk assessment may contact you if they need more information.

If we investigate, the investigating officer may contact you and, if you agree, may take a witness statement. If the matter goes to court, the witness statement may be made available to the alleged offender if it forms part of our case.

If you have any concerns about your safety because you have made a report, we will take these seriously, but this may limit our capacity to employ an appropriate regulatory response to the report. We may be able to keep your identity confidential in any subsequent court proceedings under public interest immunity.

For more information about how we respond to reports, refer to the section on reporting suspicious water activities on our website or see the NRAR compliance with water legislation guidelines.

How to access, update, correct or amend your private information

If you wish to know whether we hold private information about you, you can contact us directly to enquire. If you believe that your private information held by us is inaccurate, irrelevant, not up to date, incomplete and/or misleading, you can request that it be amended.

To make an access or amendment request, you should contact the business area holding the information (if known). Otherwise email patiunit@planning.nsw.gov.au to contact our officers, who will advise you whether we hold your private information, the nature of the private information and the main purposes for which the private information is used.

Access to your private information will be provided without excessive delay or expense, usually within 20–30 working days of receiving a request. If there is likely to be a delay in providing the information, we will explain the delay and advise when the information is likely to be available. If we refuse your request to access personal information under the PPIP Act, we will provide you with reasons.

In making a request to amend private information, you will need to demonstrate that the information is in fact inaccurate, irrelevant, not up to date, incomplete and/or misleading. That is, you will need to provide evidence to support your claim.

After receiving your request, we will determine whether it is appropriate to amend the private information within 20–30 working days. If we are not prepared to amend your private information, we will explain why and may instead add a note to the information indicating the amendment you sought. If we deny your request for amendment, you have rights to internal review under the PPIP Act. Section 10 of this plan outlines the internal review and complaints process.

How privacy principles and the GIPA Act interact

Access to private information and the accuracy of private information that are covered by information protection principles 6 to 8 and health privacy principles 6 to 9 also interact with our obligations under the GIPA Act.

The GIPA Act establishes a proactive, more open approach to gaining access to government information in NSW by:

- authorising and encouraging the proactive release of information by NSW public sector agencies, including NRAR
- giving you a legally enforceable right to access government information
- ensuring that access to government information is restricted only when there is an overriding public interest against releasing that information.

The guiding principle of the GIPA Act is public interest. It is generally presumed that we will disclose or release information unless there is an overriding public interest against doing so.

Of all categories of information held by government agencies, the type most often requested is private information. People may request access to their own personal information, either in its own right or in combination with other government information, or they may seek access to the private information of other people. This presents the following challenges:

- you have two options when applying to access your private information—under the GIPA Act and under the PPIP Act
- personal information is defined differently in the GIPA Act and the PPIP Act
- under the GIPA Act, personal information can be a public interest consideration both for and against disclosure, depending on the circumstances.

An access application under the GIPA Act should only need to be lodged as a last resort. Where access applications are needed, the GIPA Act outlines the process that applicants and agencies should follow, as well as the options for reviewing decisions about an access application.

For our staff

You should familiarise yourself with the key aspects of the GIPA Act and remember these top tips:

- do not release information unless you are delegated, authorised or required to do so
- when in doubt, seek the assistance of the Information Access and Privacy Unit.

As part of the NSW Government's Planning, Industry and Environment cluster, we are supported by the Information Access and Privacy Unit (or GIPA team) within the department.

By following the link on WATERS to the department's intranet home page, you can find:

- contact details for the Information Access and Privacy Unit
- general information about applying the privacy principles.

From the department's intranet home page, you can also navigate to 'managing information' and 'confidentiality and privacy' through the link to 'ethics and conduct'.

For more information about personal information and the GIPA Act, see the guidelines for personal information as a public interest consideration under the GIPA Act published by the NSW Information Commissioner. These guidelines are designed to assist us in dealing with requests for personal information under the GIPA Act and discuss whether we should apply the GIPA Act or PPIP Act definition of personal information.

4.4. Using private information

The use of private information is covered by information protection principles 9 and 10 and health privacy principle 10. These privacy principles ensure we only use accurate private information and that our use of private information is limited.

Before using your private information, we will ensure that the information is relevant, accurate, up to date, complete and not misleading. This means that if time has passed since the information was collected, or there is any other reason to have concerns about the adequacy of the information, we will take reasonable steps to check that it is still accurate, up to date, relevant, complete and not misleading.

We will generally only use private information for the purposes for which it was collected or a directly related purpose. If there is a need to use the information for another purpose, we will ask for your consent unless the information needs to be used to prevent or lessen a serious or imminent threat to any person's health or safety.

Please note that section 5 explains how and when exemptions may apply when applying these principles.

4.5. Disclosing private information

The disclosure of private information is covered by information protection principles 11 and 12 and health privacy principle 11. These privacy principles relate to restricting the disclosure of private information and safeguarding particularly sensitive information from disclosure.

Unless an exemption applies (see section 5), we only disclose private information to other parties if:

- you agree to the disclosure
- you are aware that this sort of information is usually disclosed
- we need to disclose the information to fulfil the purpose for which it was first collected
- disclosure is necessary to prevent a serious and imminent threat to any person's health and safety.

Information relating to ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership is never disclosed without consent unless it is necessary to prevent a serious and imminent threat to any person's health and safety.

Private information is not given to anyone outside NSW unless there are similar privacy laws in that person's state or country or the disclosure is authorised by law.

We risk disclosing private information when we send that information to you by post, email or social media. We consider the possibility of third parties intercepting your correspondence and using that information for identity fraud. To reduce this risk, we keep private information included in any correspondence to a minimum.

Information made digitally available—to conform with open government principles or otherwise—will be de-identified, anonymised or redacted to remove any personal identifying information belonging to individuals. Please note that section 5 explains how and when exemptions may apply when applying these principles.

For our staff

While most information relating to active investigations is regarded as confidential, there are additional considerations against release of commercially sensitive information under section 14 GIPA Act. Section 54 of the GIPA Act sets out what information may require third-party consultation when making a decision about an access application under Part 4 of the GIPA Act. Third-party consultation may be required for information that concerns a person's (or entity's) business, commercial, professional or financial interests.

If you are unsure about anything privacy or GIPA Act related, contact the Information Access and Privacy Unit.

As part of the NSW Government's Planning, Industry and Environment cluster, we are supported by the Information Access and Privacy Unit (or GIPA team) within the department.

By following the link on WATERS to the department's intranet home page, you can find:

- contact details for the Information Access and Privacy Unit
- general information about applying the privacy principles

From the department's intranet home page, you can also navigate to 'managing information' and 'confidentiality and privacy' through the link to 'ethics and conduct'.

4.6. Health information: identifiers and anonymity

For health information, there are additional health privacy principles (health privacy principles 12 and 13) that apply to identifying you with an identification number and giving you the option of receiving services anonymously.

We will only assign an identifier to you if it is reasonably necessary to carry out our functions efficiently.

Where it is lawful and practicable, you will be given an opportunity to retain your anonymity when transacting with us.

For our staff
Our people and culture team may collect health information in order to manage cases of injured staff and to investigate workplace incidents. Where health information has been gathered to case-manage an injured staff member, it is not given a separate identifier but kept against the relevant employee's injury management record. Where the information has been gathered as part of an investigation of a workplace incident, the information is held against the investigation file and not given any separate identifier. The people and culture team has no linkages to any health records systems.

4.7. Health information: transferrals and linkages

For health information, there are additional health privacy principles (health privacy principles 14 and 15) that apply to transferring information outside NSW and using health record linkage systems.

We will only provide health information to another person or body who is in a jurisdiction outside NSW, or to a Commonwealth agency, where:

- it is a legal requirement and upholds the health privacy principles
- you have consented to the transfer
- the transfer is for your benefit and it is impracticable to obtain consent—were it practicable to obtain, consent would likely be given
- the transfer is necessary to do something you have requested
- the transfer is reasonably necessary to lessen or prevent serious and imminent threat to your life, health or safety.

We will not include your health information or disclose an identifier about you in a health record linkage system unless you have expressly consented to the information being included.

5. When NRAR is exempt from the privacy principles

Section 4 of this plan explains how we comply with the privacy principles, but there are exemptions to this. The circumstances in which we may not have to comply with the privacy principles are explained in Part 2, Division 3 of the PIPP Act. Additional circumstances are explained in Part 3 of the PIPP Act and there are corresponding provisions in the HRIP Act. Particularly important to our activities are the exemptions relating to:

- investigative agencies and law enforcement

- information exchanges between public sector agencies
- public registers.

5.1. Exemptions for investigative agencies and law enforcement

Investigative agencies are defined in section 3 of the PPIP Act as specific offices, such as the Ombudsman's Office, as well as any other public sector agency with investigative functions where:

- those functions are exercisable under the authority of an Act or statutory rule
- the exercise of those functions may result in the agency taking or instituting disciplinary, criminal or other formal action or proceedings against a person or body under investigation.

Our investigative functions are prescribed in the NRAR Act and Water Management Act. The exercise of these functions may result in us taking or instituting disciplinary, criminal or other formal action or proceedings against a person or body under investigation—such as where a person has taken water from a river without a licence or when not authorised by a licence or has interfered with or damaged metering equipment.

As an investigative agency, we may not comply with some of the privacy principles if doing so may detrimentally affect or prevent us from properly exercising our complaint handling or investigative functions. For example, we may:

- collect private information about you from someone else—that is, not from you directly
- collect private information without informing you that it is being collected or the purpose for which it is being collected—for example, we may use surveillance cameras for the purpose of collecting evidence as part of our investigations into alleged offences of the natural resources management legislation
- share your private information with other investigative agencies.

The situations where we may not comply with the privacy principles on the grounds of being an investigative agency are limited to those prescribed in section 24 of the PPIP Act.

As an independent regulator, we are both an investigator and enforcer of the natural resources management legislation. When undertaking law enforcement, section 23 of the PPIP Act prescribes the circumstances in which we may not comply with the privacy principles. For example, we may not inform you that information is being collected where the collection is for law enforcement purposes and we may disclose your private information as part of court proceedings for an offence.

For our staff
We are developing procedures for the use of equipment, such as surveillance cameras; these will be available on WATERS. These procedures will ensure we use optical surveillance equipment in a way that complies with the *Surveillance Devices Act 2007* and the *Workplace Surveillance Act 2005*.

5.2. Exemptions for information exchanges between public sector agencies

The privacy principles protect your private information; for example, they limit the circumstances in which your information may be disclosed. However, we may not comply with some of the privacy principles if we are acting under section 16 of the NRAR Act or the exemptions provided in the PPIP Act.

Section 16(2) of the NRAR Act specifically provides for the sharing of information between the agencies associated with administration of the natural resources management legislation or the administration of the *Water Act 2007* (Cwlth). Under section 16(2) of the NRAR Act we may share information about the:

- granting of licences or other authorities
- issuing of notices, orders or directions
- exercise of enforcement powers, including information necessary to protect the safety of our staff when exercising their enforcement powers
- institution of proceedings for offences under the natural resources management legislation.

To clarify what this information sharing involves in certain circumstances, we enter into agreements with other agencies. While more agreements are being developed, we have entered into:

- a memorandum of understanding with the Murray–Darling Basin Authority
- a memorandum of understanding with WaterNSW
- a protocol with Crown Lands.

The sharing of information that is provided for in section 16 of the NRAR Act is recognised as an exemption to the privacy principles in section 25 of the PPIP Act. Similarly, under section 27A of the PPIP Act, NRAR is exempt from the privacy principles if we are providing private information to, or receiving private information from, another public sector agency and the disclosure is reasonably necessary to:

- deal with, or respond to, correspondence from a minister or member of Parliament
- enable inquiries to be referred between the agencies concerned
- enable the auditing of the accounts or performance of a public sector agency or group of public sector agencies—for example, NRAR's performance may be audited by the Natural Resources Commission to determine whether the provisions of a water management plan are being given effect to (see section 44 of the Water Management Act).

For our staff

If you receive a request for information from another agency:

- confirm if the requested information falls under a memorandum of understanding or protocol—these documents can be found on WATERS
- if the agency has relied upon legislation in its request, check that legislation to ensure the request is legitimate.

5.3. Exemptions for public registers

Public registers are defined in the PIPP Act as registers containing personal information required by law to be made publicly available or open to public inspection. Under section 12A of the NRAR Act we may keep, and may make publicly available, a register of the information about the enforcement action we take or that is taken on our behalf—this is the NRAR Public Register. We maintain the NRAR Public Register as a deterrent and to maintain transparency and public confidence in our activities.

When publishing information on the NRAR Public Register we publish in accordance with section 12A of the NRAR Act and clause 6 of the *Natural Resources Access Regulator Regulation 2018*, and apply the following principles:

- we ensure that all published information is accurate, impartial and balanced
- we provide the public and media with factual information about the outcome of investigations and charges which have been filed in courts
- we ensure that published information is not defamatory and/or in violation of the rules and conventions relating to *sub judice*. This means we will not publish information about cases that are still being considered or that are before the courts. We also will not publish information that is subject to name suppression or publication orders or that in any way prejudices the fair hearing or objectivity required for judicial matters.

The NRAR Public Register is located on our website and the information published includes most of the regulatory actions taken for breaches of the Water Management Act. This information includes convictions, written undertakings, charges for water taken, compliance audits, injunctions, orders for remedies and any fees, charges or civil penalties recovered. Information is not currently published where the outcome of an investigation is an advisory letter, warning or official caution.

While we do not comment on or publicise the specifics of ongoing investigations, we recognise that some enforcement actions taken early in investigations are of significant community interest. This can include orders to stop works or activities we have found to be in contravention of the Water Management Act, to prevent an ongoing breach or harm. While such orders may form part of any ongoing investigations, they are published on the NRAR Public Register. For those regulatory actions that are published, we publish only private information that is relevant to our regulatory action.

The NRAR Public Register is regularly updated and we try to ensure that all information published is accurate, impartial, balanced and encourages compliance with the natural resources management legislation. This includes updating the NRAR Public Register as soon as practicable after becoming aware of any:

- appeals made against a conviction—when an appeal or court election is lodged, *subject to appeal* will be added to the *Particulars* column in the NRAR Public Register
- changes made by appeal courts to orders or sentences
- decisions quashing or annulling a conviction.

Any person whose private information is recorded in the NRAR Public Register may request that their details be suppressed in accordance with section 58(1) of the PIPP Act. If you would like to make a request for anonymity, please contact us at: nrar.enquiries@nrar.nsw.gov.au

After receiving your request, we will consider:

- whether retaining the private information in the NRAR Public Register would significantly affect a person's safety or wellbeing
- whether maintaining public access is of greater public interest than any individual interest in suppressing the private information.

Unless we are of the opinion that maintaining public access is of greater public interest than any individual interest in suppressing the private information, we will supress the private information as requested.

5.4. Other exemptions relevant to NRAR

Under section 41 of the PPIP Act and section 62 of the HRIP Act, the Privacy Commissioner may make a direction to waive or modify the requirement for a public sector agency to comply with an information protection principle, a health privacy principle or a privacy code of practice.

Agencies can approach the Privacy Commissioner to request a direction. The general intent is for directions to apply temporarily. If necessary, we may approach the Privacy Commissioner to request a direction.

Under the PPIP Act, privacy codes of practice may be created to allow an agency to modify the application of one or more privacy principles or specify how they are to be applied to activities or classes of information. If necessary, we may work with the Information and Privacy Commission to incorporate our work into privacy codes of practice.

6. Data Analytics Centre and sharing information

The *Data Sharing (Government Sector) Act 2015* (DSGS Act) was created to promote sharing of information for certain purposes. It allows the government to carry out data analytics to identify issues and solutions to better develop government policy, program management and service planning and delivery.

The DSGS Act allows information to be shared quickly with the Data Analytics Centre—which operates within the Department of Customer Service—or between other government sector agencies. It also provides protections in connection with data sharing and ensures compliance with the requirements of the PPIP Act and the HRIP Act.

We are required to ensure that any private information contained in the data that is shared complies with PPIP Act and HRIP Act. We are also obliged to ensure that any confidential and commercial-in-confidence information contained in the data to be shared complies with any contractual or equitable obligations of the data provider around how it is dealt with.

Before responding to a request for information from the Data Analytics Centre, we consult internally to obtain relevant advice and may also seek advice from the Privacy Commissioner.

7. Workplace surveillance

Computer and other workplace surveillance is undertaken as a preventative measure for both internal and external threats. In general, an employer may carry out a wide range of

surveillance if employees are properly notified. This is called ‘overt surveillance’, or surveillance of which everyone is aware.

The Digital Solutions Group continuously surveils our workplace systems and equipment in line with the *Workplace Surveillance Act 2005.* This may include reviewing email accounts, electronic files and internet usage on work computers and mobile devices, such as tablets and smartphones.

Recording of private conversations is covered by the *Surveillance Devices Act 2007*. Legal advice can be sought internally or externally by staff regarding both workplace surveillance and the recording of private conversations.

If overt surveillance is in place, employees must be given written notice that includes the following items:

- the kind of surveillance used—for example, by camera, computer or tracking
- how the surveillance will be carried out
- when it will start
- whether it will be continuous or intermittent
- whether the surveillance will be ongoing or for a specified limited period.

Information or the results collected through overt surveillance cannot be used or disclosed unless the use or disclosure is:

- related to the employment of NRAR employees
- related to NRAR business activities or functions
- given to a law enforcement agency in relation to an offence
- related to civil or criminal proceedings
- reasonably believed necessary to stop an imminent threat of serious violence to persons or substantial damage to property.

A breach of the above restrictions carries a fine. Note that access to the information can be requested by an employee or a person who was captured by the surveillance. Such requests can be made under the PPIP Act or the GIPA Act.

Surveillance about which employees are not properly notified is automatically regarded as ‘covert surveillance’ and is generally prohibited by legislation, except for the purpose of establishing whether employees are involved in unlawful activity while at work. Covert surveillance of employees can only be done with the authority of a magistrate.

8. Privacy impact assessment

A privacy impact assessment may be required to assess any actual or potential effects that an activity, project or proposal may have on private information. A privacy impact assessment can also outline ways to mitigate any identified risks and enhance any positive impacts. Consulting with the public and measuring community expectations are important parts of any thorough privacy impact assessment.

Privacy risks can be avoided or mitigated by:

- ensuring a project complies with the law
- ensuring a project meets community expectations
- making a project less invasive of privacy
- making a project more privacy-enhancing.

It may not be possible to eliminate or mitigate every risk, but ultimately we will make a judgement about whether the public benefit from the project outweighs the risk posed to privacy.

The benefits of carrying out a privacy impact assessment include:

- identifying risks, benefits, costs and safeguards involved in a project
- ensuring compliance with privacy legislation
- reducing costs in management time, legal expenses and potential media or public concern by considering privacy issues early
- anticipating and responding to possible privacy concerns
- enabling informed decision-making
- increasing the legitimacy of a project, especially where some compromise is necessary.

For our staff

To know if a privacy impact assessment is required for your project, you should answer the questions in Appendix 1.

If the answer to one of more of these questions is 'yes', then advice should be sought from the Information Access and Privacy Unit and a privacy impact assessment should be seriously considered.

As part of the NSW Government's Planning, Industry and Environment cluster, we are supported by the Information Access and Privacy Unit (or GIPA team) within the Department. You can find the contact details for this team by following the link on WATERS to the department's intranet home page. From the department's intranet home page, navigate to 'managing information' through the link to 'ethics and conduct'.

You can also find information about privacy impact assessments in the Guide to PIAs in NSW, published by the Privacy Commissioner.

9. Breach of privacy and data breach notifications

If a data breach is identified—whether it is serious or not—we will notify affected individuals, unless the breach is in relation to information that is not sensitive, poses little-to-no risk of harm or if it is decided that notification is not required.

A serious data breach is defined as unauthorised access to, unauthorised disclosure of or unauthorised loss of private information where, as a result, there is a real risk of serious harm to any individual to whom the information relates.

If we become aware of a possible data breach, we will determine if a breach has occurred, noting there are circumstances that allow personal information to be released.

Should we determine a breach has occurred:

- we will contact the person
- we will report the breach to the Information Access and Privacy Unit within the department and may report it to the NSW Privacy Commissioner
- we will report the breach in the department's annual report.

For our staff
If you believe there has been a breach of privacy, contact the department's Information Access and Privacy Unit as soon as possible. Generally, it will be up to the business unit, in consultation with the Information Access and Privacy Unit, to respond to the breach, taking any action to remedy the situation and notify the affected individuals. A template for notifying affected individuals can be found in the department's privacy management plan. A copy of the notification to the affected individuals should be forwarded to the Information Access and Privacy Unit. If it has been decided that the Privacy Commissioner should also be advised, the Information Access and Privacy Unit will then notify the Privacy Commissioner and provide a copy of your notification to the affected individuals.

10. Complaints and internal reviews

If you consider that we have breached a privacy principle, a privacy code of practice or a public register provision in the PPIP Act, you are entitled to an internal review of our conduct. To resolve the issue, you can:

- raise an informal complaint with us
- raise a formal complaint with us
- submit a formal application for an internal review of conduct with us—there is no cost to request an internal review
- lodge a formal complaint with the Information and Privacy Commission.

Informal complaints

If you want to resolve an issue informally, please contact the relevant area of NRAR, if you know it, to discuss your issue. Informal complaints may be referred for an internal review to be carried out if it is considered that a serious breach of privacy has occurred, or that it is more appropriate to deal with your complaint on a formal basis.

Formal complaints

You can make a formal complaint by contacting us by:

- emailing nrar.enquiries@nrar.nsw.gov.au
- phoning 1800 633 362
- the online 'contact us' form or online feedback form, which you can access through a widget on our website.

Complaints are handled in line with the former Department of Industry's Service Related Complaints Procedure.

Applying for an internal review of conduct

If you apply for an internal review of our conduct, we must follow the requirements in Part 5 of the PPIP Act. Your application must:

- be lodged within six months of becoming aware of the legal implications or significance of the alleged conduct
- be in writing
- have a return address in Australia.

You can make an application by submitting the application form available from the Information and Privacy Commission website to paitunit@planning.nsw.gov.au

A senior officer who was not substantially involved in the matter will conduct the internal review. This officer is responsible for reviewing the action or decision and deciding if it is correct. We must complete reviews within 60 days.

If you are unhappy with the outcome of our internal review or do not receive an outcome within 60 days, you have the right to seek an external review by the NSW Civil and Administrative Tribunal.

You have 28 calendar days from the date of the internal review decision to seek an external review under section 55 of the *Administrative Decisions Review Act 1997*.

To request an external review, you must apply directly to the NSW Civil and Administrative Tribunal, which has the power to make binding decisions on an external review. To apply for an external review or to obtain more information about seeking an external review, including current forms and fees, please contact the NSW Civil and Administrative Tribunal.

For our staff
If you are undertaking an internal review under the PPIP, you should refer to the Privacy Commissioner's guidance materials. You can also seek advice from the Information Access and Privacy Unit and use the outline for an internal review report provided in the department's privacy management plan. As part of the NSW Government's Planning, Industry and Environment cluster, we are supported by the Information Access and Privacy Unit (or GIPA team) within the department. The Information Access and Privacy Unit are responsible for the department's privacy management plan. By following the link on WATERS to the department's intranet home page, you can find: • contact details for the Information Access and Privacy Unit • general information about applying the GIPA Act. From the department's intranet home page, you can also navigate to 'managing information' and 'requests for information' through the link to 'ethics and conduct'.

Lodge a complaint with the Information and Privacy Commission

If you would prefer to have an external party address your concerns, you can lodge a formal complaint with the Information and Privacy Commission. Information about lodging a complaint with the Information and Privacy Commission is available on their website: www.ipc.nsw.gov.au

11. Promoting the plan

We promote the principles of our privacy management plan through our executive team and staff.

Our executive team is committed to transparency and accountability around NRAR's compliance with the PPIP Act and the HRIP Act. The executive team reinforces transparency and compliance with the PPIP and HRIP Acts by:

- endorsing the privacy management plan and making it publicly available on the NRAR website
- identifying privacy issues when implementing new systems
- ensuring all staff are aware of sound privacy management practices.

We ensure our staff are aware of and understand this privacy management plan and particularly how it applies to the work they do. With this in mind, we have written this plan in a practical way so staff members understand what their privacy obligations are, how they can manage private information in their work and what they can do if they are unsure.

We make our staff members aware of their privacy obligations by:

- publishing the privacy management plan on our website
- publishing the privacy management plan internally on WATERS
- including the privacy management plan in induction packs
- providing privacy training
- highlighting and promoting the privacy management plan during Privacy Awareness Week and Month.

12. Accountabilities

All staff, including contractors, have a duty to act in accordance with this privacy management plan. Staff are also required to comply with the NRAR code of ethics and conduct.

Offences associated with private information can be found in Part 8 of the PPIP Act and Part 8 of the HRIP Act. It is an offence to:

- intentionally disclose or use personal information accessed as a part of our work for an unauthorised purpose
- offer to supply personal information that has been disclosed unlawfully
- hinder the Privacy Commissioner or a staff member from doing their job
- attempt to persuade an individual to refrain from making or to withdraw an application pursuing a request for access to health information or a complaint to the Privacy Commissioner or Tribunal
- by threat, intimidation or false representation, require another person to give consent or to do without consent an act for which consent is required.

Section 308H of the *Crimes Act 1900* also provides that it is an offence to access or modify computer records for purposes that are not connected with the duties of the person.

If staff feel uncertain as to whether certain conduct may breach their privacy obligations, they should seek advice from the department's Information Access and Privacy Unit.

13. Contacts

Department of Planning, Industry and Environment
Information Access and Privacy Unit
Email: paitunit@planning.nsw.gov.au
Phone: 02 9860 1440
Post: 4 Parramatta Square, Locked Bag 5022, Parramatta NSW 2124

Information and Privacy Commission
https://www.ipc.nsw.gov.au/
Email: info@ipc.nsw.gov.au
Phone: 1800 472 679
Post: GPO Box 7011, Sydney NSW 2001

NSW Civil and Administrative Tribunal (NCAT)
https://www.ncat.nsw.gov.au/
Email: aeod@ncat.nsw.gov.au
Phone: 1300 00 NCAT or 1300 006 228 and follow the prompts
Post: PO Box K1026, Haymarket NSW 1240 | DX 11539 Sydney Downtown

Appendix 1: Privacy impact assessment checklist

Will your project involve:

- the collection of personal information, compulsorily or otherwise
- a new use of personal information that is already held
- a new or changed system of regular disclosure of personal information, whether to another agency, another State, the private sector or to the public at large
- restricting access by individuals to their own personal information
- new or changed confidentiality provisions relating to personal information
- a new or amended requirement to store, secure or retain particular personal information
- a new requirement to sight, collect or use existing ID, such as an individual's driver's licence
- the creation of a new identification system, such as using a number or a biometric
- linking or matching personal information across or within agencies
- exchanging or transferring personal information outside NSW
- handling personal information for research or statistics, de-identified or otherwise
- powers of entry, search or seize or other reasons to touch another individual, such as taking a blood or saliva sample
- surveillance, tracking or monitoring of individuals' movements, behaviour or communications
- moving or altering premises that include private spaces
- any other measures that may affect privacy?